Radio Frequency Identification Fundamentals and Applications, Bringing Research to Practice

Radio Frequency Identification Fundamentals and Applications, Bringing Research to Practice

Edited by

Cristina Turcu

Intech

Published by Intech

Intech

Olajnica 19/2, 32000 Vukovar, Croatia

Free online edition of this book you can find under www.sciyo.com
Additional copies can be obtained from:
publication@sciyo.com

First published February 2010
Printed in India

Preface

This book, entitled *Radio Frequency Identification Fundamentals and Applications, Bringing Research to Practice*, bridges the gap between theory and practice and brings together a variety of research results and practical solutions in the field of RFID. The book is a rich collection of articles written by people from all over the world: teachers, researchers, engineers, and technical people with strong background in the RFID area. Developed as a source of information on RFID technology, the book addresses a wide audience including designers for RFID systems, researchers, students and any person who would like to learn about this field.

The first chapter of this book analyzes an algorithm for interrogation zone estimation in inductive coupled anti-collision RFID identification systems. The field aspects of operation conditions are taken into consideration.

Chapter 2 presents an overview of the RFID identification process and focuses on how RFID systems work in static and dynamic scenarios, collisions in the Medium Access Control (MAC) layer, the more relevant and adopted EPCglobal specifications and the performance analysis of the identification process.

In chapter 3 the author reviews several approaches in solving passive RFID tag collision problems.

Chapter 4 addresses two important issues related to RFID system: electronic and MAC protocol characterization to avoid reader-reader and reader-tag collisions in a dense RFID network.

Chapter 5 aims to analyze the MAC technologies adopted in RFID, considering both deterministic and stochastic MAC protocols for RFID systems proposed in standards, specifications and recent literature. Their principles are described and their performance is assessed and compared through theoretical and numerical arguments.

Chapter 6 is dedicated to stochastic model and performance analysis of RFID. The chapter comprises reviews of the frame slotted ALOHA based tag anti-collision protocols. Also, the authors investigated a stochastic model for RFID tag collision resolution. Various methods proposed for the estimation of RFID tag population within the vicinity of the RFID reader are examined and evaluated.

Chapter 7 presents an overview of several RFID anti-collision algorithms and proposes an improved dynamic framed slotted ALOHA algorithm for a large number of tags.

Chapter 8 briefly reviews already existing RFID systems and provides an in-depth analysis of a commercial development system. The authors present a speed measurement application using the same RFID system and important EMC information regarding the use of high frequency RFID system.

In chapter 9 the authors propose an IP-based RFID architecture that allows low cost and large scale deployment, as well as an easy integration with IP-based services.

Chapter 10 presents the fundamentals of object tracking and focuses on one special technique to develop an RFID network and the ways in which tagged objects can be tracked in such a network.

Chapter 11 deals with the designing and verifying the secure authentication protocol, which is widely researched in RFID systems using formal methods. Thus, the RFID security requirements in home network environments are defined, and an authentication mechanism among reader, tag and database is proposed.

The authors of chapter 12 propose an RFID tag system that includes an interrogator with an algorithm that generates RFID passwords to protect both the RFID data and consumer privacy.

In chapter 13 the authors describe an authentication mechanism based on the COMP-128 algorithm to be used in mobile RFID environments.

Chapter 14 offers an introduction to RFID systems, summarizes several concepts of RFID system integration, and introduces some integration examples of RFID applications.

Chapter 15 focuses on major short and long-term benefits of RFID systems and advices on efficient RFID technology integration.

Chapter 16 explores fundamentals of data management in RFID applications so that the data retrieved out of RFID applications is non-redundant and filtered.

Chapter 17 discusses different design possibilities for data storage in RFID systems and their impact on the quality factors of the resulting system.

In the final chapter of this book the authors introduce the widely applied RFID middlewares with the technique of Web services and propose a Context store approach to improve the performance of data transmission between a mobile client and a Web services server.

At this point I would like to express my thanks to all scientists who were kind enough to contribute to the success of this project by presenting numerous technical studies and research results. But, we couldn't have published this book without InTech team's effort. I wish to extend my most sincere gratitude to the InTech publishing house for continuing to publish new, interesting and valuable books for all of us.

Editor

Cristina TURCU
Department of Computer Science
Stefan cel Mare University of Suceava
Romania

Contents

Field Conditions of Interrogation Zone in Anticollision Radio Frequency Identification Systems with Inductive Coupling

Piotr Jankowski-Mihułowicz
Rzeszów University of Technology
Poland

1. Introduction

Passive Radio Frequency IDentification (RFID) systems with inductive coupling are the most widespread nowadays (Yan et al., 2008; Wolfram et al., 2008). These systems operate thanks to direct inductive coupling between antenna units of the communication system which consist of Read/Write Device (RWD) and electronic identifier (called a tag or transponder). The communication in transmitter – receiver set is carried out in two ways. In the first case, only one object with electronic tag can be placed in the correct working area called **interrogation zone** of the RFID system. This arrangement is called **a single identification system** or also single system. In the second case of multiple identification system, called **anticollision system**, the communication process is carried out simultaneously with multiple RFID tags. In this process, the algorithms of multi-access to the radio channel are used, what provides an effective way to distinguish simultaneously between multiple objects (Yeh et al., 2009; Dobkin & Wandinger, 2005). It should be note that synthesis procedure of interrogation zone includes the simultaneous analysis of electromagnetic field (presented in this paper), communication protocols and electric aspects of operation conditions in the process of system efficiency identification. The typical applications of anticollision RFID systems are concentrated on different economic and public activity in industry, commerce, science, medicine and others (Harrison, 2009, Donaljdson, 2009; Steden, 2005; Wyld, 2009 and 2005; Åhlström, 2005).

When determining the interrogation zone for the given automatic identification process, it is necessary to define a maximum working distance of the RFID system. This parameter determines the distance between the specified point of the RWD's and the midpoint of the tag's antenna loop. It is very important because the magnetic field generated around the RWD's antenna loop is not only medium of information signal but also provides passive tags with energy. The proper supply is essential to carry out operations of recording and reading information which is stored in the transponder's semiconductor memory (Fig. 1).

The basic parameter, which determines the working area and characterizes the maximum working distance of the RFID system, is H_{min} minimum value of magnetic field strength or more often used B_{min} **minimum value of magnetic induction** at which the correct data transmission between the RWD and the tag takes place (Jankowski-M. & Kalita, 2008). The minimum value of magnetic induction required in the process of writing data to the

internal memory of tag ($B_{minWrite}$) is several percent larger than the value of this parameter in the process of reading ($B_{minRead}$). So the operation mode of the internal memory affects occurrence of changes in the interrogation zone. There is decreasing the maximum distance in writing mode in comparison to reading process. During the analysis of field conditions in RFID system the general case will be considered and represented by notation B_{min}.
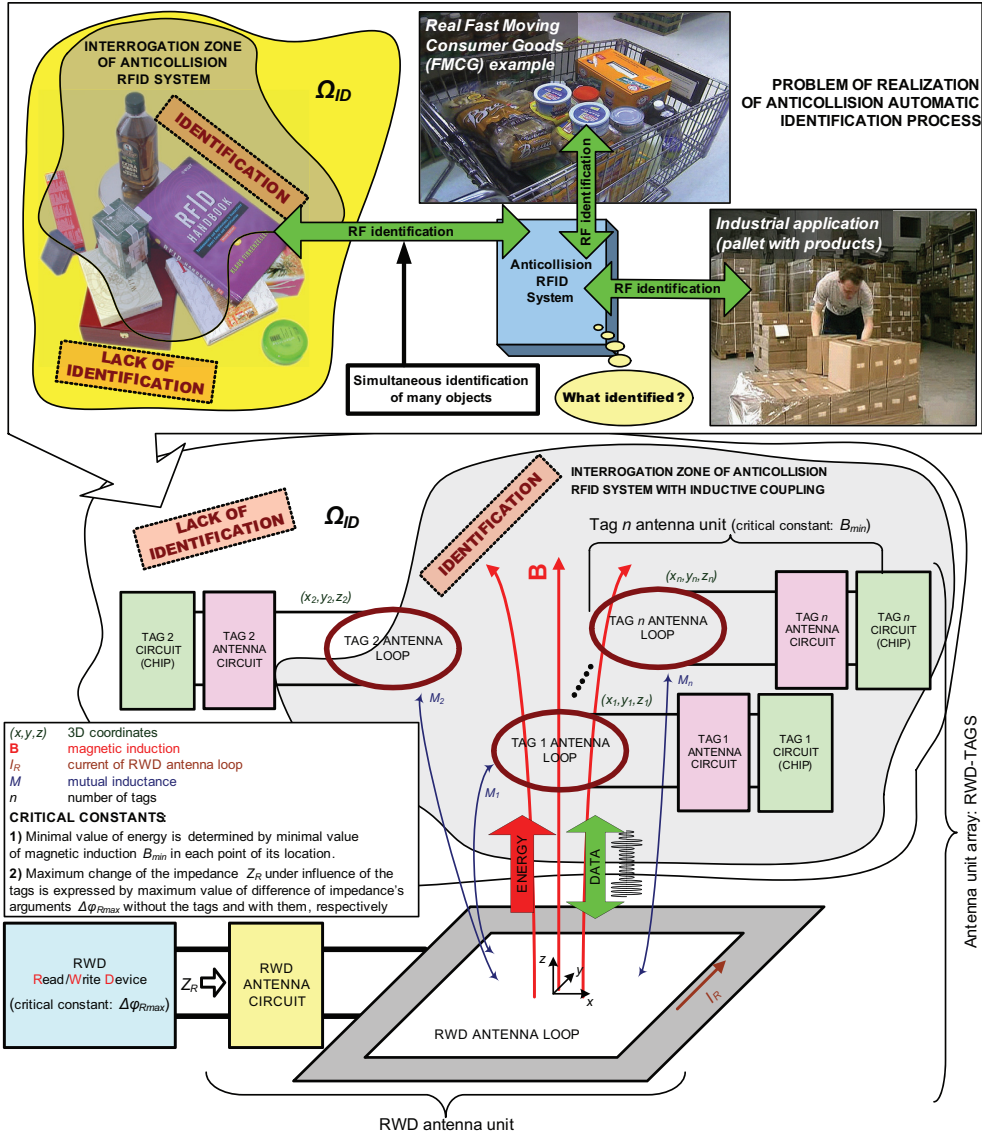
Fig. 1. Block diagram of anticollision RFID system with inductive coupling and illustration of practical automatic RFID process

The B_{min} value, which is considered individually for each transponder in a magnetic field of RWD loop (Ω_{ID} area – Fig. 1), depends on the structure and parameters of this loop but also of tag antenna. In the case of multiple identification process, it is necessary to provide all tags placed within the interrogation zone of RWD antenna with proper power. For this geometric configuration, the parameters of magnetically coupled transponders affect significantly the total loop impedance of RWD antenna and cause big changes in many parameters of its electrical circuit. In consequence, this phenomenon leads to disruption in communication with the tags which are placed within the working area but close to boundary points where the magnetic induction has the minimal value. The correct analysis of the total impedance in coupled system (consisted of RWD and tags antenna loops), and thereby analysis of changes in the magnetic field in the considered interrogation zone, allows to estimate the proper boundary of area with spatial placed multiple tags for the case of designing anticollision RFID system with inductive coupling.

2. The operating range of RFID systems with inductive coupling

In terms of emission of electromagnetic field, the RFID systems are placed in a group of radio equipment devices and they use allocated band in respective frequency range (Fig. 2).
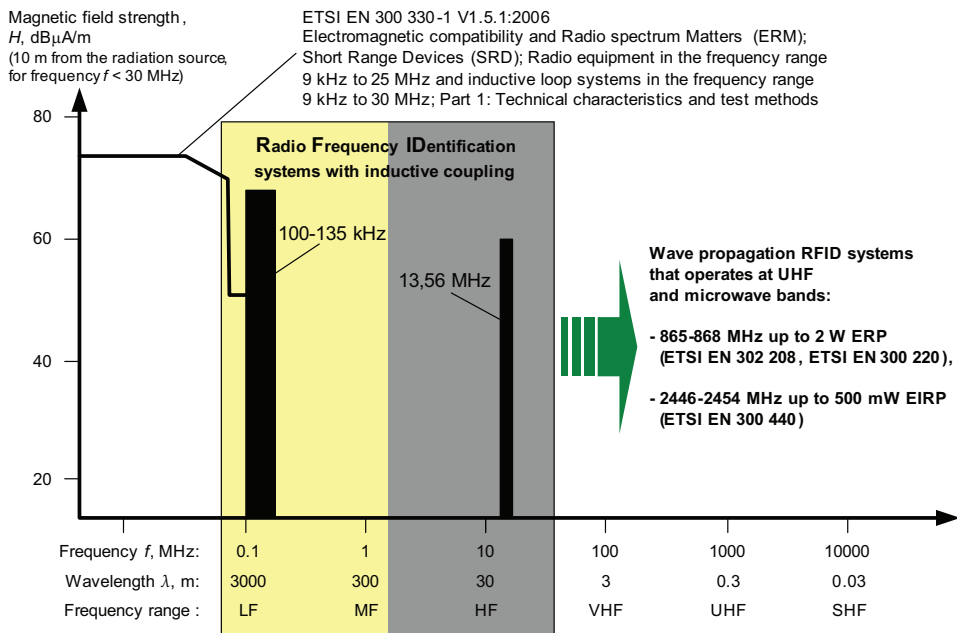
Fig. 2. Frequency ranges and European licensing regulation for RFID systems

Frequency bands widely available for different kind of radio systems (called ISM - Industrial-Scientific-Medical) are used in contact-less identification of objects (ERC, 2008). Therefore, it is required to reduce the magnetic field strength produced by a transmitting antenna of low frequency systems, and reduce the effective radiated power for systems operating in the range of ultra-short waves and microwaves.

Contact-less inductively coupled systems are used to identify objects in the range of the lowest frequencies (in the wave ranges from medium to short). These systems are currently the most widespread, developed and supported by all the key suppliers of RFID components (Yan et al., 2008). They are characterized by working in the area where a strong magnetic coupling between antennas of transmitting components occurs and also where there is strong wave mismatching between communication equipments (Flores et al., 2005). Assuming that the wave propagates in a vacuum, the phase coefficient β takes the real value:

$$\beta = \omega \sqrt{\mu_0 \varepsilon_0} \tag{1}$$

where ω denotes the pulsation, μ_0 – magnetic permeability of vacuum whereas ε_0 means electric permittivity of vacuum.

With respect to the classical theory of antennas, it is possible to specify the working distance of inductively coupled RFID systems according to the following conditions (Fig. 3):

• for an induction zone - near field (all systems with inductive coupling):

$$z << \lambda \tag{2}$$

• for a Fresnel zone (systems operating in the range of short-wave):

$$\beta \cdot z > 1 \tag{3}$$

with signs appearing in the dependencies (2) and (3) described in Fig. 3.

Frequency	100 – 135 kHz	13.56 MHz
Region defined by the antenna theory	Near field (near zone), $z << \lambda$, z – distance from radiation source , λ - wavelength (for 125 kHz – λ = 2400 m)	Fresnel zone , $\beta\, z > 1$, β – phase constant
Region defined for the RFID technology	RFID near field (RFID near zone) functioning range approximately up to a dozen cm; proximity range RFID systems RFID far field (RFID far zone) functioning range up to approximately a few dozen cm (LF) or a few meter (HF); long range RFID systems	
Example applications	Industry, Science, Medicine (ISM) For memory tags in particular : logistics, access control, work time registration, animal identification, etc.	For memory and microchip tags : automatic charging, bank cards, parking cards, etc.

Fig. 3. Operating region of RFID systems with inductive coupling

The average distance between the transmitter and the receiver is from a few centimetres to several meters in the case of RFID systems operating in the range of short-wave. For such a separated working area, the value of the energy flux density transmitted by an

electromagnetic wave (Poynting vector) is zero. This means that the functional principle of RFID systems with inductive coupling is primarily storage of energy in the magnetic field. Examples of working distances, detailed specified ranges and operating limit of two inductively coupled RFID systems are shown in Fig. 4.
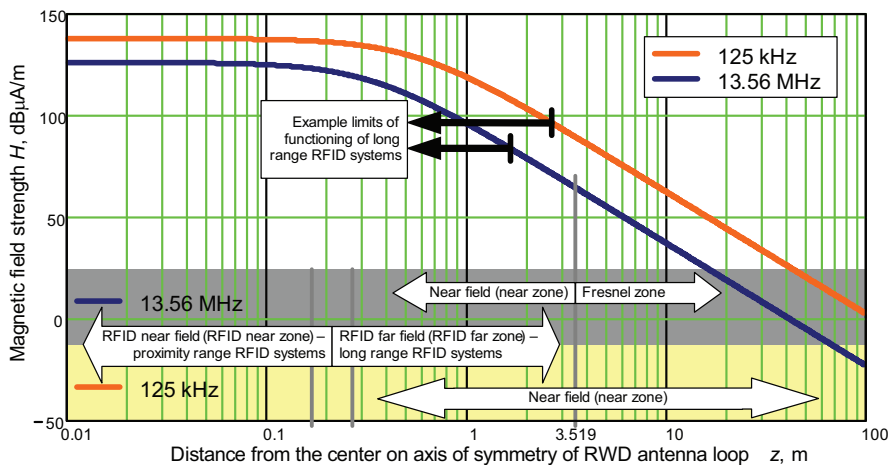
Fig. 4. Magnetic field strength for the transmitting antennas operating at the frequency of 125 kHz and 13.56 MHz with a specification of the working scope according to the classical theory of antennas and for RFID systems with inductive coupling.

With regard to the established characteristic of working distance in RFID systems, the two working scopes are defined. The RFID near field which means the operating distance up to about a dozen centimetres and the RFID far field where the operating range is around from few dozen centimetres to several meters (Bhatt & Glover, 2006; Finkenzeller, 2003; Paret, 2005). It should be noted that these limits, for both the classical theory of antennas as well as RFID systems, are not distances at which rapid changes in transmission parameters occur. Both the changes in properties of the electromagnetic field (zero or nonzero value of the Poynting vector) as well as changes in the efficiency of interaction between communication equipments (which differ in structures depending on a range for RFID near-and far field) have continuous character at estimated boundaries.

3. Restrictions on the magnetic field strength in RFID systems with inductive coupling

The issue of radio system operation is connected with electromagnetic radiation. With regard to the operation correctness and proper construction of RFID system it is necessary to recognise harmful effects of electromagnetic field on the human body and to determine acceptable radiation standards (EN 50364, 2001; EN 50357, 2001; IEC 62369, 2008). In the field of RFID systems with inductive coupling the restrictions of the magnetic field strength are contained in ETSI EN 300 330 standard (ETSI, 2006), which is based on CEPT/ERC Recommendation 70-03 document (ERC, 2008). This document was prepared by the European Telecommunications Standards Institute whose goal is to define standards in the broad area of telecommunications systems.

Class	Device description	Antenna area S	Length of antenna	Description
1	Inductive loop coil transmitter	< 30 m²	< $\lambda/4$ or < 75 m / f where: λ – wavelength f – frequency in MHz	Integrated antenna with a transmitter or directly connected with it
2	Inductive loop coil transmitter	< 30 m²	< $\lambda/4$ or < 75 m / f	Designed antenna with attached instructions
3	Customized large size loop antennas only	> 30 m²	-	-
4	E-field transmitter	-	-	-

Table 1. Description of classes of transmitting device in accordance to ETSI EN 300 330

In the Part 1*: Technical characteristics and test methods of the ETSI EN 300 330: Electromagnetic compatibility and Radio spectrum Matters (ERM); Short Range Devices (SRD); Radio equipment in the frequency range 9 kHz to 25 MHz and inductive loop systems in the frequency range 9 kHz to 30 MHz*, are defined four classes of transmitting devices, which are summarized in Table 1. Due to the fact that all of RFID systems with inductive coupling operating in the frequency range 9 kHz to 30 MHz belong to Class 1 and 2, the restrictions of the magnetic field strength are compared in Table 2 only for those classes of transmitting devices.

Nr.	Frequency f, MHz	Magnetic field strength limits at 10 m H_{10max}, dBμA/m
1	$0.009 \leq f < 0.315$	30
2	$0.009 \leq f < 0.03$	72
3	$0.03 \leq f < 0.05975$ $0.06025 \leq f < 0.07$ $0.119 \leq f < 0.135$	72 at 0,03 MHz descending 3 dB/oct
4	$0.05975 \leq f < 0.06025$ $0.07 \leq f < 0.119$ $0.135 \leq f < 0.140$	42
5	$0.140 \leq f < 0.1485$	37.7
6	$0.1485 \leq f < 30$	-5
	$0.315 \leq f < 0.600$	-5
7	$3.155 \leq f < 3.400$	13,5
8	$7.400 \leq f < 8.800$	9
9	$10.20 \leq f < 11.00$	9
10	$6.765 \leq f < 6.795$ $13.553 \leq f < 13.567$ $26.957 \leq f < 27.283$	42
11	$13.553 \leq f < 13.567$	60

Table 2. Magnetic field strength limits at 10 m from radiation source

The restrictions listed in items 2 and 3 of Table 2 for the frequency bands 9-10 kHz and 119-135 kHz are valid for loop antennas with an area of $S \geq 0.16$ m². If the antenna surface of the transmitting devices is in the range from 0.05 m² to 0.16 m², the limit value of H_{10max} has to be corrected according to the following relationships:

$$H_{10max,cor} = H_{10max} + 10\log\left(\frac{S}{0,16\,m^2}\right) \tag{4}$$

It is necessary to reduce the limit values given in Table 2 by 10 dB for loop antennas with an area of $S <0.05$ m².
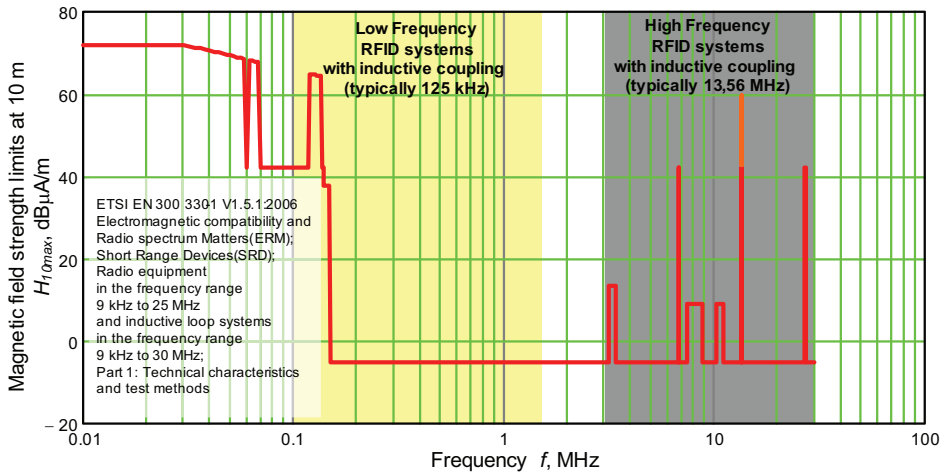
(a)
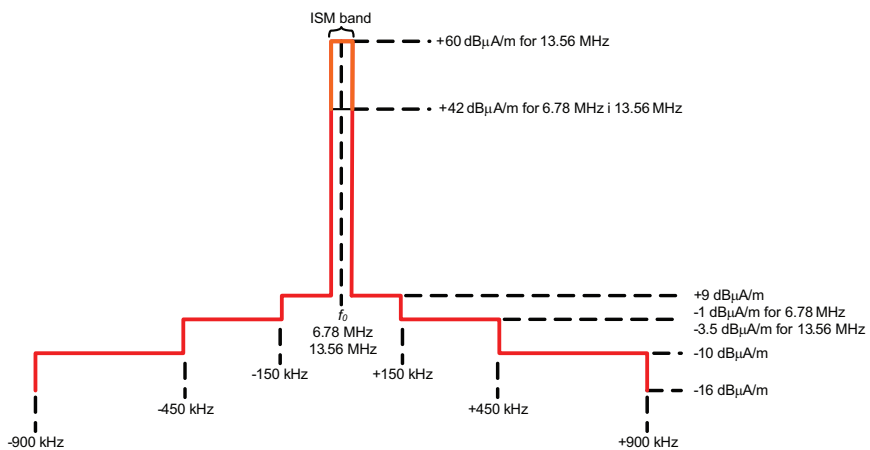
(b)

Fig. 5. Magnetic field strength limits at 10 m from radiation source: a) frequency range 0.01 MHz – 30 MHz, b) spectrum mask limit for frequency: 6.78 MHz and 13.56 MHz

A graphical representation of the magnetic field strength limit specified in Table 2 is shown in the Fig. 5-a. Apparent increase in this curve from 42 dBµA/m to 60 dBµA/m in the range including an operating frequency of 13.56 MHz applies only to systems with inductive coupling, and also to electronic supervision systems called *Electronic Article Surveillance* (EAS). In this case, detailed representation of the magnetic field strength limit reflects a mask which defines the reduction of the limit value H_{10max} in the band ± 900 kHz of working frequency 13.56 MHz (Fig. 5-b).

In most cases, as was already mentioned communication between the transmitter and receiver in inductively coupled RFID systems takes place at a maximum distance of several meters. For this reason, it is useless to define magnetic field strength limit at the distance of 10 m from the radiation source. In order to fulfil the requirements of radiation standards with regard to designing of antenna units the maximum magnetic field strength is determined at a distance of 3 meters from the antenna, according to the relationship:

$$H_{3max} = H_{10max} + C_3 \tag{5}$$

where C3 is a correction factor (expressed in dB) described by a curve which is shown in the Fig. 6.
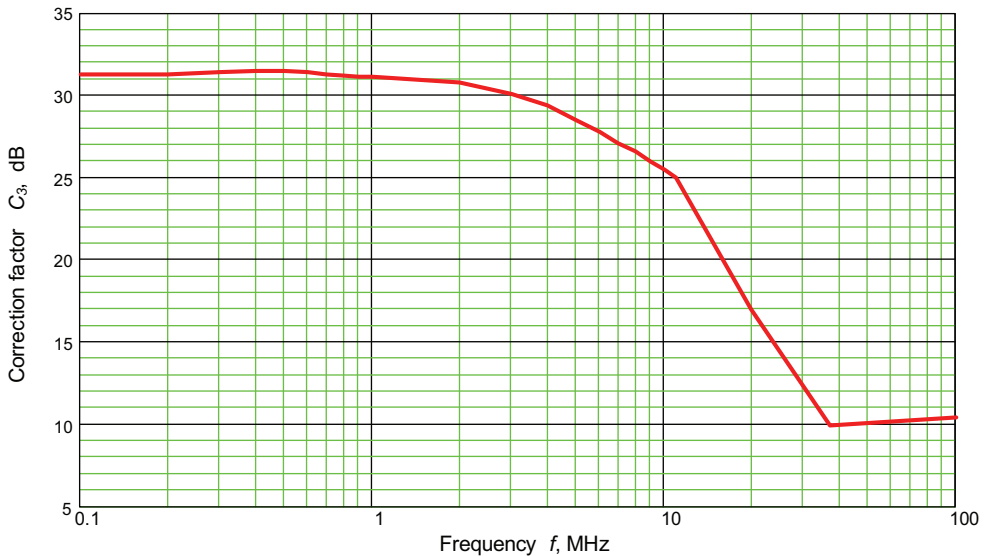
Fig. 6. Correction factor C_3 versus frequency, for limits of magnetic field strength at the distance of 3 m from radiation source

Paying attention to the maximum working distance between elements of the RFID system, in particular for systems working in the RFID far field, it is necessary to estimate the simulated and built antenna set RWD-tags in relation to the obligatory normalizations in communication systems and Electro-Magnetic Compatibility (EMC).

4. Energy transfer in RFID system with inductive coupling

4.1 Magnetic induction value around RWD antenna loop

Analysis of the Read/Write Device (RWD) antenna unit in the area of RFID systems with inductive coupling, permits to make an assumption, that the antenna loop current (I_R) is constant along the whole flow way. This means that the current intensity is constant for any part of the loop which forms an RWD antenna. Fluctuation in the electric charge density equals zero in given period of time, so in that case the divergence of electric current density **J** equals zero as well:

$$\nabla \cdot \mathbf{J} = 0 \tag{6}$$

Making the above mentioned assumptions allows to apply the magnetostatic laws to magnetic field analysis for any shape of RWD antenna loops.
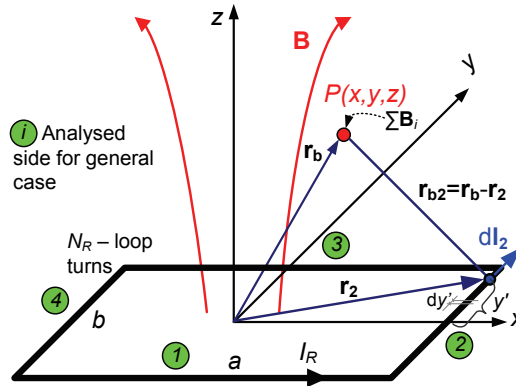
Fig. 7. Analyzed case of polygon shape of RWD antenna loop

In the case of RWD antenna loop constructed as polygon (Fig. 7), Biot-Savart law with superposition theorem (Halliday et al., 2004) permits to sum vectors of magnetic induction **B** that descend from individual antenna parts at location $P(x,y,z)$. In this case the total magnetic induction is calculated from equation:

$$\mathbf{B} = \sum_i \mathbf{B}_i \tag{7}$$

where i denotes analysed side for RWD antenna loop constructed as polygon.
The vectors $\mathbf{r}_{bi}$ describing the $d\mathbf{l}_i$ (for i=1, 2, 3, 4) location at P point, in which the value of magnetic induction is calculated, are given by formulas:

$$\mathbf{r}_{b1} = \mathbf{r}_b - \mathbf{r}_1 , \tag{8}$$

$$\mathbf{r}_{b2} = \mathbf{r}_b - \mathbf{r}_2 , \tag{9}$$

$$\mathbf{r}_{b3} = \mathbf{r}_b - \mathbf{r}_3 , \tag{10}$$

$$\mathbf{r}_{b4} = \mathbf{r}_b - \mathbf{r}_4 \tag{11}$$

where the vectors describing $d\mathbf{l}_i$ elements location, and the vector $\mathbf{r}_b$ describing location of point P, are given as follows:

$$\mathbf{r}_1 = \begin{pmatrix} x' \\ -b/2 \\ 0 \end{pmatrix}, \tag{12}$$

$$\mathbf{r}_2 = \begin{pmatrix} a/2 \\ y' \\ 0 \end{pmatrix} \tag{13}$$

$$\mathbf{r}_3 = \begin{pmatrix} x' \\ b/2 \\ 0 \end{pmatrix}, \tag{14}$$

$$\mathbf{r}_4 = \begin{pmatrix} -a/2 \\ y' \\ 0 \end{pmatrix}, \tag{15}$$

$$\mathbf{r}_b = \begin{pmatrix} x \\ y \\ z \end{pmatrix} \tag{16}$$

The unit vectors $\mathbf{u}_1$-$\mathbf{u}_4$ connected with $d\mathbf{l}_{1,3} = \mathbf{u}_{1,3} \cdot dx'$ and $d\mathbf{l}_{2,4} = \mathbf{u}_{2,4} \cdot dy'$ are given by formulas:

$$\mathbf{u}_1 = \mathbf{u}_3 = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \tag{17}$$

$$\mathbf{u}_2 = \mathbf{u}_4 = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \tag{18}$$

After the $\mathbf{B}_i$ calculated for analysed side of RWD antenna loop, on the basis of (7), the magnetic vector at any space location with (x,y,z) coordinates is given as follows:

$$\mathbf{B} = \frac{\mu_0 I_R N_R}{4\pi} \left[\int_{\frac{-a}{2}}^{\frac{a}{2}} \frac{\mathbf{u}_1 \times \mathbf{r}_{b1}}{|\mathbf{r}_{b1}|^3} dx' + \int_{\frac{-b}{2}}^{\frac{b}{2}} \frac{\mathbf{u}_2 \times \mathbf{r}_{b2}}{|\mathbf{r}_{b2}|^3} dy' + \int_{\frac{a}{2}}^{\frac{-a}{2}} \frac{\mathbf{u}_3 \times \mathbf{r}_{b3}}{|\mathbf{r}_{b3}|^3} dx' + \int_{\frac{b}{2}}^{\frac{-b}{2}} \frac{\mathbf{u}_4 \times \mathbf{r}_{b4}}{|\mathbf{r}_{b4}|^3} dy' \right] \tag{19}$$

where: $\mu_0 = 4 \cdot \pi \cdot 10^{-7}$ H/m.

The components of magnetic induction B in any space point $P(x,y,z)$ are given for polygon shape of RWD antenna loop by equations:

$$B_x = \frac{\mu_0 I_R N_R}{4\pi} \left[\int_{\frac{-b}{2}}^{\frac{b}{2}} \frac{z}{\left[\left(x - \frac{1}{2}a\right)^2 + (y - y')^2 + z^2\right]^{3/2}} dy' + \int_{\frac{b}{2}}^{\frac{-b}{2}} \frac{z}{\left[\left(x + \frac{1}{2}a\right)^2 + (y - y')^2 + z^2\right]^{3/2}} dy' \right] \quad (20)$$

$$B_y = \frac{\mu_0 I_R N_R}{4\pi} \left[\int_{\frac{-a}{2}}^{\frac{a}{2}} \frac{-z}{\left[(x - x')^2 + \left(y + \frac{1}{2}b\right)^2 + z^2\right]^{3/2}} dx' + \int_{\frac{a}{2}}^{\frac{-a}{2}} \frac{-z}{\left[(x - x')^2 + \left(y - \frac{1}{2}b\right)^2 + z^2\right]^{3/2}} dx' \right] \quad (21)$$

$$B_z = \frac{\mu_0 I_R N_R}{4\pi} \cdot \left[\int_{\frac{-a}{2}}^{\frac{a}{2}} \frac{y + \frac{1}{2}b}{\left[(x - x')^2 + \left(y + \frac{1}{2}b\right)^2 + z^2\right]^{3/2}} dx' + \int_{\frac{-b}{2}}^{\frac{b}{2}} \frac{-x + \frac{1}{2}a}{\left[\left(x - \frac{1}{2}a\right)^2 + (y - y')^2 + z^2\right]^{3/2}} dy' + \right.$$

$$\left. + \int_{\frac{a}{2}}^{\frac{-a}{2}} \frac{y - \frac{1}{2}b}{\left[(x - x')^2 + \left(y - \frac{1}{2}b\right)^2 + z^2\right]^{3/2}} dx' + \int_{\frac{b}{2}}^{\frac{-b}{2}} \frac{-x - \frac{1}{2}a}{\left[\left(x + \frac{1}{2}a\right)^2 + (y - y')^2 + z^2\right]^{3/2}} dy' \right] \quad (22)$$

The obtained equations (20)-(22) permit numerical calculation of magnetic induction value separately for individual components in directions x, y and z (B_x, B_y, B_z). These equations enable to evaluate direction and sense of magnetic induction vector. The example of MathCad 14 calculation for polygon shape of RWD antenna loop, which parameters are given by: a=0.3 m, I_R=0.2 A, has been presented in Fig. 8.

The variable value of z component of magnetic induction (B_z) (which has been presented as an example) reveals the problem of the correct localization of the tag in the space what is necessary in order to fulfill the condition of minimum value of induction (B_{min}). In turn, the alternating direction of the normalized magnetic induction vector (B_{norm}) indicates the problem of correct orientation for tag in relation to individual components of this vector. For example, the correction of tag orientation can occur in order to ensure its maximum distance from the RWD antenna. It can also be forced by the characteristic of the objects that are identified, namely it means the need to locate a tag on the labeled object in a special way (e.g. in bevel boxes placed on a pallet exposed to a process of anticollision identification). In many cases, the anticipated specification of tags localization in practical applications (for transponders working first of all in anticollision but also in single RFID systems) indicates the necessity of considering induction component in the direction of z axis. However, for correct estimation of the performance efficiency for the real RFID system in the field conditions area it is required to determine the tag orientation influence on the correct identification (Jankowski-M. et al., 2008).
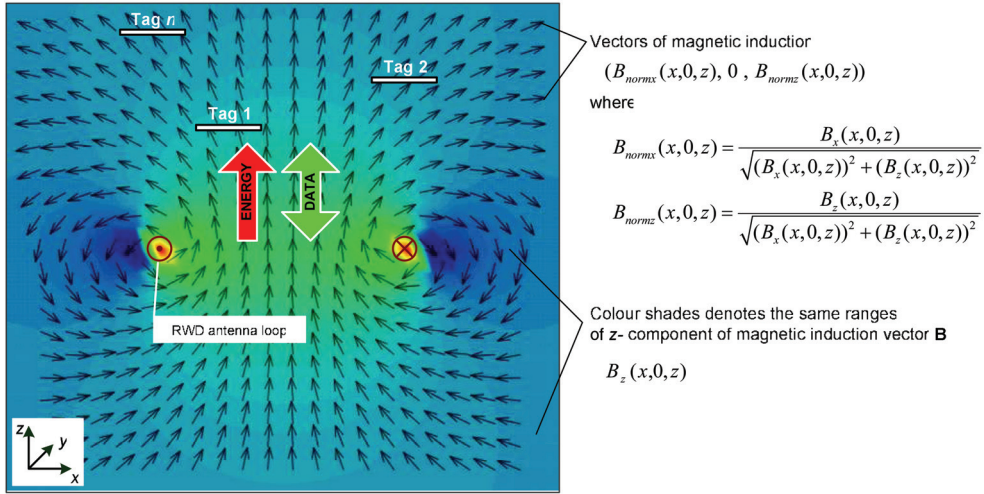
Fig. 8. Magnetic induction in *x*-z plane and tags localization in magnetic field of RWD antenna loop

4.2 Tag orientation in magnetic field of RWD antenna loop

A lot of practical solutions of identification are characterized by parallel location of tag antenna and RWD loop. This location of individual tags allows the magnetic induction B_{min} to reach its minimum value only in relation to *z*-magnetic induction components. This case applies to places, in which tags working in anticollision process has been located ($P_1(x_1,y_1,z_1) \div P_n(x_n,y_n,z_n)$ – Fig. 1). Presented approach creates a lot of limits connected with decrease of the interrogation zone in RFID system. This results from too low value of the **perpendicular magnetic induction component** in relation to tag antenna loop plane.

The efficient use of communication space, in which anticollision process is going to be done, and also specification of the object marked by passive RFID tag, requires consideration of any tag orientation with regard to the individual components of magnetic induction vector (Fig. 9).

The issue of any tag orientation in three dimensions *x-y-z* comes down to tag deviation by α and β angles from parallel location of RWD-tag antenna loops (Fig. 9-a). In accordance with presented model (Fig. 9-b and Fig. 9-c), deviation by α angle occurs in *z-x* plane, however deviation by β angle occurs in α-*y* plane. The value calculation of perpendicular magnetic induction component for tag, which is deviated by α and β angles ($B_{\alpha\beta}$), has been divided in two parts. In the first part, by using superposition theorem, after deviating tag by α angle, the perpendicular magnetic induction component is given by:

$$B_{xz\alpha} = B_{x\alpha} + B_{z\alpha} \tag{23}$$

where the values of vector components are given by:

$$B_{x\alpha} = B_x \cdot \sin(\alpha), \tag{24}$$

$$B_{z\alpha} = B_z \cdot \cos(\alpha) \tag{25}$$
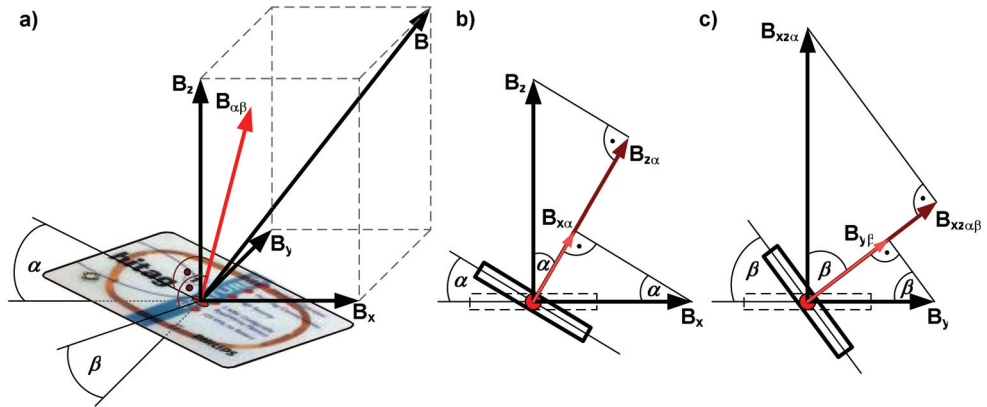
Fig. 9. Orientation of tag, which is deviated by α and β angles from components of magnetic induction vector: a) deviation in 3D coordinate *x-y-z*; b) deviation by α angle in *z-x* plane; c) deviation by β angle in *α-y* plane

Next, in second part, by using of the superposition theorem, after deviating tag by β angle, the perpendicular magnetic induction component is given as follows:

$$B_{\alpha\beta} = B_{y\beta} + B_{xz\alpha\beta} \tag{26}$$

where the values of vector components are given by:

$$B_{y\beta} = B_y \cdot \sin(\beta) \, , \tag{27}$$

$$B_{xz\alpha\beta} = B_{xz\alpha} \cdot \cos(\beta) \tag{28}$$

It comes from the equations (23)-(28) that the perpendicular magnetic induction component for passive tag which is deviated by α and β angles is given by:

$$B_{\alpha\beta} = B_z \cdot \cos(\alpha) \cdot \cos(\beta) + B_x \cdot \sin(\alpha) \cdot \cos(\beta) + B_y \cdot \sin(\beta) \tag{29}$$

Knowing the magnetic induction separately for individual components in directions *x*, *y* and *z* (B_x, B_y, B_z), the obtained equation (29) permits calculation of the perpendicular magnetic induction component. The aforementioned necessity of changing tag orientation should be carried out for assurance of correct tag work in the individual space point *P(x,y,z)*. In this way, there is possible to calculate the system interrogation zone which is forced by specification of identified object what results from the necessity of individual tag location on marked object.

Changes of the interrogation zone for single tag with minimal value of magnetic induction have been presented as examples in Fig. 10-c, d (calculated results) and Fig. 10-b (measured results). The black colour represents **no communication area** between tag and RWD. The area results from no fulfil condition of minimal magnetic induction (B_{min}) for the tag and its location in relation to perpendicular magnetic induction component.

Above mentioned parallel location of tag and RWD antenna loops causes appearance of symmetrical interrogation zone and lack of communication area in relation to symmetry axis

of RWD antenna (Fig. 10-c). The both areas on *x-y* plane have been presented in upper part of diagram. Any changes in tag orientation by α and β angles (Fig. 10-b, d) lead to modifications in the interrogation zone. For the given tag and its hypothetical orientation, the communication area has been significantly shifted in direction of tag deviation, while no communication areas between tag and RWD has appeared in the central part of *x-y* plane.

The axial symmetry of interrogation zone and no-communication zone disappears in case of tag deviation by α and β angles. Such state complicates forecast and unambiguous description of the tag location, which permits its correct work.
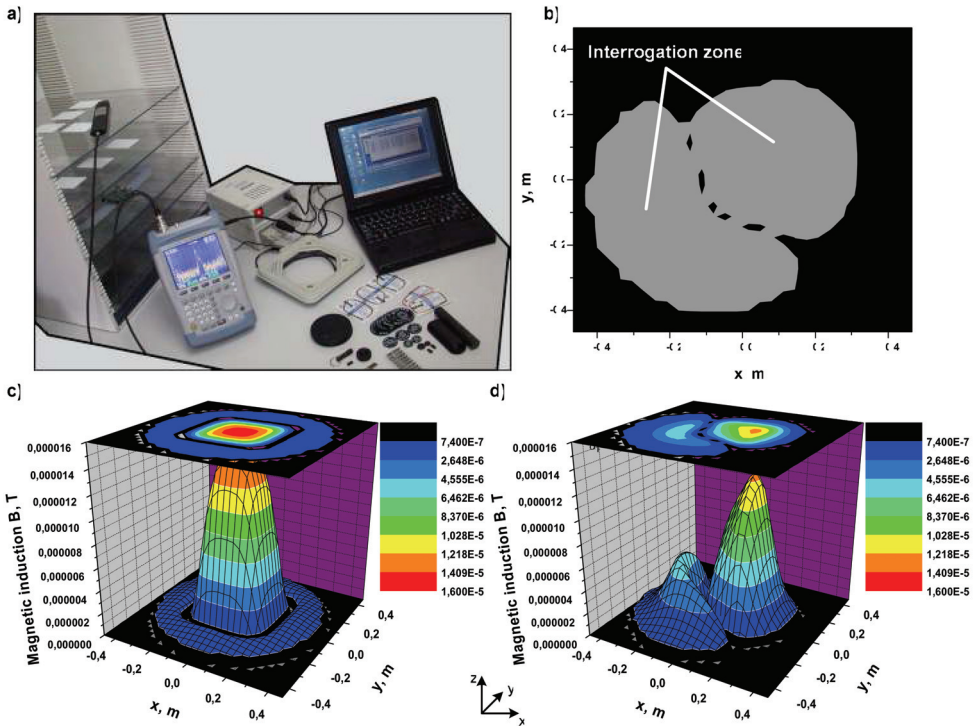
Fig. 10. Perpendicular magnetic induction component for HITAG 1 ISO CARD (B_{min}=740 nT) placed in 0.1m distance from square RWD antenna (*a* side = 0.3 m):
a) laboratory system, b) measured interrogation zone for deviated tag by α, β=45°,
c) calculated result - α, β=0°; d) calculated result - deviated tag by α, β=45°

In case of required passive tag deviation from symmetry axis of antenna loops, the value of perpendicular magnetic induction component should be always corrected according to the equation (29), which takes into consideration tag deviation by α and β angles. During the analysis of field conditions, the effect of RWD antenna shape on communication should be considered additionally. Calculation of the above parameters for given single and anticollision 3D identification system gives the basis to determine the interrogation zone of passive RFID systems.

4.3 Structural conditions of RWD antenna loop

In the literature on the subject, the magnetic induction relationship for circular conductor with current is often applied (Cichos, 2002; Microchip, 2004). A situation, when tag antenna loop is placed on axis of symmetry with RWD antenna loop, is the characteristic case of radio frequency identification system functioning. The estimation of circle radius on the basis of the real RWD loop area which is a polygon can lead to errors during the calculation of maximum working distance for RFID system. The shape of RWD antenna influences on location of magnetic lines in 3D space, therefore the relationships for different shape of read/write device antenna loop have been presented in Table 3. They are derived from the Biot-Savart law in accordance with the described method, which permits to analyze any shape of RWD antenna loop required by system designer (Jankowski-M. & Kalita, 2004).
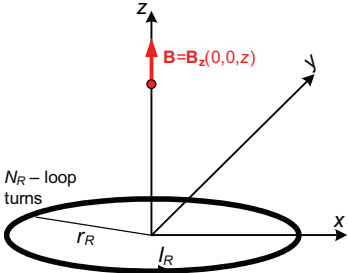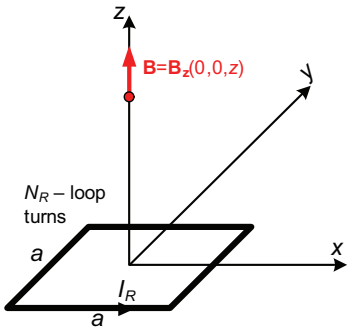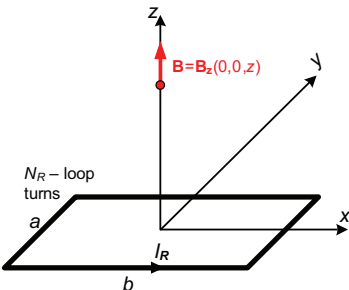
Nr.	RWD antenna shape	Magnetic induction B in distance z from the center on axis of symmetry of RWD antenna loop
1		$$B = \frac{\mu_0 I_R N_R r_R^2}{2\left(z^2 + r_R^2\right)^{3/2}}$$
2		$$B = \frac{4\mu_0 I_R N_R a^2}{\pi\left(4z^2 + a^2\right)\left(4z^2 + 2a^2\right)^{1/2}}$$
3		$$B = \frac{2\mu_0 I_R N_R}{\pi}\left[\frac{a^2}{\left(4z^2 + a^2\right)\left(4z^2 + 2a^2\right)^{1/2}} + \frac{b^2}{\left(4z^2 + b^2\right)\left(4z^2 + 2b^2\right)^{1/2}}\right]$$

Table 3. Magnetic induction value for different shape of RWD antenna loop

For the sake of the fact that the shape of RWD loop determines the magnetic field, there has been presented below the method of calculating the magnetic induction B created on the square coil consisted of N_R loop turns, each through the current I_R is flowing. Considerations concern z axis, because RFID systems are projected in such way, that the tag antenna loop is situated on one of axis of symmetry with RWD loop.

In accordance with Biot-Savart law, the d$\mathbf{B}$ value is given by equation:

$$d\mathbf{B} = \frac{\mu_0 I_R N_R}{4\pi} \cdot \frac{d\mathbf{l}\sin(\theta)}{r^2} \tag{30}$$
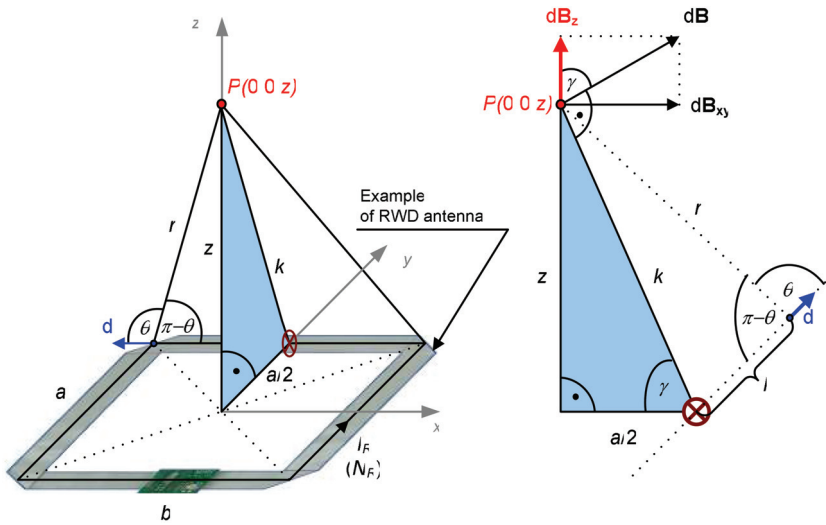
Fig. 11. Analyzed case of polygon shape of RWD antenna loop

Spreading d$\mathbf{B}$ on two components: d$\mathbf{B_{xy}}$ - perpendicular to z axis and d$\mathbf{B_z}$ - parallel to z axis, there can be noticed, that at location $P(0,0,z)$ only the d$\mathbf{B_z}$ has an influence on magnetic induction $\mathbf{B}$ vector. Such state result from the fact, that the sum of d$\mathbf{B_{xy}}$ components, with reference to whole current currying conductor - equals 0 for the sake of symmetry. In that case:

$$\mathbf{B} = \int d\mathbf{B_z} \tag{31}$$

where:

$$d\mathbf{B_z} = d\mathbf{B}\cos(\gamma) \tag{32}$$

Defining the geometrical relationships between the individual angles and sides at location P, placed in x distance, they can be rewritten:

$$\sin(\theta) = \sin(\pi - \theta) = \frac{k}{r}, \tag{33}$$

$$r = \sqrt{k^2 + l^2} \, , \tag{34}$$

$$k = \sqrt{z^2 + \left(\frac{a}{2}\right)^2} \, , \tag{35}$$

$$\cos(\gamma) = \frac{a}{2k} \tag{36}$$

Substituting suitably (30) and (33)-(36) to (32) equation, and then whole to (31) equation, there can be received:

$$B = \int dB_z = \int dB \cdot \cos(\gamma) = 2 \cdot \frac{\mu_0 I_R N_R}{4\pi} \left[\int_{-\frac{a}{2}}^{+\frac{a}{2}} \frac{\frac{a}{2}}{\left(z^2 + \left(\frac{a}{2}\right)^2 + l^2\right)^{3/2}} \, dl + \int_{-\frac{b}{2}}^{+\frac{b}{2}} \frac{\frac{b}{2}}{\left(z^2 + \left(\frac{b}{2}\right)^2 + l^2\right)^{3/2}} \, dl \right] \tag{37}$$

In result of the (37) integration, the (38) equation can be obtained. It allows to estimate the value of magnetic induction B in distance z from the centre on symmetry axis of square RWD antenna loop:

$$B = \frac{2\mu_0 I_R N_R}{\pi} \left[\frac{a^2}{\left(4z^2 + a^2\right)\left(4z^2 + 2a^2\right)^{1/2}} + \frac{b^2}{\left(4z^2 + b^2\right)\left(4z^2 + 2b^2\right)^{1/2}} \right] \tag{38}$$

In the Fig.12, there are presented the curves $B=f(z)$ for the RWD antenna loops with equal areas but different shapes: (1) - circular, (2) - square and (3, 4, 5, 6) - rectangle, where the ratio of the sides a/b is given as follows: 0.028, 0.111, 0.25, 0.44. The line B_{min} (for analyzed tag) intersects the curve of value of the magnetic induction for analyzed shape of RWD antenna loop, what leads to evaluation of the maximum working distance z_{max} of RFID system.

The equation number 1 from table 3 is valid only for a case of circular and square shape of RWD antenna loop. In the case of rectangle RWD antenna (or a loop which is constructed as other polygon) where a/b < 1, there is irregularity in calculation of the maximum working distance of RFID system (Fig. 12). If the coefficient a/b << 1 or when RWD antenna is constructed as a complicated polygon, the error may be significant and as a consequence may lead to wrong result in estimation process of interrogation zone which was assumed at first. The interrogation zone of RFID system for two extreme cases from Fig. 12 has been presented in Fig. 13.

Depending on required uses (the identification of animals, access control or objects identification in logistics), the process of calculating the maximum working distance should take into consideration the fallowing aspects: the real shape of RWD antenna, three-dimensional location of tag, its orientation and kind of executed operation - writing or reading data from internal tag memory (Jankowski-M. & Kalita, 2004).
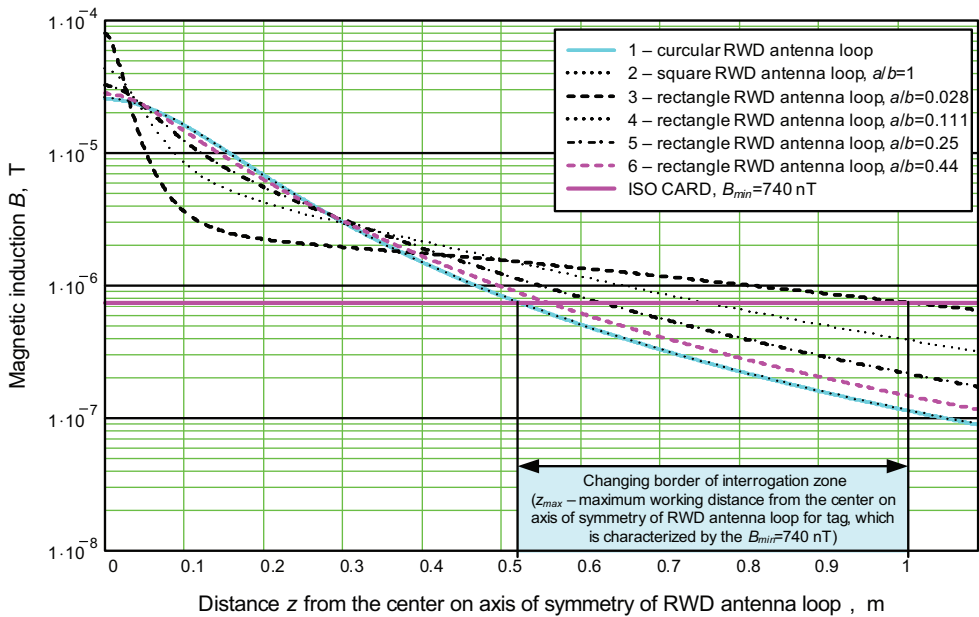
Fig. 12. Curves of value of the magnetic induction in function of distance z from the center on axis of symmetry of RWD antenna loop with equal areas

(a)   (b)
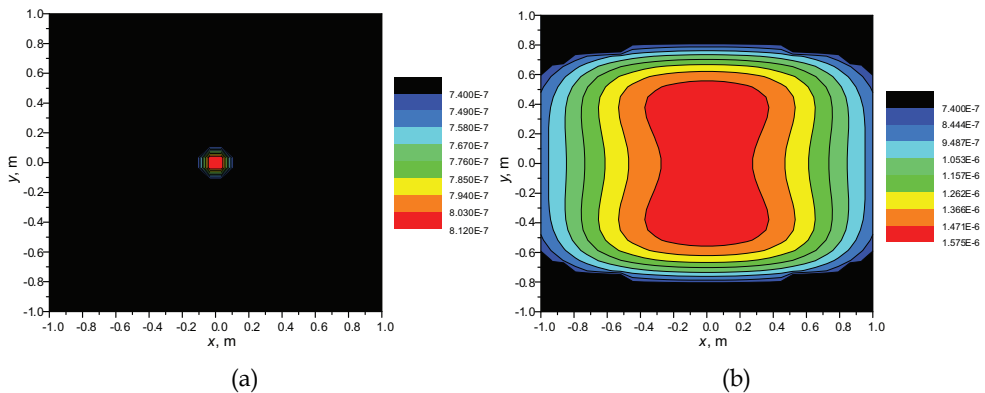
Fig. 13. Perpendicular magnetic induction component for tag (B_{min}=740 nT), which is located at distance 0,5 m from the centre on axis of symmetry of RWD antenna surfaces with equal areas: a) circular loop, b) rectangle loop - a/b=0.028

4.4 Conditions of identification conducted nearby objects which disturb data transfer

Prior considerations of the energy transmission through the magnetic field generated within the RWD antenna have related to the no disturbed environment that is characterized only by a magnetic permeability of free space μ_0 (relative magnetic permeability of air -

μ_r=1.00000036 - is assumed with value equal 1). However, sometimes it is necessary to take into consideration the impact of objects placed into a magnetic field of RWD antenna on changes in the magnetic induction vector at the point of identifiers location. The need for carrying out an identification process of ferromagnetic objects or these which are located near to ferromagnetic materials can be given as an example (Fig. 14-a).
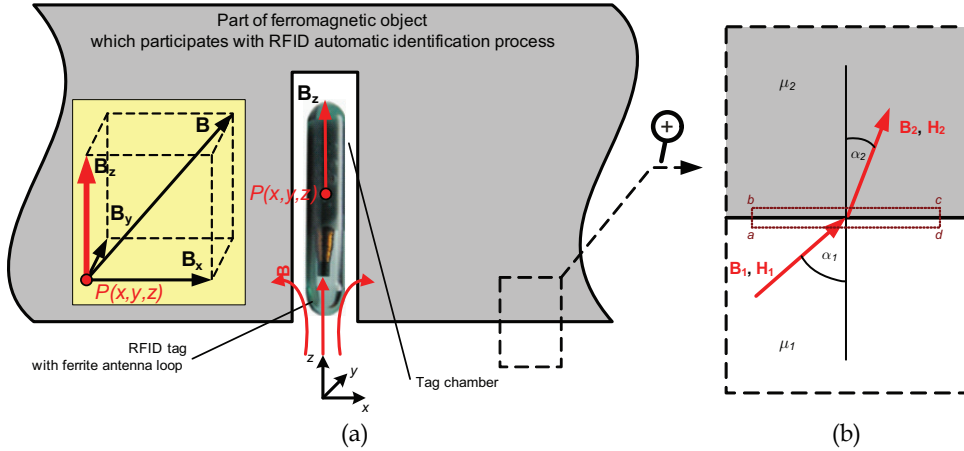
Fig. 14. Identification of the object distorting a data transmission: a) orientation of tag attached to ferromagnetic elements with reference to the RWD antenna loop, b) the magnetic field at the boundary of environments

A knowledge about strongly influenced (with respect to the system without ferromagnetic materials) direction and sense of the magnetic induction vector in the area in which there are ferromagnetic objects allows the correct analysis of a transponder orientation in the magnetic field of RWD antenna loop (see 4.2). It also gives reason for a proper determination of the tag interrogation zone and thus to fulfil the field conditions of specific work environment.

If the rectangular contour *abcd* (Fig. 14-b) will be assumed on the boundary of the ferromagnetic object then the fallowing equation is fulfilled in the open circuit for the vector of magnetic field strength **H**:

$$\oint_l \mathbf{H} \cdot d\mathbf{l} = 0 \tag{39}$$

Assuming that the lengths of sides (rectangle with perimeter *l*) *ab* and *cd* are negligibly small in relation to *bc* and *da*, from equation (39) follows the equality:

$$H_1 \sin \alpha_1 = H_2 \sin \alpha_2 \tag{40}$$

On the other hand, for the area where there is no current flow and the equation of the vector magnetic induction **B** is satisfied:

$$\oint_S \mathbf{B} \cdot d\mathbf{S} = 0 \tag{41}$$

and assuming that there is negligible small surface S of rectangle located in *abcd* contour, perpendicular to the surface of figure 14-b, it is possible to write:

$$B_1 \cos\alpha_1 = B_2 \cos\alpha_2 \tag{42}$$

It follows from equation (40) that there is continuity of tangential component of the vector **H** at the environment boundary, while from equation (42) - continuity of normal component of vector **B**. On the base of the fallowing equation of material:

$$\mathbf{B} = \mu\mathbf{H} \tag{43}$$

boundary conditions (40) and (42) can be presented in the form of the vector refraction law for the magnetic field:

$$\frac{\mu_1}{\mu_2} = \frac{tg\alpha_1}{tg\alpha_2} \tag{44}$$

Equation (44) is true with assumption that the identification system from the Fig. 14-a is placed in the *z-x* plane, that is there is not its shift in the *y*-axis direction. In the identification process carried out nearby objects disturbing the magnetic field of RWD antenna loop it is better to use the magnetic vector potential **A** when determining induction **B** in the tag placement area. The dependences (40) and (42) show that there is continuity of vector potential at the boundary in the Fig. 14 where the equation is satisfied:

$$\mathbf{B} = \nabla \times \mathbf{A} \tag{45}$$

After using equations (43), (45) and the expression describing the area of tag placement without current flow, $\nabla \times \mathbf{H} = 0$, the relationship was obtained:

$$\Delta\mathbf{A} = 0 \tag{46}$$

Relationship (46) is the vector Laplace equation which describes the distribution of vector potential in the placement area of tag. So the problem of the correct location for the tag placed nearby ferromagnetic objects is reduced to such a boundary problem which has to be solved. Moreover, in order to meet field condition requirements, it is necessary to find out such an tag orientation in the magnetic field of RWD antenna loop (see 4.2) at which the condition of minimum magnetic induction value is fulfilled for the given tag. This implies the need for determining the perpendicular component of magnetic induction vector at the location point of tag which will be used to mark the object.

In the most general case, the lack of symmetry indicates the need to solve the system of three Laplace equations formulated for each of the Cartesian coordinates *x, y* and *z*:

$$\Delta\mathbf{A} = \begin{vmatrix} \dfrac{\partial^2 A_x}{\partial x^2} + \dfrac{\partial^2 A_x}{\partial y^2} + \dfrac{\partial^2 A_x}{\partial z^2} \\[2mm] \dfrac{\partial^2 A_y}{\partial x^2} + \dfrac{\partial^2 A_y}{\partial y^2} + \dfrac{\partial^2 A_y}{\partial z^2} \\[2mm] \dfrac{\partial^2 A_z}{\partial x^2} + \dfrac{\partial^2 A_z}{\partial y^2} + \dfrac{\partial^2 A_z}{\partial z^2} \end{vmatrix} = 0 \tag{47}$$

Analytical methods for solving these issues (e.g. separation of variables method) often can not be used because of complicated shapes of ferromagnetic objects which sometimes affect the identification process very strong. Then, it is necessary to use numerical methods and specialized software that allows to define the problem, enter boundary conditions and obtain convergent results in quick way.
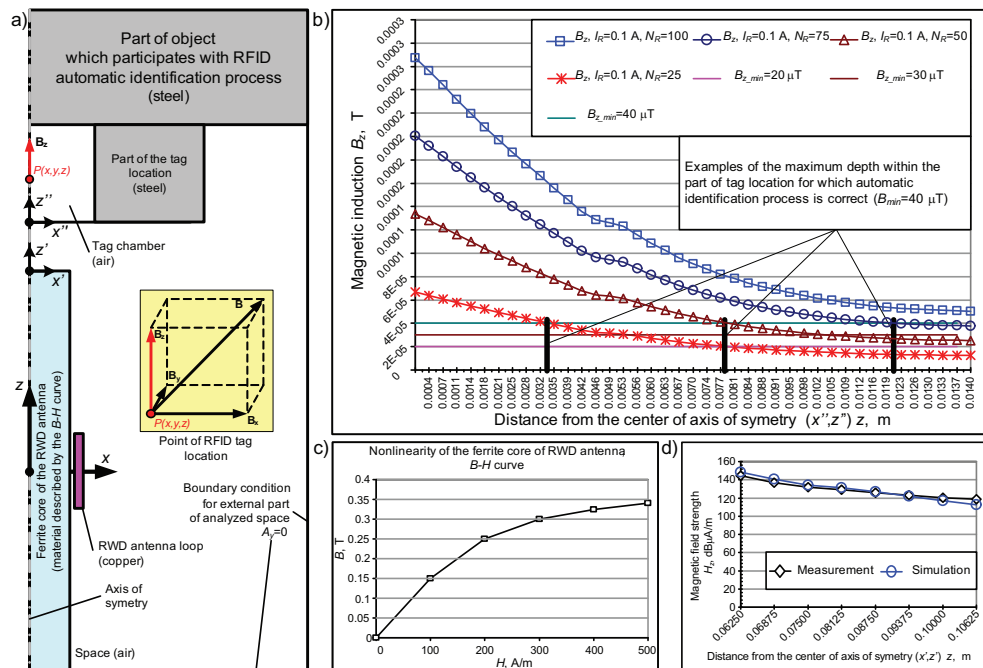
Fig. 15. FEM model for an example of RFID identification of ferromagnetic object:
a) axially symmetric model, b) calculation results from ANSYS software – component B_y inside a mounting element chamber, c) the curve **B-H** for the ferrite core of RWD antenna, d) experimental verification of model

An example of RFID identification process for ferromagnetic object is shown in the Fig. 15. It is necessity to use a directional antenna in order to read information from tag working in this system. The antenna has to stably operate at resonant frequency of RFID system. Placing the antenna close to the ferromagnetic object determines the need of the maximum distance between the RWD loop and the object and using small antennas. It makes impedance component contributed by the object to the electrical circuit of RWD antenna loop lees significant. Barriers to the operation of antenna units in the field of electrical conditions were presented in (Jankowski-M. & Kalita, 2008 and 2009).

Using a small loop, which is about a few centimetres from the identified object, does not allow for stable operation of the RWD antenna unit. It is also impossible to meet the requirement for the minimum value of magnetic induction for one or more tags. For this reason, it is necessary to use an antenna with a ferrite rod, which forms the magnetic

amplifier (magnetic core). Adoption of the previous assumptions according to the RWD antenna operation (4.1) makes possible to develop a simulation model with using the finite element method. The model has been analyzed in the magneto-static field (Fig. 15-a).
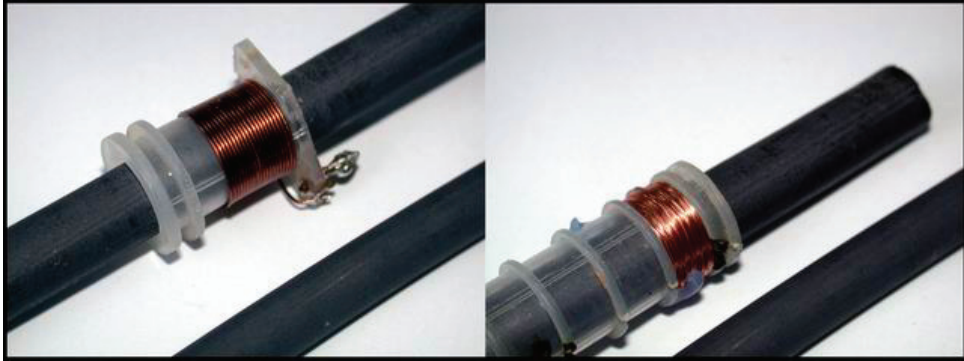
Fig. 16. Measuring samples of ferrite RWD antenna

The FEM model that was built for the ANSYS software (Fig. 15-c,d) was verified by simulating and measuring the H_z component of magnetic field strength for the tested antenna (Fig. 16). The antenna was made by winding 100 turns of wire with a diameter of 0.3 mm round the ferrite cores with a length of 0.125 m, diameter of 0.005 m and initial permeability of 20. Highlighted the discrepancy between simulation results and measurements was at the level of 3-4 %, in the worst case. It is due to conducting simulation process of magnetic field in a long air gap occurring between the metal elements.

The results (Fig. 15-b) clearly show the maximum value of depth within the mounting element of identifier. The value determines the range of depth where the tag with precisely fixed minimum value of magnetic induction should be placed. Ferromagnetic cylinder with a drilled hole constituted attachment part of the transponder.

Same of the magnetic induction flux and vector observations in the tag placement area (Fig. 17-a,b) show the possibility of finding the correct set of system components for the purpose of carrying out the identification process. It is possible with proper placing RWD antenna or by re-orientating the antenna loop.

Developed FEM simulation model is widely discussed in publications (Jankowski-M., 2007). It can provide a basis for synthesis of solutions in RFID identification systems modified in its construction. In particular it is useful in industrial logistics systems, presented in Fig. 18 and in publication (Fitowski et al., 2005) as an examples. In the first case (Fig. 18-a), a method of passive RFID tag affixing on the flange of technical gas cylinders is presented. The method was developed in Department of Electronic and Communication Systems of Rzeszów University of Technology within the confines of a whole computer system for RFID identification of gas cylinders. The presented method has been also used practically in an innovative and unique design of the RFID system for collection of mining equipment in underground environment - Fig. 18-b. Powered roof support units pose difficult objects in identification process due to the metal construction and adverse operating conditions such as vibration, stress, corrosive environment, very high humidity and dust.
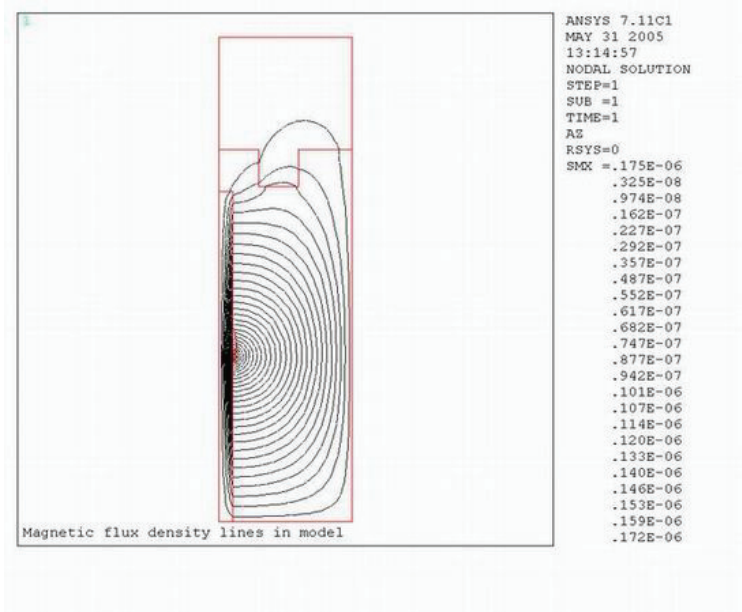
(a)
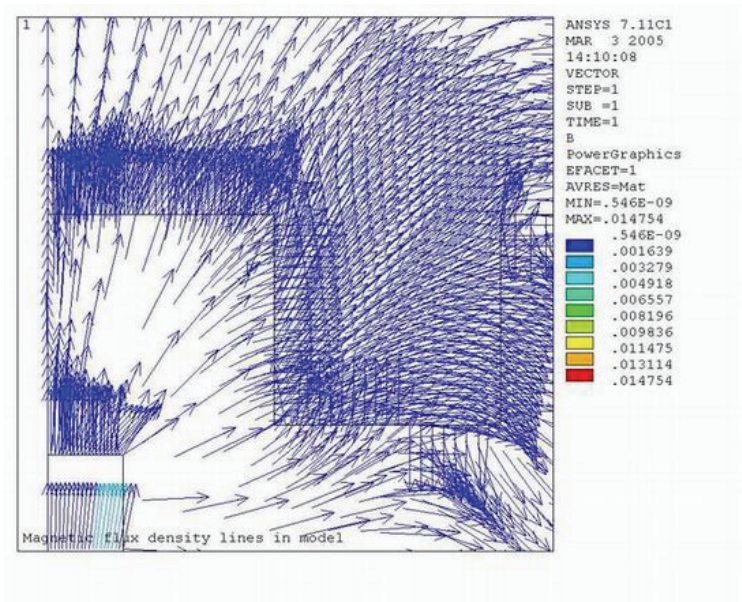
(b)

Fig. 17. Examples of simulation results in ANSYS software for the modeled identification system: a) magnetic induction flux in the system, b) normalized magnetic induction vectors nearby the identifier chamber
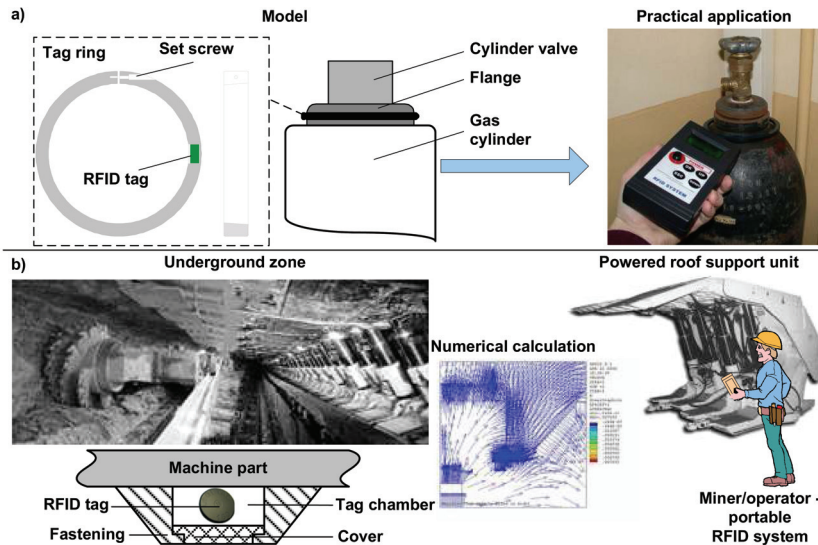
Fig. 18. Parts of a computer systems: a) RFID identification of gas cylinders,
b) RFID data collection in underground environment

5. Conclusion

The operation of passive anticollision RFID systems with inductive coupling is characterized by the interrogation zone, which is estimated in any direction of 3D space for group of electronic tags. The elements of algorithm for interrogation zone estimation in inductive coupled anticollision RFID identification system, taking into consideration the field aspects of operation conditions has been presented in this chapter. The special procedure of theoretical and experimental investigations, designed and made in Department of Electronic and Communication Systems, Rzeszów University of Technology, allows to determinate the functional efficiency of whole anticollision RFID system for all typical operating frequencies. The efficiency is just defined as the interrogation zone for group of n-tags and selects process of automatic identification on different economic and public activity in industry, commerce, science, medicine and others. This procedure is the last and most important stage of algorithm of synthesis of RWD and tag antenna set for the anticollision RFID system with inductive coupling. This is only preceded by stages, where the selection of RWD and tags along with antenna sets is carrying out. The final solution is calculation of the antenna unit array - based on Monte Carlo method and computer program with use of Mathcad (Jankowski-M., 2007) - with taking into consideration the algorithm of its synthesis according to equations, which have been determined during the synthesis of its electric model (Jankowski-M. & Kalita, 2008).

Paying attention to the maximum work distance between elements of the RFID system, in particular for systems working in the RFID far field, it is necessary to estimate the simulated and built antenna set RWD-tags in relation to the obligatory normalizations of communication and EMC. The electro-magnetic compatibility problems and current legal status for selected frequency bands used in different dedicated solutions (i.e. the animals'

identification, access control and objects identification in logistic process) have been taken into account in detail. The method of synthesis interrogation zone in accordance with EMC has enabled exact estimation of the non-interference of data transmission area (for write and read process) between RWD and electronic tags.

6. References

Åhlström, L. (2005). Flight RFID now boarding, *Global Ident. Magazine*, Vol. October, pp. 22-25

Bhatt, H.; Glover, B. (2006). *RFID Essentials*, O'Reilly, ISBN 978-0596009441

Cichos, S. (2002). Performance Analysis of Polymer Based Antenna-Coils for RFID, *IEEE Polytronic Conference*, pp.120-124, June 23-26, 2002, Zalaegerszeg, Hungary

Dobkin, D.; Wandinger, T. (2005). A Radio-Oriented Introduction to RFID-Protocols, Tags and Applications, *High Frequency Electronics*, Vol. 4, No. 6, pp. 32-46

Donaldson, J. (2009). Plugging profit leaks in the apparel sector, *ID World*, Vol. June, pp. 40-42

EN 50357 (2001). *Evaluation of human exposure to electromagnetic fields from devices used in Electronic Article Surveillance (EAS), Radio Frequency Identification (RFID) and similar applications*, IEC

EN 50364 (2001). *Limitation of human exposure to electromagnetic fields from devices operating in the frequency range 0 Hz to 10 GHz, used in Electronic Article Surveillance (EAS), Radio Frequency Identification (RFID) and similar applications*, CENELEC

ERC Rec. 70-03 (2008). *Relating to the use of short range devices (SRD)*, Edition of May 2008

ETSI EN 300 330-1 (2006). *Electromagnetic compatibility and Radio spectrum Matters (ERM); Short Range Devices (SRD); Radio equipment in the frequency range 9 kHz to 25 MHz and inductive loop systems in the frequency range 9 kHz to 30 MHz; Part 1: Technical characteristics and test methods*. V1.5.1

ETSI EN 300 330-2 (2006). *Electromagnetic compatibility and Radio spectrum Matters (ERM); Short Range Devices (SRD); Radio equipment in the frequency range 9 kHz to 25 MHz and inductive loop systems in the frequency range 9 kHz to 30 MHz; Part 2: Harmonized EN under article 3.2 of the R&TTE Directive*, V1.3.1

Finkenzeller, K. (2003). *RFID Handbook: Fundamentals and Applications in Contactless Smart Card and Identification*, Second Edition, Wiley, ISBN 978-0470844021, New York

Fitowski, K., Stankiewicz, J.; Jankowski, H.; Szczurkowski, M.; Jankowski-Mihułowicz, P.; Warzecha, M.; Krzak, Ł.; Worek, C.; Meder, A. (2005). RFID collection system of mining equipment in underground environment, *IV International Conference New electrical and electronic technologies and their industrial implementation (NEET'05)*, pp. 250-253, ISBN 83-87414-87-5 , June 21-24, Zakopane, Poland

Flores, J.; Srikant, S.; Sareen, B.; Vagga A. (2005). Performance of RFID tags in near and far field, *IEEE International Conference Wireless Communications (ICPWC'05)*, pp. 353-357, ISBN 0-7803-8964-6, 23-25, January 2005, New Delhi, India

Halliday, D.; Resnick, R.; Walker, J. (2004). *Fundamentals of Physics*, 7th Edition, Wiley, ISBN 978-0471216438, New York

Harrison, R. (2009). A practice of vetting RFID, *Global Ident. Magazine*, Vol. July, pp. 18-20

IEC 62369 (2008). *Evaluation of human exposure to electromagnetic fields from short range devices (SRDs) in various applications over the frequency range 0 GHz to 300 GHz - Part 1: Fields*

produced by devices used for electronic article surveillance, radio frequency identification and similar systems, IEC

Jankowski-Mihułowicz, P.; Kalita, W. (2009). Efficiency of Tag Antenna Unit in Anticollision Radio Frequency Identification Systems with Inductive Coupling, *Acta Electrotechnica et Informatica*, Vol. 9, No. 2. pp. 3-7, ISSN 1335-8243

Jankowski-Mihułowicz, P.; Kalita, W.; Pawłowicz, B. (2008). Problem of dynamic change of tags location in anticollision RFID systems, *Microelectronics Reliability*, Vol. 48, Issue 6, pp. 911-918

Jankowski-Mihułowicz, P.; Kalita, W. (2008). Problem of Interrogation Zone Synthesis in Anticollision Radio Frequency Identification Systems, *31th International Spring Seminar on Electronics Technology Reliability and Life-time Prediction (ISSE'08)*, pp. 647-652, ISBN 978-9630649155, May 7-11, 2008, Budapest, Hungary

Jankowski-Mihułowicz, P. (2007). Creation conditions of antenna array efficiency of anticollision Radio Frequency Identification systems with inductive coupling, *PhD dissertation*, AGH University of Science and Technology, Kraków

Jankowski-Mihułowicz, P.; Kalita, W. (2004). Passive tag supply work in radio frequency identification system, *Elektronika*, Vol.1, pp. 26-30, ISSN 0033-2089

Microchip (2004). *MicroID 125 kHz 13.56 MHz RFID System Design Guide*

Paret, D. (2005). *RFID and Contactless Smart Card Applications*, Wiley, ISBN 978-0470011959

Steden, G. (2005). A business case for RFID, *Global Ident. Magazine*, Vol. December, pp. 58-61

Wolfram, G.; Gampl. B.; Gabriel, P. (2008). *The RFID Roadmap: The Next Steps for Europe*, Springer, ISBN 978-3540710189

Wyld, D. C. (2009). Reinventing trash, *Global Ident. Magazine*, Vol. March, pp. 58-62

Wyld, D. C. (2005). RFID in the public sector, *Global Ident. Magazine*, Vol. October, pp. 46-51

Yan, L.; Zhang, Y.; Yang, L. T.; Ning, H. (2008). *The Internet of Things: From RFID to the Next-Generation Pervasive Networked Systems*, Auerbach, ISBN 978-1420052817

Yeh, M.-K.; Jiang, J.-R.; Huang, S.-T. (2009). Adaptive Splitting and Pre-Signaling for RFID Tag Anti-Collision, *Computer Communications*, Vol. 32, Issue 17, pp. 1862-1870, ISSN 0140-3664

Characterization of the Identification Process in RFID Systems

J. Vales-Alonso[1], M.V. Bueno-Delgado[1], E. Egea-López[1],
J.J. Alcaraz-Espín[1] and F.J. González-Castaño[2]
[1]Department of Communications and Information Technologies
Technical University of Cartagena,
[2]Department of Telematics Engineering, University of Vigo
Spain

1. Introduction

Radio Frequency Identification (RFID) is increasingly being used to identify and track objects in supply chains, manufacturing process, product traceability, *etc*. These environments are characterized by a large number of items which commonly flow in conveyor belts, pallets and lorries, entering and leaving logistic installations. In these scenarios the RFID systems are installed as follows: one or more readers are placed in a strategic place, creating checking areas. The tags, attached to items, enter and leave the checking areas (traffic flow). The goal of RFID in these applications is to guarantee the communication with the tags as quickly and reliably as possible, ensuring that all tags are identified before they leave the checking areas (Finkenzeller, 2003).

One of the main problems related to RFID in these applications is that both readers and tags share the RF spectrum. Hence, when two or more tags/readers transmit simultaneously a collision occurs. The collisions diminish the system performance, producing a delay in the identification, and may cause tags leaving the workspace unidentified. The parameter that measures the rate of unidentified tags is the *Tag Loss Ratio* (TLR). Depending on the application, even a TLR = 10^{-3} may be disastrous and cause thousands of items lost per day.

The collisions resolution on RFID has been extensively studied during the last years, for active and passive RFID systems. In active RFID, the collision resolution is not only mandatory to reduce the identification time, but also to decrease the tag energy consumption in order to maximize the batteries lifetime. In this case, tag hardware permits to put forward sophisticated anti-collision mechanisms. Nevertheless, this complex hardware also entails high-cost-devices and, in the end, the tag price becomes the dominant factor in the final deployment.

On the other hand, in passive RFID, the extreme simplicity of the tags is a hard constraint for the design of new collision resolution methods. However, the low-cost-price of passive tags is its most attractive characteristic which permits to think about a massive adoption in a near future. Several proposals have been conducted during the last years with the aim at minimizing the collision problems in passive RFID systems, suggesting new anti-collision protocols that, *a priori*, outperform the current standards. Most of these studies have been

addressed assuming *static* scenarios, that is, populations of tags that enter the workspace and stay there until all of them are identified, computing throughput (rate of identified tags per time unit), and the mean identification time. Although these results provide us insight into the performance of the algorithms, do not help to discern the conditions and phenomena which render to have uncontrolled tags (tags which are not identified when they leave the workspace) in *dynamic* scenarios, *i.e.,* scenarios where tags are entering and leaving the workspace.

In this chapter the analysis of the identification process is addressed either in static (section 4) and dynamic scenarios (section 5). In the former, the mean identification time is computed for the standard EPCglobal Class-1 Gen-2 anti-collision protocol (*Framed-Slotted-Aloha,* FSA). For the latter scenario, the rate of unidentified tags is also derived for the standard. Both studies are focused on the *Medium Access Control* (MAC) layer. Before, section 2 describes the identification process in RFID, Section 3 overviews MAC solutions presented in the scientific literature, including the current standard. A brief classification of the current passive RFID readers in the market is also introduced.

2. Identification process overview

Passive RFID technology has been inevitably selected in the majority of the industrial systems with a large number of identification objects. Several reasons can be adduced: The main one is the extremely low-cost of the tags (prices below 0.10 €), as well as lack of maintenance for the tags, reusability, easy installation, *etc.*

Passive RFID systems are installed in industrial environments to collect, automatically and transparently, the information regarding the items that enter and leave the workspace. The information is stored and managed by means of specialized middleware and software. Thus, updated information can be managed in real-time, decreasing the time to recognize, find, locate and manage items, therefore, improving facilities. Besides, RFID makes product traceability possible, which is an important issue in some industrial sectors.

As stated in the introduction, passive RFID system consists of one or more readers or interrogators placed in strategic zones and a potentially large population of cheap and small devices called tags or transponders. The readers transmit electromagnetic waves continuously, creating checking areas. Tags enter and leave the checking areas. To simplify the description in this chapter a passive RFID system with only one reader is assumed (see Fig. 1).

Passive tags are composed by an antenna, a simple electronic circuitry and a minimum amount of memory where it stores some information about the object (*e.g.* standard codes, history of transactions, expiration date). Since passive tags do not incorporate their own battery, they obtain the energy from the electromagnetic waves emitted by the reader (backscatter procedure) (Finkenzeller, 2003). This energy activates the electronic circuitry of the tag, which delivers a signal response with its carried data. Nevertheless, the simplicity of the tags limits their operative range, varying from some centimetres to a pair of meters.

The uplink and downlink communication between the reader and the tags share the RF spectrum. When several tags are in the coverage area at the same time, collisions may occur as a result of simultaneous transmissions. Hence, *Medium Access Control* (MAC) protocols are needed to handle/avoid collisions, but the extreme simplicity of the tags constraints the design of suitable anti-collision protocols. Complex or sophisticated behaviour can only exist in the reader system.
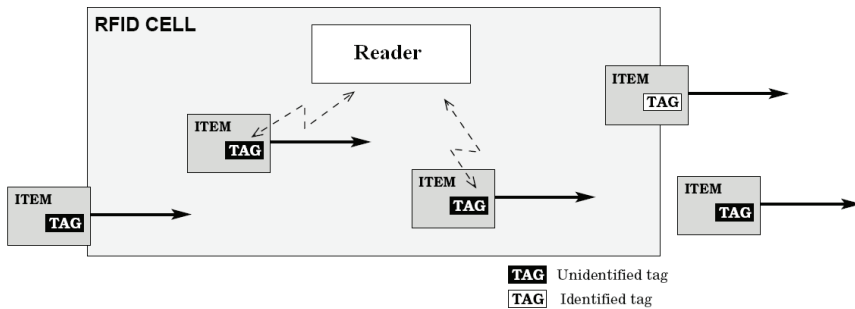
Fig. 1. Passive RFID scenario

During the last decade some standards have been proposed, not only for clarifying the specifications of hardware on passive tags and readers, but also for setting the anti-collision procedure to handle/avoid collisions (ISO, 2003) (EPC, 2004). Since 2005, the standard EPCglobal Class-1 Gen-2 for passive RFID has been the most extended and adopted by the manufacturers. However, it has been outperformed by new anti-collision algorithm proposals. Most of these studies have been addressed assuming *static* scenarios, that is, blocks of tags entering the checking area and staying there until all of them are successful identified. Disappointedly, actual RFID systems may involve a flow of tags entering and leaving the workspace (see Fig. 1). In these scenarios, the collision resolution is not only mandatory to reduce the identification time and to improve the system throughput, but also for minimizing the number of unidentified tags that leave the workspace, that is, the TLR.

3. The collision problem: Anti-collision mechanisms for RFID

Several multiple-access techniques and anti-collision protocols have been developed with the aim of minimizing colliding signals. The anti-collision procedures are focused on the Physical and MAC layer. We review these procedures in the following subsections.

3.1 Anti-collision protocols at Physical layer
At physical layer, FDMA, TDMA, SDMA, CDMA and CSMA have been the alternatives most studied (Finkenzeller, 2003). Albeit they can not be used directly in RFID because the following problems:

- *Frequency Division Multiple Access* (FDMA). The channel is divided into different sub-channels and the users are allocated different carrier frequencies. In RFID systems, this technique adds a cost to the readers, because they must provide a dedicated receiver for every reception channel. On the other hand, tags should be able to distinguish between different frequencies and to select the sub-channels of interest. Only active tags add the previous functionality.
- *Time Division Multiple Access* (TDMA). The channel is divided into time slots that are assigned to the users. One of the most important problems of this technique is the users must be synchronized to send their information in the slot selected. This technique can be applied directly to RFID. For passive RFID systems, the tag's simplicity requires the reader controls the synchronization (centralized). For active RFID system, the

synchronization can be centralized or the tags can control the synchronization themselves (distributed).

- *Space Division Multiple Access* (SDMA). This technique reuses certain resources, such as channel capacity in spatially separated areas. This technique can be applied to an RFID system as follows: in a scenario with two or more readers, the read range of each one is reduced but compensated by forming an array of antennas, providing then a large coverage area. The main drawback is the high implementation cost of the complicated array antennas system.

- *Code Division Multiple Access* (CDMA). It consists of using spread-spectrum modulation techniques based on a pseudo random code to spread the data over the entire spectrum. CDMA is the ideal procedure in many applications, e.g. navigation systems, GPS, *etc*. However, in RFID systems, this technique means more complex hardware in the tags and hence, higher cost.

- *Carrier Sense Multiple Access* (CSMA). This technique requires the tags to sense the channel traffic before sending their information. If there is no traffic, the tag starts to send. This mechanism can be only used with active tags because passive tags cannot monitor the channel.

Many of these solutions are not cost-effective due to the extra complexity of the tag. This is why solutions to the collision issue are usually sought at the MAC layer, tackling the burden of the algorithm at the reader equipment. Besides, new reactive procedures are being explored. Namely, those which extract useful information from colliding signals at Physical layer:

- The application of *Radar-Cross-Section* (RCS) has been proposed in the field of RFID by (Khasgiwale *et al.*, 2009). The number of collided tags is detected by means of the analysis of the RCSs. Then, *Minimum Distance Detector* (MDD) mechanism is used to decode colliding signals. Notice that this technique may only be useful for collisions where only two tags are involved. Indeed, this mechanism has been only simulated using ISO 18000-6C as the underlying standard (ISO, 2003).

- Constellations analysis computes IQ constellations produced by additive simultaneous tag responses, and determines symbol decoding regions of transmissions. This technique has been described for *Low Frequency* (LF) RFID systems in (Shen *et al.*, 2009) and for *Ultra High Frequency* (UHF) in (Angerer *et al.* 2009).

Although these techniques are still immature, the authors point out their feasibility and compatibility with current standards and tags.

3.2 Anti-collision protocols at MAC layer

When a number of tags/readers are presented simultaneously in the coverage area an appropriate *Medium Access Control* (MAC) protocol is needed to handle/avoid collisions caused by simultaneous transmissions. Collisions in RFID occur in a number of ways:

- Case of a single reader-multiple tags collisions. Multiple tags are in the reading range of the same reader and respond simultaneously. The reader detects the electromagnetic wave but is unable to interpret the signal received.

- Case of multiple readers-single tag collisions. Only one tag is in the read range of multiple readers. The interferences occur when the signal from a neighboring reader collides with the tag transmission.

- Case of reader-reader collisions. Multiple readers configured to work within the same frequency band, interfere each other and thus a collision occurs.

Discussion of these three types of collisions would require a complete volume. Therefore, in this chapter, an overview of the single reader-multiple tags collisions is presented, as well as the most relevant anti-collisions proposals.

3.2.1 Tree-based tag anti-collision protocols

Tree-based anti-collision protocols put the computational burden the reader. The reader attempts to recognize a set of tags in the coverage area in several interrogation cycles. Each interrogation cycle consists of a *query* packet, sent by the reader, and the response of tags in coverage. If a set has more than one tag, a collision occurs. When a collision occurs, the mechanism splits the set into two subsets using the tags identification numbers or a random number. The reader keeps on performing the splitting procedure until each set has one tag. Tree-based protocols are not efficient when the number of tags to recognize is large due to the lengthy identification delay (see Fig. 2).

Tree based anti-collision protocols have been extensively studied during the last years (Hush & Wood, 1998; Jacomet *et al.*, 1999; Law *et al.* 2000; Shih *et al.*, 2006; Myung & Lee 2006).

3.2.2 Aloha protocols

Aloha protocols are classified into four main groups. The first one is the *Pure-Aloha* (Leon-Garcia & Widjaja, 1996) protocol which is the simplest anti-collision scheme for passive tags with read-only memory. The second group is the *Slotted Aloha* protocol (Weselthier, 1988) Slotted Aloha protocol is based on Pure-Aloha. A tag can transmit only at the beginning of a slot. Therefore, packets can collide completely or not collide at all. The mechanism is as follows: the reader sends a packet announcing the number of slots (*K*) that tags can compete to use. Each tag receives the data and generates a random number between [0, *K-1*]. The result is the slot where the tag must transmit their identification number.

Slotted-Aloha outperforms Pure-Aloha at the cost of requiring a reading system that manages slotted time synchronization. The third group, Frame-Slotted-Aloha (FSA), is a variation of Slotted-Aloha. In FSA, the time is divided into discrete time intervals but slots are confined in consecutive frames, also called cycles. Each frame has a length of a fixed number of slots (see Fig. 3). FSA has been implemented in many commercial products and has been standardized in ISO/IEC-18000-6C (ISO, 2003) and in EPCglobal Class-1 Gen-2 (EPC, 2004).

In FSA, when the number of tags is much larger than the number of slots, the identification delay increases considerably. On the other hand, if the number of tags is low and the number of slots is high, many empty slots can occur, which leads to increased identification time.

In Dynamic FSA, the number of slots per frame is variable. Tags randomly choose a slot within the frame to send their information to the reader. When a frame finishes, an identification cycle concludes and the reader, following some rules, makes a decision about whether to increase/decrease/maintain the number of time-slots per frame in the next identification cycle.

According to (Schoute, 1983), the optimum throughput in a cycle of a DFSA protocol is achieved if the number of tags N equals the number of slots K in that cycle, and this throughput is given by $e^{-1} \approx 0.36$. Since the number of tags in range per cycle is commonly unknown, first the reader must estimate the number of tags that are going to compete per cycle, possibly through the statistical information collected on a cycle-by-cycle basis or any

heuristic methods. Then, the reader adjusts the frame size to guarantee the maximum throughput and minimize the identification delay. The main anti-collision DFSA algorithms for RFID applications have been comprehensively studied in ((a) Bueno-Delgado *et al.*, 2009).
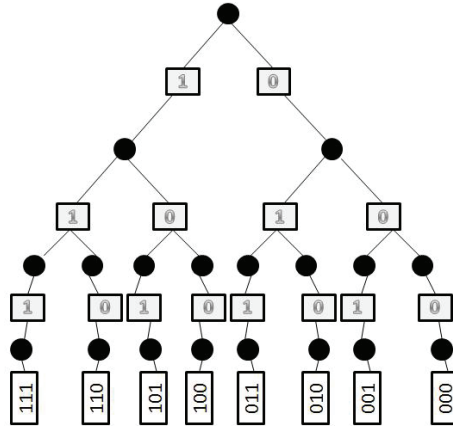
Fig. 2. Tree-based protocol procedure

3.3 EPCglobal Class-1 Gen-2

EPCglobal is an institution focused on the development of industry-driven standards for the Electronic Product Code (EPC) to support the use of Radio Frequency Identification (RFID). Regarding passive RFID, EPCglobal provides the EPCglobal Class-1 Gen-2 standard.

EPCglobal Class-1 Gen-2 is called "the worldwide standard for RFID systems" because it has been implemented to satisfy all the needs of the final customer, irrespective of the geographic location. For passive RFID systems, EPCglobal Class-1 Gen-2] is considered the *de facto* standard. It includes a set of specifications for the hardware of the passive tag and the hardware and software in the reader systems (which carry the true system complexity). After its publication in year 2005, it has been widely adopted by RFID systems manufacturers. Many commercial RFID systems have been implemented following this standard.
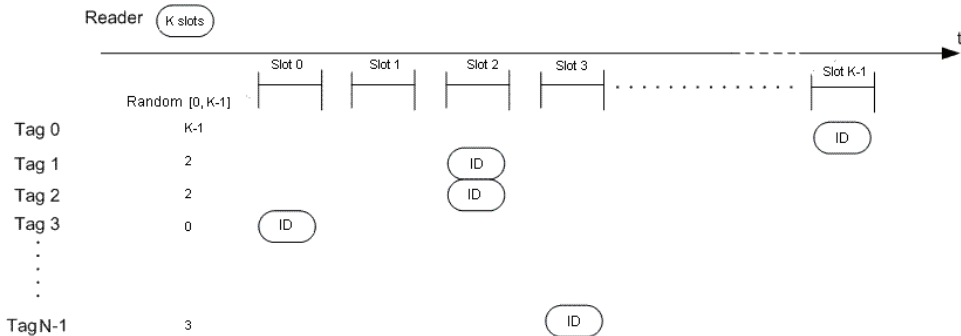
Fig. 3. Frame Slotted Aloha procedure

EPCglobal Class-1 Gen-2 works at UHF band (860MHz-930MHz). It proposes an anti-collision mechanism based on a variation of FSA. Fig. 4 illustrates EPCglobal Class-1 Gen-2 operation.

At a first stage the reader system is continuously monitoring the environment to detect the presence of tags by means of *Broadcast* packets. Tags in the coverage area are excited by the electromagnetic waves of the reader and send a reply immediately, producing a multiple collision. The reader detects the collision and starts the identification cycle. During each identification cycle, the time is structured as one frame, which is itself divided into slots, following a FSA scheme.

EPCglobal Class-1 Gen-2 shows two configuration alternatives:

- Fixed frame-length procedure: All identification cycles (frames) have the same value (number of slots). It is common to find commercial systems with this configuration.
- Variable frame length procedure (denoted as frame-by-frame adaptation). The number of slots per frame can be changed by the reader in each identification cycle. The reader decides if increase, decrease or maintain the number of slots per frame in function of some criteria.

In the following subsections both procedures are overviewed, as well as the implementation status of current readers.

3.3.1 Fixed frame length procedure

An identification cycle starts when the reader transmits a *Query* packet, including a field of four bits with the value $Q \in [0,…,15]$, stating that the length of the frame will be of 2^Q slots. Tags in coverage receive this packet and generate a random number *r* in the interval $[0, 2^Q-1]$. The *r* value represents the slot within the frame where the tag has randomly decided to send its identification number ID=*r*. Inside each frame, the beginning of a slot is governed by the reader by transmitting the *QueryRep* packet, excepting the slot 0, which is automatically initiated by the *Query* packet. The tags in coverage use an internal counter to track the number of transmitted *QueryRep* packets since the last *Query* packet, and then recognize the slot when they should transmit.

When the moment arrives, the tag transmits its identification number ID, which corresponds to the random value *r* calculated for contention, which is also equal to the slot number in the frame. After transmitting its ID, three actions can follow:

- If more than one tag has chosen the same slot, a collision occurs which is detected by the reader. Then, the reader reacts initiating a new slot with a *QueryRep* packet (see slot 0 in Fig. 4). The tags which transmitted their ID assume that a collision occurred, and must update their counter value to 2^Q-1. That means that they will not compete again in this identification cycle.
- If the reader receives the ID correctly, and this coincides with the slot number within the frame, then it responds with an *Ack* packet. All tags in coverage receive the packet but only the identified tag answers with a *Data* packet, e.g. an EPC code.
  If the reader receives the *Data* packet, it answers sending a *QueryRep* packet, starting a new slot. The tag identified will finish its identification process (see slot 1 in Fig. 4).
- If the reader does not receive a correct *Data* packet within a given time, it considers the time-slot has expired, and sends a *Nack* packet. Again, all tags in coverage receive it, but only the tag in the identification reacts by updating its counter value to 2^Q-1. Thus, this tag will not contend again in this identification cycle (see slot 3 in Fig. 4). After this, the

reader will send a new *Query* or *QueryRep* packet to start a new frame or slot respectively.

Finally, when a cycle finishes, a *Query* packet is sent again by the reader to start a new identification cycle. Tags unidentified in the previous cycle will compete again, choosing a new random *r* value.

3.3.2 Variable frame length procedure

The fixed frame length EPCglobal Class-1 Gen-2 standard provides a low degree of flexibility. If the Q value selected is high and the number of tags in coverage is low, many empty slots appear in the frame. On the contrary, if the Q value is low and the number of tags is high, many collisions arise. To mitigate this problem the standard proposes a variable frame length procedure (EPC, 2004) that selects the Q value in each cycle by means of some arbitrary function. ((a) Bueno-Delgado *et al.*, 2009) analyzes the different variable frame length algorithms. Since current readers usually implement only the fixed frame length procedure, in this chapter we focus exclusively on it.
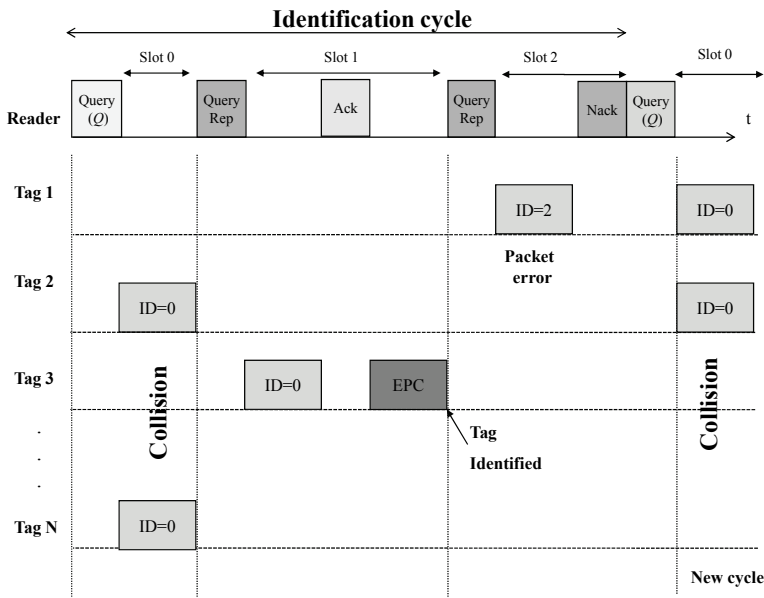
Fig. 4. EPCglobal Class-1 Gen-2 identification procedure

3.3.3 EPCglobal Class-1 Gen-2 in the market

The current UHF RFID readers available in the market implement the worldwide standard EPCglobal Class-1 Gen-2. Some of them only permit to work with one of the two procedures explained before. Besides, some readers do not permit to configure the initial frame-length (the Q value) or only some certain values which can influence directly to the final system performance. Depending on the level of frame-length configuration, the readers can be classified as follows:

- Readers with fixed frame length, without user configuration (Symbol, *on-line*; ThingMagic, *on-line*; Mercury4, *on-line*; Caen, *on-line*; Awid, *on-line*; Samsys, *on-line*). Identification cycles are fixed and set up by the manufacturer. It is not possible to modify by the user (it is usually fixed to 16 slots). Therefore, these readers are not able to optimize the frame-length.
- Readers with fixed frame length with user configuration(Samsys, *on-line*; Intermec, *on-line*; Alien, *on-line*). Before starting the identification procedure the user can configure the frame length, choosing between several values, which depend on the manufacturer. Then, the identification cycle cannot be changed. If the user wants to establish a different value of frame-length, it is necessary to stop the identification procedure and restart with the new value of frame-length.
- Readers with variable frame length (Samsys, *on-line*; Intermec, *on-line*; Alien, *on-line*). The user only configures the frame- length for the first cycle. Then the frame-length is self-adjusted trying to adapt to the best value in each moment, following the standard proposal (EPC, 2004).

4. Identification process in *static* scenarios

S*tatic* scenarios are characterized by a block of tags (modeling a physical pallet, box, *etc.*) that enter the checking area and never leave. Two related performance measures are commonly considered: The identification time, defined as the *mean* number of time units (slots, cycles, seconds, *etc.*) until all tags are identified, and the system throughput or efficiency, defined as the inverse of the mean identification time, *i.e.*, the ratio of identified tags per time unit.

4.1 Markovian analysis

The identification process in a *static* scenario is determined by the number of remaining unidentified tags. Thus, the identification process can be modeled as a homogeneous (*Discrete Time Markov Chain*) DTMC, X_c, where each state in the chain represents the number of unidentified tags, being c the cycle number. Thus, the state space of the Markov process is {N, N-1,…, 0}. Fig 5 shows DTMC state diagram from the initial state, $X_0=N$. The transitions between states represent the probability to identify a certain quantity of tags t or, in other words, the probability to have (N-t) tags still unidentified.

The transition matrix P depends on the anti-collision protocol used and its parameters. For EPCglobal Class-1 Gen-2, the parameter K denotes the number of slots per frame (frame length). To compute the matrix P, let us define the random variable μ_t, which indicates the number of slots being filled with exactly t tags. Its mass probability function is (Vogt, 2002):
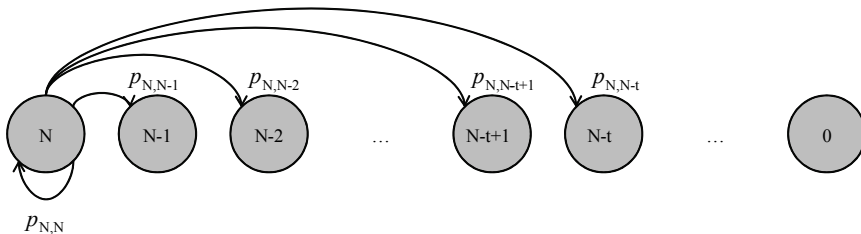
Fig. 5. Partial Markov Chain

$$\mathrm{Pr}_{K,N}(\mu_t = m) = \frac{\binom{K}{m} \prod_{i=0}^{m-1} \binom{N-it}{t} G(K-m, N-mt, t)}{K^N} \tag{1}$$

Where *m=0,...,K* and:

$$G(M,l,v) = M^l + \sum_{i=1}^{\left\lfloor \frac{l}{v} \right\rfloor} \left\{ (-1)^i \prod_{j=0}^{i-1} \left\{ \binom{l-jv}{v} (M-j) \right\} (M-i)^{l-iv} \frac{1}{i!} \right\} \tag{2}$$

Since the tags identified in a cycle will not compete again in the following ones, then the transition matrix *P* is ((b) Bueno-Delgado *et al.*, 2009):

$$p_{i,j} = \begin{cases} \mathrm{Pr}_{K,i}(\mu_1 = i-j) & ,i-K \le j < i \\ 1 - \sum_{y=i-1}^{i-K} p_{i,y} & ,i = j \qquad \text{for } i = 1,...,N. \\ 0 & ,otherwise \end{cases} \tag{3}$$

The chain has a single absorbing state, $X_c=0$. The mean number of steps until the absorbing state is the mean number of identification cycles ($\bar{c}$). It can be computed by means of the fundamental matrix, *D*, of the absorbing chain (Kemeny, 2009):

$$D = (I - F)^{-1} \tag{4}$$

As usual, *I* denotes the identity matrix, and *F* denotes the submatrix of *P* without absorbing states. Then,

$$\bar{c} = \sum_{j \in B} D_{Z,j} \tag{5}$$

Where *B* is the set of transitory states, and *Z* is the absorbing state.
In addition, using the physical and FSA standard parameters (Table 1 enumerates the typical EPCglobal parameters) is possible to transform the identification time to seconds as follows: T_{id} is the duration of a slot with a valid data transmission (EPC code). T_v and T_c is the duration of an empty and collision slot, respectively. Then, the identification time in seconds is approximated by:

$$\bar{T}_{total} \approx \bar{c} \cdot \left[\bar{k}_v \cdot T_v + \bar{k}_c \cdot T_c + \bar{k}_{id} \cdot T_{id} \right] \tag{6}$$

$\bar{k}_v$, $\bar{k}_c$ and $\bar{k}_{id}$ denote the average number of empty, collision and successful slots, respectively. These variables depend on the particular FSA algorithm and its configuration, and on the population size. For instance, setting M=4 (see Table 1), T_{id}=2.505 ms and T_v=T_c=0.575 ms. Since an empty slot and a collision slot have the same duration, the previous equation can be simplified:

$$\bar{T}_{total} \approx \bar{c} \cdot \left[(\bar{k}_v + \bar{k}_c) T_c + \bar{k}_{id} \cdot T_{id} \right] \tag{7}$$

Since,

$$\overline{k}_v + \overline{k}_c \approx K \cdot \overline{c} - \overline{k}_{id} \tag{8}$$

Then,

$$\overline{T}_{total} \approx \overline{c} \cdot \left[(K \cdot \overline{c} - \overline{k}_{id})T_c + \overline{k}_{id} \cdot T_{id} \right] \tag{9}$$

Different populations of tags and Q values have been considered and the identification time has been measured. Fig. 6 shows the mean number of slots required to identify each tag population.

4.2 System throughput

The throughput (th) can be computed from the previous Markov analysis, just as the inverse of the identification time. Another way is described in this section. Let us remark that, obviously, the result of both methods is equal, and the second one is provided for completeness. Given N tags, and K slots, the probability that t tags respond in the same time-slot is binomially distributed:

$$\Pr(t) = \binom{N}{t}\left(\frac{1}{K}\right)^t \left(1 - \frac{1}{K}\right)^{N-t} \quad \text{for } t=0,...,N \tag{10}$$

Then, $Pr(t=0)$ is the probability of an empty slot, $Pr(t=1)$ the probability of a successful slot, and $Pr(t \geq 2)$ the probability of collision:

$$\Pr(t = 0) = \left(1 - \frac{1}{K}\right)^N \tag{11}$$

$$\Pr(t = 1) = \frac{N}{K}\left(1 - \frac{1}{K}\right)^{N-1} \tag{12}$$

$$\Pr(t \geq 2) = 1 - \Pr(t = 0) - \Pr(t = 1) = 1 - \left(1 - \frac{1}{K}\right)^N \left(1 - \frac{N}{K-1}\right) \tag{13}$$

Since every identification cycles is composed by K slots, the throughput per slot is computed as follows:

$$th = K \cdot \Pr(t = 1) = N\left(1 - \frac{1}{K}\right)^{N-1} \tag{14}$$

4.3 Optimum Q configuration

As seen in the previous sections, the identification performance depends on the number of tags competing and on the frame length. The best throughput performance occurs when there are as many competing tags as slots in the frame, $N=K$, yielding a maximum

Parameter	Symbol	Value
Electronic Product Code	EPC	96 bits
Initial Q value	Q_0	4
Reference time interval for a data-0 in Reader-to-Tag signaling	TARI	12.5us
Time interval for a data-0 in Reader-to-Tag signaling	DATA0	$1.0 \cdot$TARI
Time interval for a data-1 in Reader-to-Tag signaling	DATA1	$1.5 \cdot$TARI
Tag-to-Reader calibration symbol	Trcal	64us
Reader-to-Tag calibration symbol	RTcal	31.25us
Divide Ratio	DR	8
Backscatter Link Frequency	LF	DR/Trcal
Number of subcarrier cycles per symbol in Tag-to-Reader direction	M	1,2,4,8
Reader-to-Tag rate	Rrate	64Kbps
Tag-to-Reader Rate	Trrate	LF/M
Link pulse-repetition interval	T_{pri}	1/LF
Tag-to-Reader preamble	T→R Preamble	$6\ T_{pri}$
Tag-to-Reader End of Signaling	T→R EoS	$2\ T_{pri}$
Delimiter		12.5us
Reader-to-Tag Preamble	R→T Preamble (RTP)	Delimiter+DATA0+TRcal+Rtcal
Reader-to-Tag Frame synchronization	R→T FrameSync	RTP –Rtcal
Time for reader transmission to tag response	T_1	Max(RTcal, 10 T_{pri})
Time for tag response to reader transmission	T_2	$5\ T_{pri}$
Time a reader waits, after T_1, before it issues another command	T_3	$5\ T_{pri}$
Minimum time between reader commands	T_4	$2 \cdot$Rtcal
Query packet	22 bits	22 bits
QueryAdjust packet	9 bits	9 bits
QueryRep packet	4 bits	4 bits
Ack packet	18 bits	18 bits
Nack packet	8 bits	8 bits

Table 1. Typical values of EPCglobal Class-1 Gen-2 parameters

throughput of $1/e \approx 0.36$ (Schoute, 1983). For EPCglobal Class-1 Gen-2, K can not be set to any arbitrary natural number, but to powers of two, *i.e.* $K=2^Q$, for $Q \in [0, …, 15]$. For every N value, the value of Q that maximizes the throughput has been computed in ((b) Bueno-Delgado, 2009). Fig. 7 shows the results, and Table 2 summarizes them.

The former optimal configurations are useful for variable length readers. Readers with fixed frame length can be optimized as well, setting the best value of Q for a given population size. Notice that both criteria are different: the first one optimizes the reading cycle by cycle, whereas the second one minimizes the whole process duration. These values have been calculated by means of simulations in ((b) Bueno-Delgado, 2009), and are also shown in Table 2.

5. Identification process in *dynamic* scenarios

Many real RFID applications (*e.g.* a conveyor belt installation) work in *dynamic* scenarios. For this type of systems, the performance analysis must be linked with the *Tag Loss Ratio.* This parameter measures the rate of unidentified tags in an identification process and, depending on the final application, even a low TLR (*e.g.* TLR=10⁻³) may be disastrous and cause thousands of items lost per day. In this section, the TLR is computed for a RFID scenario similar to the one depicted in Fig. 1. There is an incoming flow of tags entering the coverage area of a reader (RFID cell), moving at the same speed (*e.g.*, modeling a conveyor belt). Therefore, all tags stay in the coverage area of the reader during the same time.

Every tag unidentified during that time is considered lost. As in the previous analysis, once acknowledged, a tag withdraws from the identification process. This problem has been studied previously in (Vales-Alonso *et al.,* 2009). Thereafter, the following notation and
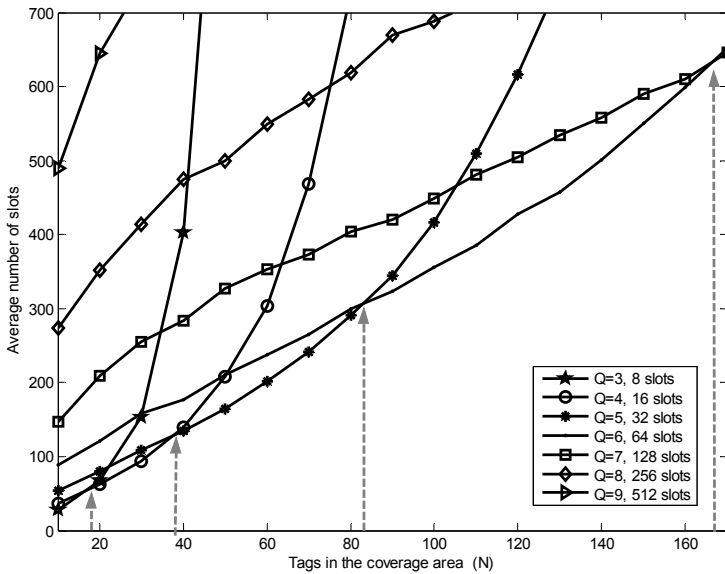
Fig. 6. Mean identification time (in number of slots) vs. *N,* for different *Q* values
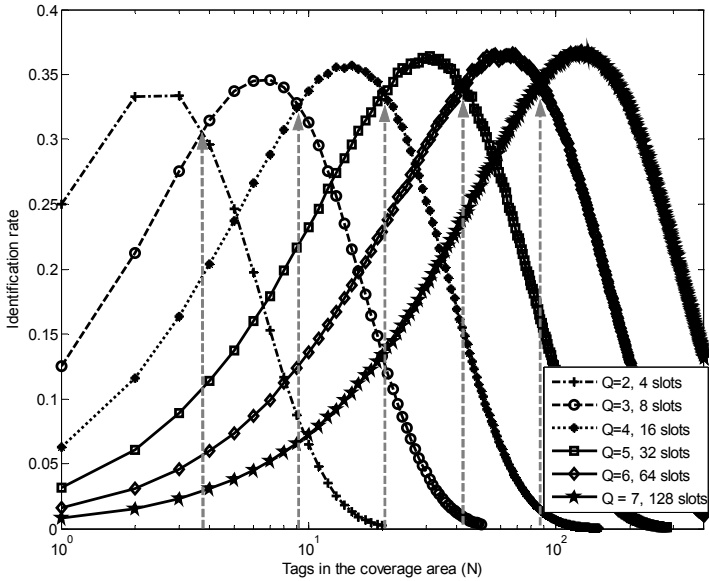
Fig. 7. Throughput (Identification rate) vs. *N* for different *Q* values

Optimal *Q*	Cycle by cycle optimization		Whole process optimization	
	Number of slots (*K*)= 2^Q	*Tags* **in coverage** (*N*)	*Number of slots* (*K*)= 2^Q	**Tags in coverage** (*N*)
1	2	$N \leq 2$	2	$N \leq 4$
2	4	$2 \leq N < 4$	4	$4 \leq N < 8$
3	8	$4 \leq N < 9$	8	$8 \leq N < 19$
4	16	$9 \leq N < 20$	16	$19 \leq N < 38$
5	32	$20 \leq N < 42$	32	$38 \leq N < 85$
6	64	$42 \leq N < 87$	64	$85 \leq N < 165$
7	128	$87 \leq N < 179$	128	$165 \leq N < 340$
8	256	$179 \leq N < 364$	256	$340 \leq N < 720$
9	512	$364 \leq N < 710$	512	$720 \leq N < 1260$
10	1024	$710 \leq N < 1430$	1024	$1260 \leq N < 2855$
11	2048	$1430 \leq N < 2920$	2048	$2855 \leq N < 5955$
12	4096	$2920 \leq N < 5531$	4096	$5955 \leq N < 12124$
13	8192	$5531 \leq N < 11527$	8192	$12124 \leq N < 25225$
14	16384	$11527 \leq N < 23962$	16384	$25225 \leq N < 57432$
15	32768	$23962 \leq N$	32768	$57432 \leq N$

Table 2. Throughput Maximization

conventions are used: a row vector is denoted as $\vec{V}$, the i-th component of a vector is denoted $(\vec{V})_i$, and $\sigma(\vec{V})$ denotes the sum of the values of the components of a vector $\vec{V}$.

For the sake of simplicity, let us assume tags remain C complete cycles in the reading area. Then, once a tag has entered the coverage area, it should be identified in the following C identification cycles. Otherwise (if it reaches the cycle $C+1$), tag is lost.

A truncated Poisson distribution, with parameter λ, has been selected as the arrival process in the system:

$$a(t) = \frac{\lambda^t}{t! \sum_{i=0}^{H} \frac{\lambda^t}{i!}}$$

(15)

For $t=,...,H$, being H the maximum number of tags entering per cycle.

The former assumptions allow to express the dynamics of the system as a discrete model, evolving cycle by cycle, such that,

- Each tag is in a given reading cycle in the set [$1,...,C$]
- After a cycle, identified tags withdraw from the identification process.
- After a cycle, each tag unidentified and previously in the i-th cycle moves to the ($i+1$)-th cycle.
- If a tag enters cycle $C+1$, it is considered out of the range of the reader, and, therefore, lost.
- At the beginning of each cycle, up to H new tags are assigned to cycle 1, following a truncated Poisson distribution.

For any arbitrary cycle, the evolution of the system to the next cycle only depends on the current state. Thus, a DTMC can be used to study the behavior of the RFID system. Next section describes this model.

5.1 Markovian analysis

Based on previous considerations, the system can be modeled by a homogeneous discrete Markov process X_c, whose state space is described by a vector $\vec{E} = \{e_1, ..., e_{C+1}\}$, where each $e_j \in [0,...,H]$, representing the number of unidentified tags in the j-th cycle. The following figures illustrate the model. They describe the state of the system for two consecutive cycles, showing tags entering and leaving the system, in both identification and no identification scenarios. Therefore, e_j is the number of tags which are going to start their j-th identification cycle in coverage. e_1 component also represents the number of tag arrivals during the previous identification cycle (which do not contend since they have not received a *Query* packet yet). Finally, component e_{C+1} indicates the number of tags lost at the end of the identification cycle, since tags leave coverage area after $C+1$ cycles.

In addition, let us define the mapping Ψ as a correspondence between the state vector and an enumeration of the possible number of states:

$$\Psi : [0,...,H] \times^{(C+1)} \times [0,...,H] \rightarrow \left[1,...,(H+1)^{C+1} \right]$$
$$\vec{E} = \{e_1, e_2,...,e_{C+1}\} \rightarrow \Psi : (\vec{E}) = 1 + \sum_{j=1}^{C+1} e_j H^{j-1}$$

(16)

This allows defining *i*-th state in our model as the state whose associated vector is given by Ψ^{-1}. Let us denote $\vec{E}_i$ as the vector associated to *i*-th state, *i.e.*, $\vec{E}_i = \Psi^{-1}(i)$. Finally, let e_{ij} denote to the *j*-th component of the $\vec{E}_i$ state vector.

The goal is to describe the transition probability matrix *P* for the model, from every state *i* to another state *j*. The stationary state probabilities is computed as $\vec{\pi} = \vec{\pi}\ P$. Let us denote λ_j as the average incoming unidentified tags to cycle *j*, which can be computed as:

$$\lambda_j = \sum_{j=1}^{(H+1)^{C+1}} e_{ij}\vec{\pi}_i \tag{17}$$

Obviously, λ_1 is the average incoming traffic in the system and λ_{C+1} is the average outgoing traffic of unidentified tags. Then, TLR can be calculated as:

$$TLR = \frac{\lambda_{C+1}}{\lambda_1} = \frac{\sum_{i=1}^{(H+1)^{C+1}} e_{i(C+1)} \cdot \vec{\pi}_i}{\lambda_1} \tag{18}$$

To build the transition probability matrix *P* let us define the auxiliary vectors $\vec{L}_i$ and $\vec{U}_i$ as:

$$\vec{L}_i = \{e_{i1},...,e_{iC}\} \tag{19}$$

$$\vec{U}_i = \{e_{i2},...,e_{i(C+1)}\}$$

That is, the $\vec{E}_i$ state vector without either the last or the first component. Let us define the *outcome* vector as:

$$\vec{O}^{ij} = (\vec{L}_i - \vec{U}_j) = \{o_1^{ij}...o_C^{ij}\} \tag{20}$$

Figures 8 and 9 graphically show this computation. To construct the transition matrix let us define the function *id(i,j)* that operates on an outcome vector $\vec{O}^{ij}$ providing the number of identified tags in a transition from a state *i* to a state *j*:

$$id(i,j) = \vec{O}^{ij} \cdot \vec{1}' \tag{21}$$

Notice that, for $\vec{E}_i$ and $\vec{E}_j$, if $e_{ik}<e_{j(k+1)}$ for some *k*=1,...,*C*, such transition is impossible (new tags cannot appear in stages other than stage 1). These impossible transitions will result in *id(i,j)* providing a negative value. The random variable *s(K,N)* indicates the number of contention slots being filled with a single tag. The *mass probability function* of *s(K,N)* has been computed in (Vogt, 2002) (see equation (1) and (2)). Henceforth, let us denote *Pr{s(K,N)=k}* as $s_k=(N,K)$.

As stated in section 4.2, using FSA, up to *K* tags may be identified in a single identification cycle. Therefore, possible cases range from *id(i,j)*=0 to *id(i,j)*=*K*. The probability of *id(i,j)* successful identifications is uniformly distributed among the contenders, whose distribution depends on the particular state, and hence the transition probability. From equations (1) and (2) and the previous definitions, the transition matrix *P* can be computed as follows:

$$
p_{i,j} = \begin{cases} a(e_{j1})s_0(K,N) & ,id(i,j)=0 \\ \\ a(e_{j1})\dfrac{\prod_{k=1}^{C}\binom{e_{ik}}{o_k^{ij}}}{\binom{N}{id(i,j)}}s_{id(i,j)}(K,N) & ,id(i,j)\in[1,K] \\ \\ 0 & ,otherwise \end{cases} \tag{22}
$$
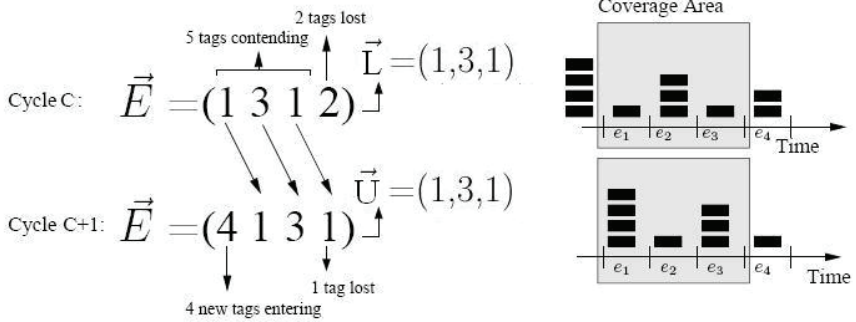
Fig. 8. Representation of the transition state. Case 1: No identification
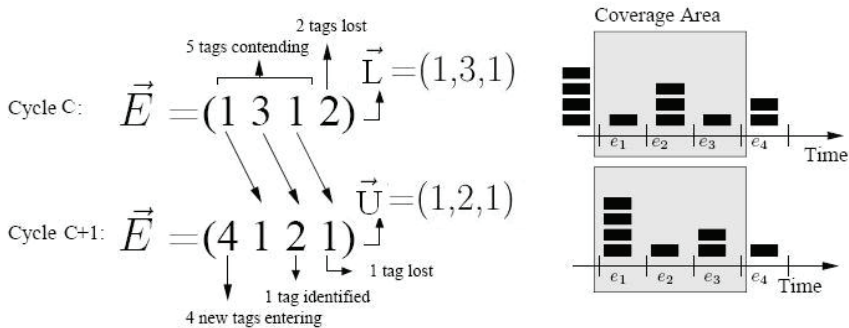
Fig. 9. Representation of the transition state. Case 2: Identification

5.2 Experimental evaluation: a postal mail control system

From a practical point of view, TLR evaluation may become critical in some realistic scenarios. As an example, this section evaluates a postal mail control system, where mails are carried over conveyor belts for distribution, with an attached tag.

Two configurations for the mail sojourn times of 2 and 3 identification cycles have been considered, for a frame length of $K=8$ slots. The slot time is assumed to be 4 ms based on parameters shown in Table 1. Therefore, the time sojourn is around 64 ms for $C=2$ and 100 ms for $C=3$. λ range spans from 1 to 7. Results are provided in figures 10 and 11. As expected, for a fixed C, TLR increases as the maximum number of arrivals H increases. In addition, for the parameters analyzed, keeping fixed H decrements TLR if C grows, because there are more opportunities for identification. For example, the maximum number of tags for $H=6$ and $C=2$ is 12 tags, whereas for $H=6$ and $C=3$ there might be up to 18 tags.

The main issue of the previous analysis is that it becomes computationally unfeasible for moderate values of H and C. In this case, simulation is mandatory. Figure 12 shows simulations performed for $\lambda=[10,...,60]$ and $H=[3; 6]$. In this case, envelopes sojourn time is close to 800ms. We can observe that, if we set $H=3$, TLR reaches 10^{-4} and does not vary, independently of the λ value. On the other hand, with $H=6$, the TLR reaches up to 10^{-3}. It means that, one out of a thousand envelopes will be lost, showing the impact in the final system.

In summary, last section allows the evaluation of TLR for different protocol parameters, such as the number of slots, the arrival process, the time in coverage (conveyor belt velocity), *etc.*
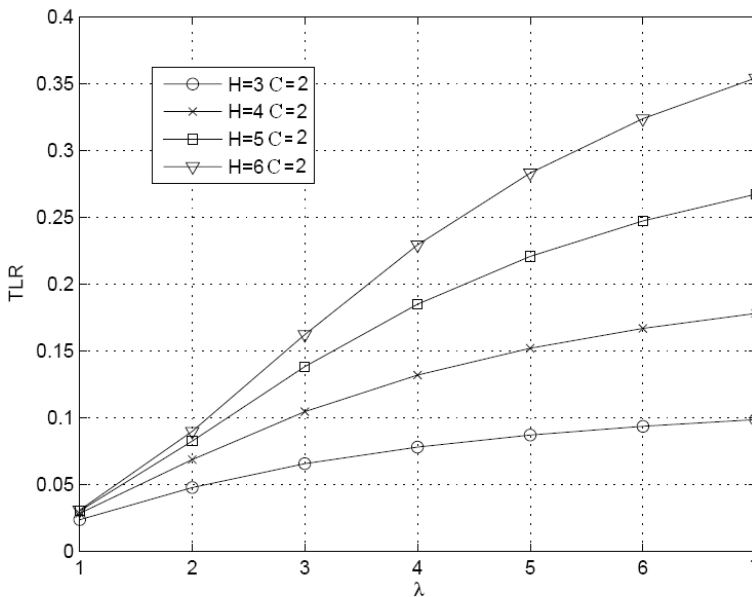
Fig. 10. TLR results for FSA with 8 slots and Poisson arrivals. C=4, and H=3 to H=6
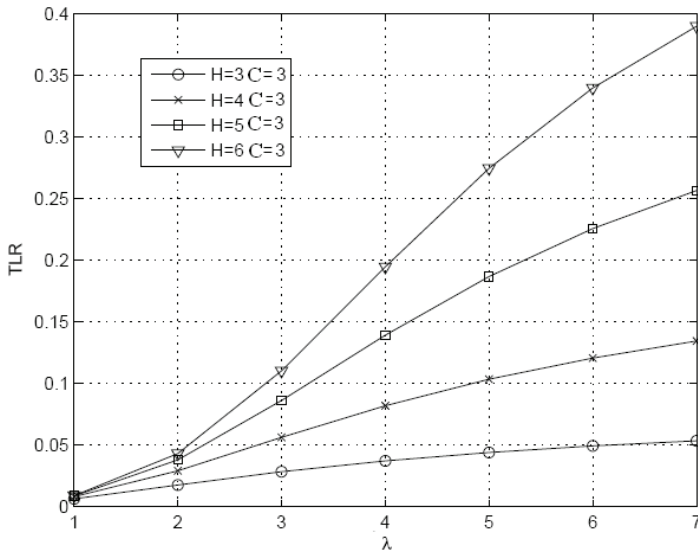
Fig. 11. TLR results for FSA with 8 slots and Poisson arrivals. C=5, and H=3 to H=6
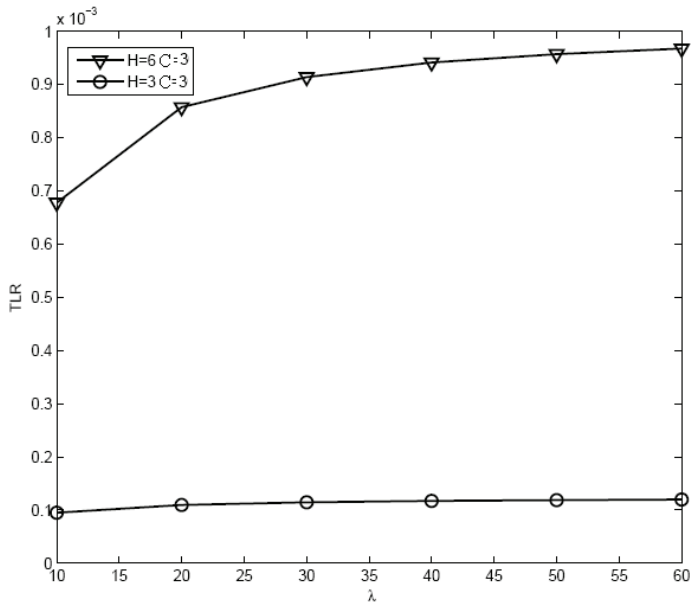
Fig. 12. TLR results for FSA with 64 slots and Poisson arrivals, C=4 and H=3, H=6

6. Conclusions and open issues

This chapter has presented an overview of the RFID identification process and how the RFID systems work in *static* and *dynamic* scenarios. The latter are common in traceability, inventory control, *etc.* Studying the identification process is mandatory to minimize the items that leave the checking areas unidentified. Since collisions are the main factor that produces delay in the RFID identification process, the chapter overviews this phenomenon in the *Medium Access Control* (MAC) layer. The study has been been addressed for passive RFID protocols due to their high market penetration.

The lack of standardization has traditionally been one of the limiting factors for the adoption of RFID technology. This situation has undergone an evolution during the last years, since the EPCglobal Class-1 Gen-2 standard have been widely accepted by RFID companies. The more relevant and adopted EPCglobal specifications have been described along the chapter, in particular, its physical and its anti-collision protocol.

The performance analysis of the identification process has been introduced. On the one hand, the analysis has been focused on *static* scenarios, where identification time has been computed, as well as system throughput. On the other hand, the identification process analysis of *dynamic* scenarios has been oriented to determine the *Tag Loss Ratio*. Configuration of actual implementations of RFID systems could make use of the results achieved to improve their identification process quality.

Finally, some open issues related to identification procedure have not been addressed yet: the analytical characterization of DFSA algorithms, more complex incoming traffics for dynamic systems, as well as considering another types of collisions, such as reader to reader. The study of these issues will be important in the research field of RFID for the next years.

7. Acknowledgments

8. References

Angerer, C., Maier, G., Bueno-Delgado, M.V., Rupp, M., Vales-Alonso, J. (2010), *Recovering from Collisions in Multiple Tag RFID Environments*. In Proc. of International Conference on Industrial Technology, Viña del Mar, Chile.

(a) Bueno-Delgado, M.V., Vales-Alonso, J., Gonzalez-Castaño, F.J. (2009), *Analysis of DFSA Anti-Collision Protocols in passive RFID environments*. In Proc. of 35th Annual Conference of the IEEE Industrial Electronic Society. pp. 2630-2637.

(b) Bueno-Delgado, M.V., Vales-Alonso, J., Egea-Lopez, E., Garcia-Haro, J (2009), *Optimum Frame-length configuration in passive RFID systems installations*. In Proc of

International Workshop on RFID Technology, Concepts, Applications and Challenges. Milan, Italia. pp. 69-77.

EPC Radio-Frequency Identify protocol for communications at 868–960 MHz,Version 1.0.9: EPCglobal Standard Specification, 2004. Available Online at: http://www.epcglobalinc.org/standards.

Finkenzeller, K., (2003) RFID Handbook*: Fundamentals and Applications in Contactless Smart Cards and Identification*, chapters 1–2, 1-7,11-28. 2nd Edition, John Wiley and Sons, Chichester. New York.

Hush, D.R. and Wood, C. (1998), *Analysis of tree algorithms for RFID arbitration*. In Proc. of IEEE International Symposium on Information Theory.

ISO/IEC 1800–6:2003(E), Part 6: Parameters for Air Interface Communications at 860–960 MHz.

Jacomet, M., Ehrsam, A. and Gehring, U. (1999), *Contactless identification device with anti-collision algorithm*. In Proc. of IEEE Conference on Circuits, Systems, Computers and Communications, Athens, Greece, pp. 269–273.

Kemeny, J. G., & Snell, J. L. (1960). *Finite Markov chains*. Princeton, NJ: D. Van Nostrand Company, Inc.

Khasgiwale, R.S., Adyanthaya, R:U., Engels, D.E. (2009), *Extracting Information from tag collisions*. In Proc. of IEEE International Conference on RFID, Orlando USA.

Law, C., Lee, K. and Siu, K. (2000), *Efficient memoryless protocol for tag identification*. In Proc. of the 4th International Workshop on Discrete Algorithms and Methods for Mobile Computing and Communications,. Boston, Massachusetts,pp. 75–84.

Leon-Garcia A. and Widjaja, I. (1996), *Communication Networks: Fundamental Concepts and Key Architectures*, McGraw-Hill, Press, Boston, Chapter 6, part 1, 368-421.

Myung, J. and Lee, W. (2006), *Adaptive binary splitting: A RFID tag Collision arbitration protocol for tag identification*, Mobile Networks and Applications Journal, 11, pp. 711–722.

Schoute, F.C., (1983), *Dynamic frame length ALOHA*, IEEE Transactions on Communications, 31(4), 565–568.

Shen, D., Woo, G., Reed, D.P., Lippman, A.B., Wang, J. (2009), *Separation of Multiple Passive RFID Signals Using Software Defined Radio*. In Proc. of IEEE International Conference on RFID, Orlando USA.

Shih, D.H., Sun, P.L., Yen, D.C., Huang S.M. (2006), *Taxonomy and survey of RFID anti-collision protocols*, Elsevier Computer Communications, 29, 2150-–2166, 2006.

Vales-Alonso, J, Bueno-Delgado, M.V., Egea-Lopez, E., Alcaraz-Espin, J.J, Garcia-Haro, J. (2009), *Markovian Model for Computation of Tag Loss Ratio in Dynamic RFID Systems*. In Proc. of 5th European Workshop on RFID Systems and Technologies, RFID SysTech, Bremen, (Germany).

Weselthier, J.E., Ephremides, A., and Michaels, L.A. (1988), *An exact analysis and performance evaluation of framed ALOHA with capture.* IEEE Transactions on Communications, 37 (2), pp. 125–137.

William J. Stewart, *Introduction to the Numerical Solution of Markov Chains*. Princeton University Press.

On-line references:

Awid, RFID Reader. Documentation available on-line at: http://www.awid.com

Caen,   RFID   Reader.   Documentation   available   on-line   at:
          http://www.caen.it/rfid/index.php
Intermec, RFID Reader. Documentation available on-line at: http://www.intermec.com.
Impinj, RFID Reader. Documentation available on-line at: http://www.impinj.com.
Samsys, RFID Reader. Documentation available on-line at: http://www.samsys.com
Symbol,   RFID   Reader.   Documentation   available   on-line   at: http://   www.tecno-
          symbol.com/
ThingMagic   Mercury4,   RFID   Reader.   Documentation   available   on-line   at:
          http://www.thingMagic.com

3

The Approaches in Solving Passive RFID Tag Collision Problems

Hsin-Chin Liu
National Taiwan University of Science and Technology
Taiwan

1. Introduction

Radio Frequency Identification (RFID) systems are being intensively used recently for automated identification. Every object can be detected as one form of an electronic code. At the beginning, the main purpose of RFID tag usage is meant to be an improvement of barcodes. Besides the fact that an RFID tag does not need line of sight to obtain its ID, the tag is also water and dirt resistant. Moreover, it also has a read-and-writable memory chip, which can store much more data than a barcode, and is difficult to be imitated. The above are the main factors that many enterprises and government associations consider to extensively apply the RFID technology to many applications.

An RFID tag is composed of two major components: an IC to store data and to handle communication processing and an attached antenna to transmit and receive radio signal. There are several types of RFID tags based on the differences of their power sources and communication methods. In general, a passive RFID tag does not have an internal power supply, and cannot work without collecting continuous wave from a reader. Oppositely, an active RFID tag has an attached battery and can communicate with other tags or reader on its own. A semi-passive tag is a mixed of above two types, which has an external battery for its operating power and yet communicates with reader in the same way as a passive tag does.

In an RFID system, a reader is able to communicate with many tags within its coverage. However the tag identification process may fail when multiple tags are sending their data simultaneously. The signals from the tags may interfere with each other and hence the reader may not receive any correct data at all. If this happens, the tags will have to retransmit their data, which wastes the tag reading time and hence degrades the system performance. Such a problem is often called "tag collision" in an RFID system.

To overcome the tag collision problem, researchers are still looking for the most effective anti-collision method to achieve high speed detection with nearly 100% data accuracy ID retrieval. The collision problems are usually classified into two types: the reader collision problems and tags collision problems (Burdet 2004; Dong-Her Shih 2006; Okkyeong Bang 2009). In this chapter, we focus on the latter one.

The tag collision problems are in conjunction with the anti-collision protocols used in various RFID systems, of which the objective is to retrieve a tag's ID accurately with low transmission power, low computational complexity, and minimum time delay. In the

following we will overview a variety of anti-collision methods in solving RFID tag collision problems. Unlike many other surveys of RFID anti-collision methods that are mostly focusing on Time Division Multiple Access (TDMA) schemes, this work elaborates more details of applying other multiple access technologies to the passive RFID systems.

2. Review of anti-collision schemes for passive RFID systems

Multiple access technologies are extensively used to allow multiple communications to coexist in the communication channel with little interference with each other in modern communication systems. In an RFID system, a reader usually communicates with many tags within its read range, which means that all the reader and tag communications share the same air medium as their communication channel. Thus a variety of multiple access technologies have been used in recent RFID systems, such as Time Division Multiple Access (TDMA), Code Division Multiple Access (CDMA), Spatial Division Multiple Access (SDMA), Frequency Division Multiple Access (FDMA), and the hybrid multiple access technologies. In the following, we overview the multiple access technologies that have been proposed. Fig. 1 illustrates the category of multiple access schemes used in different RFID systems.
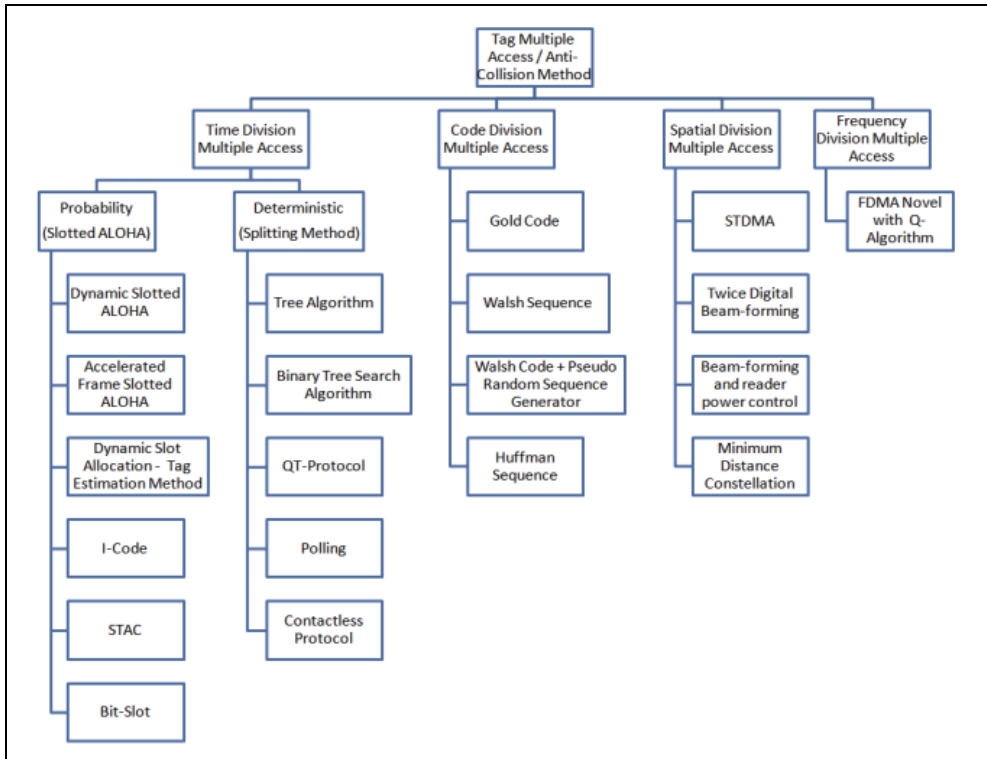
Fig. 1. Map of tag anti-collision schemes in RFID system

2.1 Time Division Multiple Access (TDMA) based schemes

With the TDMA technology, the reader and tag communications can use the same frequency in the same reader coverage, and each tag response can be differentiated by the time interval that it used. This kind of multiple access technology is the most popular RFID tag anti-collision schemes and can easily jointly incorporate with other multiple access technologies. As seen in Fig. 1, the RFID tag anti-collision schemes using TDMA technologies can be divided into two categories, the deterministic schemes and the probabilistic schemes (V. Sarangan 2008). The deterministic schemes are usually referred to as binary tree-search based schemes. The schemes are deterministic because each root-to-leaf path denotes a unique tag ID and all IDs can be retrieved once all branches are completely searched. On the other hand, the probabilistic schemes are usually referred to as slotted ALOHA based schemes. Each tag ID in the probabilistic schemes will have a chance to be retrieved successfully; however, there is a possibility that some tags may not be accessed due to recurrent collisions. Other than the above two categories, some hybrid schemes are also proposed; for instance, Bonuccelli et al. proposed a tree slotted ALOHA (TSA) is proposed in (Bonuccelli et al. 2006), and Shin et al. also proposed another hybrid tag anti-collision scheme (Shin et al. 2007).

Because the fundamental binary tree-search scheme interrogates one branch completely to obtain a tag ID, it is naturally slow. Let $L(N)$ denote the average number of iterations that are required to retrieve one tag ID among N tags. The $L(N)$ can be calculated as Eq. (1) (Finkenzeller 2004).

$$L(N) = \log_2 N + 1 \tag{1}$$

Obviously the value $L(N)$ becomes large when there are many tags in the reader's coverage. Hence, a variety of tree-search schemes have been proposed to mitigate this problem. The tree-search schemes are further categorized into two major types: Binary Tree Walking schemes and Query Tree schemes (Dong-Her Shih 2006; Okkyeong Bang 2009).

Compared with the tree-search scheme, the slot ALOHA schemes usually interrogate tags faster. Because slotted ALOHA scheme segments the reader and tag communications into many time slots. Each time slot can be empty (which means no tag response in the time slot), collided (which means multiple tag responses in the time slot), or successful (which means exactly one tag response in the time slots). Because using a pure TDMA scheme, only one tag response can be read by the reader in a time slot. The performance of the schemes is hence determined by the probability of occurrence of a successful time slot. The probability of observing a successful time slot P_{succ} can be written as Eq. (2).

$$P_{succ} = n_{tag} \left(\frac{1}{n_{frame}} \right) \left(1 - \frac{1}{n_{frame}} \right)^{n_{tag}-1}, \tag{2}$$

where the n_{tag} denotes the number of tags in the reader's coverage, and n_{frame} denotes the number of slots that a tag can select, which is also called as a frame size. When the number of tags in the reader's coverage is large, it is reasonable to assume that the distribution of the probability of receiving a tag response is a Poisson distribution. Under such a circumstance, the optimal system performance (or throughput) of a slotted ALOHA scheme can achieve as 36.8% (that is, $MAX(P_{SUCC}) = 36.8\%$) when $n_{frame} = n_{tag}$ (Proakis 1995; Finkenzeller 2004). Apparently, the ratio of the frame size to the number of tags in the reader's coverage determines the system throughput. As the amount of tags that needs to be read is unknown

in advance for most cases, to choose a proper frame size is a key factor that can determine the system performance. Moreover, the proper frame size is usually time-variant because the number of unread tags decreases in an inventory process, which gives a challenge on choosing the most suitable frame size (Wang & Liu 2006). Since several papers have addressed this kind of research comprehensively (Dong-Her Shih 2006; Okkyeong Bang 2009), we will not describe further details on the TDMA schemes in this chapter but refer readers to those papers.

2.2 Code Division Multiple Access (CDMA) based schemes

As mentioned earlier, the TDMA based anti-collision schemes can only retrieve one tag's ID at one time slot. In order to significantly increase the system throughput, incorporating the TDMA technology with other multiple access technology is necessary.

The CDMA technology has been extensively used in many modern communication systems. The CDMA schemes allow multiple communications to coexist in the same medium using the same time and frequency resources. The CDMA technology is usually categorized into two types: frequency hopping CDMA (FH-CDMA) and direct sequence spreading CDMA (DS-CDMA). Because a passive tag is unable to select the communication frequency actively but only backscatters the radio signal emitted from a reader, the FH-CDMA technology is hence not suitable for the passive RFID system. The DS-CDMA technology however uses a spread sequence as the signature of a signal source. Different signal sources can transmit their signals at the same time, and the receiver is able to separate each signal from the received signals by dispreading the received signals with its corresponding signature.

There are a variety of spreading sequences for different DS-CDMA applications. The sequences are generally separated into two groups. One is called "orthogonal sequences", and the other is called "pseudo random sequences". For instance, the well-known Walsh code is one of the orthogonal sequences and another well-known Gold code is one of widely used pseudo random sequences. Most orthogonal sequences require perfect synchronization (that is, each code should arrive at the receiver at the same time) to preserve their mutual orthogonality. On the other hand, the perfect synchronization is not required for pseudo random sequences to be low cross-correlated; however, the pseudo random sequences are not mutually orthogonal. Due to the low cross-correlation value, a near-far problem can be caused if the received powers from the signal sources are different. Another kind of spreading sequence is called shift-orthogonal sequences. A shift-orthogonal sequence can maintain orthogonality with a different shift-orthogonal sequence and with a delayed version of itself. Thus, the sequences do not require synchronization and can resist the near-far effect. A Huffman sequence is one example of the shift-orthogonal sequences.

A passive tag can generate a desired signal by changing its antenna reflection coefficient to produce the proper backscatter signal. This is usually referred to as backscatter modulation. Using the backscatter modulation, the tag can easily produce a desired coded signal.

Several studies on using CDMA technology onto RFID systems have been revealed (Fukumizu et al. 2006; Rohatgi 2006; Wang et al. 2006; Maina et al. 2007; Liu and Guo 2008). Rohatgi and Wang et al. both proposed methods of applying Gold sequences to RFID systems. However, due to the non-zero cross-correlation of each spreading sequence, the performance of this method deteriorates when there exists power inequality amount the tag backscatter signals. In general, a passive tag merely returns its response by backscattering the incident continuous wave, which is emitted from a reader. The strength of a received tag backscatter signal is determined by a variety of factors, including the power of the incident

continuous wave, the radar cross section (RCS) of the tag, the polarization of the tag antenna, the propagation loss in the tag-to-reader link, and so on. In order to mitigate the near-far problem, a sophisticated power control scheme is required. Unfortunately, the implementation of power control mechanism on each individual tag is impractical due to the limitations of the tag power and cost.

Maina et al. apply Walsh codes to spread the tag backscatter signals (Maina et al. 2007), which allows multiple tags to respond simultaneously. However, the paper does not reveal how to assign the spreading sequences to the tags, which reply in the same time slot. In addition, the demodulation and decoding process are not clearly mentioned in the paper.

Fukumizu et al. presents a scheme by applying both Walsh code and pseudo random sequence to solve the tag collision (Fukumizu et al. 2006). The approach is very similar to a modern wireless transmitter, such as a mobile phone. However, the scheme may not be suitable for a RFID system with passive tags due to the complexity constraint of the passive tags.

Liu and Guo proposed a method by applying Huffman sequences, which is nearly orthogonal to its delay version, to passive backscatter signals (Liu & Guo 2008). The Huffman sequences are more near-far resistant and can preserve code orthogonality without precise synchronization of received signals. Unlike aforementioned system, where each tag uses a unique spreading sequence, the proposed RFID anti-collision scheme uses only one Huffman sequence system for all tags. Consequently the reader can have the knowledge of the Huffman sequence used to spread the tag backscattering signal *a priori*, which can significantly reduce the complexity of reader design. Furthermore the tag backscatter signal spread by the sequence can be easily generated using a set of preset circuit with corresponding reflection coefficients, because only a Huffman sequence is used in a RFID system. However, no experimental results but simulation results are provided in (Liu & Guo 2008). In practice, in order to recover the backscatter Huffman sequence, the reader requires high sensitivity and low phase noise, which is quite a challenge in reader design.

It is noteworthy that all CDMA based anti-collision methods (in physical layer) need to incorporate with proper TDMA methods (in Media Access Control layer) to optimize the performance of the system throughput. Up-to-now scant researches dedicating in this issue have been found, which makes it an interesting future research topic. The details of the cross-layer design, however, are beyond the scope of this chapter.

2.3 Space Division Multiple Access (SDMA) based schemes

SDMA is a relatively new technology in modern communication systems compared with the rest three multiple access schemes. Typically, the SDMA architecture is capable of providing a collision-free access to the wireless channel and a qualitative delay-bounded communication in real time for delay sensitive applications. Because the SDMA method divides the available channels in spatial domain, the system can significantly increase the channel capacity of the same frequency and the same time slot.

In general, a SDMA scheme separates the coexisting transmission sources via the angle of arrival (AOA) of each signal source, which is also called as spatial signature. In the passive RFID system, this property is especially useful because it does not require any change of the physical communication protocol but use a reader with array antennas.

Several schemes using SDMA has been proposed (Abderrazak et al. 2006; Liu et al. 2007; Yu et al. 2008). In (Abderrazak et al. 2006; Yu et al. 2008), a reader employs multiple directive antennas (Abderrazak et al. 2006) or uses twice digital beam-forming (Yu et al. 2008) to

segment the reader coverage into several subsets. The tags in different subsets can be read in the same time; hence the throughput can be multifold of that of a conventional RFID system, where only one antenna is activated in the same time.

The trade-off between the system throughput and the complexity of the reader requires more attention, which is not well-addressed in the papers. Similar to CDMA methods, the technical challenge of seamlessly combining of TDMA and SDMA is remained unsolved. For instance, if the tags are not uniformly distributed in all subsets, the time slot allocation should be designed accordingly to optimize the system throughput. Thus it is expected that such a cross-layer anti-collision design will be an interesting research topic in the near future.

2.4 Frequency Division Multiple Access (FDMA) based scheme

The FDMA technology allows a number of transmission channels to work together at the same time by using different operating frequency. In a passive RFID system, the signal from the reader is usually broadcasted in some operating frequencies to provide power and reader's command to passive tags. A tag not only receives the power from the reader broadcasted signal but also utilizes the signal as the carrier of its modulated backscatter signals. Indeed, a tag can receive any signals within its operation frequency band and use the received signal as the carrier to backscatter its modulated signal. Thus it is possible to take the advantage of such a property to apply the FDMA technology to passive RFID systems.

The FDMA technology has been used in the ISO 18000-3 mode 2 HF RFID system (ISO/IEC18000-3 2004), which has 8 reply channels for simultaneous communication with 8 different RFID tags; however the FDMA technology has not yet been adopted in any passive UHF RFID standards.

(Liu et al. 2007) proposed a method that can allow a tag response happens in the different frequency band, which is called as multi-carrier backscatter. In (Liu & Ciou 2009) a feasible deployment similar to a cellular system is proposed as shown in Fig. 2. Each continuous wave emitter (CWE) occupies a different frequency which is different with that of its neighbor CWEs. Each tag in a CWE's coverage uses the continuous wave emitted from the CWE as the carrier of its modulated backscatter signal. In that way, a reader is able to correctly receive multiple tag response simultaneously by separating each individual tag response according to its carrier frequency.

Incorporating with the original framed slotted ALOHA scheme, the system throughput is nearly doubled because the idle time slots can be fully utilized as successful slots. However, the system still allows to retrieve one ID tag in a time slot. An optimal jointly combining TDMA and FDMA scheme, however, is not investigated in (Liu and Ciou 2009). With a proper protocol develop, it is reasonable to believe that the system throughput can be multi-fold faster than the current system. Another problem of the scheme is the system cost issue, which is expected to be reduced once the technology is more mature.

3. Conclusions

The RFID technology is a key technology toward the goal of internet of things. As RFID systems are pervasively deployed, our daily life will highly depend on the technology. High system reliability and performance will be demanded. Consequently the tag collision problems will keep drawing researcher's attention. Up-to-now most literatures use TDMA
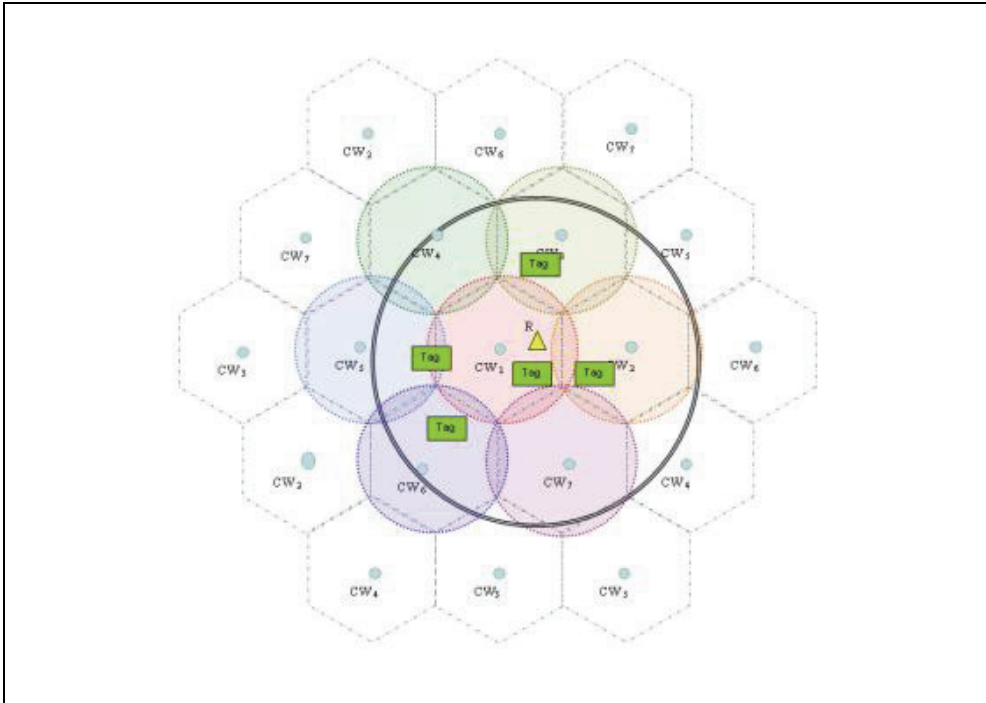
Fig. 2. A possible deployment of a multi-carrier RFID system, where R denotes the reader and CW*i* denotes that the CWE using the *i*-th frequency band.

based method to solve this problem. However, due to the nature of TDMA technology, only one tag ID can be retrieved in a time slot. In order to rapidly improve the system performance, similar to other modern communication systems, jointly using other multiple access schemes are required. So far, most papers deal with different multiple access schemes on RFID systems individually. To optimize the system throughput, it requires more advanced technologies such as cross-layer optimization technology. A passive RFID system, unlike other communication system, is an unbalanced client–server (tag-reader) structure, where the passive tag has power and cost constraints and hence can only perform low complexity anti-collision algorithm. The property results in the anti-collision scheme for passive RFID system a unique and challenging problem.

4. Acknowledgements

5. References

Abderrazak, H., et al. (2006). A Transponder Anti-collision Algorithm Based on a Multi-Antenna RFID Reader, *Proceedings of 2nd Information and Communication Technologies, ICTTA '06.* , pp. 2684-2688.

Bonuccelli, M. A., et al. (2006). Tree slotted ALOHA: a new protocol for tag identification in RFID networks, *Proceedings of 2006 International Symposium on a World of Wireless, Mobile and Multimedia Networks*, pp. 603-608.

Burdet, L. A. (2004). RFID Multiple Access Methods, pp.15.

Dong-Her Shih, P.-L. S., David C. Yen, Shi-Ming Huang (2006). Taxonomy and survey of RFID anti-collision protocols, *Computer Communications*, Vol.29, pp.17.

Finkenzeller, K. (2004). RFID Handbook: Fundamentals and Applications in Contactles Smart Cards and Identification, Wiley.

Fukumizu, Y., et al. (2006). Communication Scheme for a Highly Collision Resistive RFID System, *IEICE TRANS. FUNDAMENTALS*, Vol.E89–A, No.2, pp.408-415.

ISO/IEC18000-3 (2004). RFID for item management – Air interface, Part 3: Parameters for Air interface communications at 13.56MHz, ISO/IEC Std. 18000-3, 2004.

Liu, H.-C., et al. (2007). A Frequency Diverse Gen2 RFID System with Isolated Continuous Wave Emitters, *Journal of Network*, Vol.2, No.5, pp.54-60.

Liu, H.-C. and Ciou, J.-P. (2009). Performance Analysis of Multi-Carrier RFID Systems, *Proceedings of 2009 International Symposium on Performance Evaluation of Computer and Telecommunication Systems*, pp. 112-116, Istanbul, Turkey.

Liu, H.-C. and Guo, X.-C. (2008). A Passive UHF RFID System with Huffman Sequence Spreading Backscatter Signals, *The Internet of Things, LNCS 4952*, pp.184-195.

Liu, Z., et al. (2007). A Novel Passive UHF RFID Transponder with Space Division Anti-collision Algorithm, *Proceedings of 7th International Conference on ASIC, 2007. ASICON '07.* , pp. 878-881.

Maina, J. Y., et al. (2007). Application of CDMA for anti-collision and increased read efficiency of multiple RFID tags, *Journal of Manufacturing Systems*, Vol.26, No.2008 The Society of Manufacturing Engineers. Published by Elsevier Ltd. All rights reserved,pp.7.

Okkyeong Bang , J. H. C., Dongwook Lee ,Hyuckjae Lee (2009). Efficient Novel Anti-collision Protocols for Passive RFID Tags, *Auto-ID Labs White Paper WP-HARDWARE-050*,pp.30.

Proakis, J. G. (1995). *Digital Communications*, McGraw Hill, Malaysia.

Rohatgi, A. (2006). Implementation and Applications of an Anti-Collision Differential-Offset Spread Spectrum RFID System, *Georgia Institute of Technology*.

Shin, J.-D., et al. (2007). Hybrid Tag Anti- Collision Algorithms in RFID Systems, *Proceedings of ICCS, Part IV, LNCS 4490*,pp.693-700.

V. Sarangan , M. R. D., S. Radhakrishnan (2008). A framework for fast RFID tag reading in static and mobile environments, *Computer Networks*, Vol.52, No.2007 Elsevier B.V. All rights reserved, pp.16.

Wang, L.-C. and Liu, H.-C. (2006). A Novel Anti-collision Algorithm for EPC Gen2 RFID Systems, *Proceedings of 3rd International Symposium on Wireless Communications Systems (ISWCS'06)*, pp., Valencia, Spain.

Wang, P., et al. (2006). The Design of Anti-collision Mechanism of UHF RFID System based on CDMA, *Proceedings of IEEE Asia Pacific Conference on Circuits and Systems, 2006. APCCAS 2006.* , pp. 1703 1708.

Yu, J., et al. (2008). A Novel RFID Anti-collision Algorithm Based on SDMA, Proceedings of 4th International Conference on Wireless Communications, Networking and Mobile Computing, 2008. WiCOM '08. , pp. 1-4.

4

Electronic and Mac Protocol Characterization of RFID Modules

Nasri Nejah, Kachouri Abdennaceur, Andrieux Laurent and Samet Mounir
[1]*LETI-ENIS, B.P.868-3018- SFAX*
[2]*LATTIS-IUT, BLAGNAC TOULOUSE -*
[1]*Tunisia*
[2]*France*

1. Introduction

Radio Frequency IDentification (RFID) is an advanced automatic identification technology, relying on storing and remotely retrieving data using devices called RFID tags or transponders. An RFID tag is a small object that can be attached to or incorporated into a product; animal or person (rami khouri, 2007). The application of RFID in industry warehouse, monitoring system and personal life brings researchers and engineers to focus on it. In this chapter, we address two important issues in an RFID system: Electronic and MAC protocol characterization to avoid reader-reader and reader-tag collisions in a dense RFID network.

In the first part, we present an operational description of RFID hardware components especially RFID antenna.

Current generation RFID systems address the multi-reader coordination problems, effectively where multiple readers are rarely used in the same physical layers (Sok-Won Lee, 2005). For thus, in the second part we present a survey of several collision problems that occurs when multiple readers are used within close proximity of each other. Furthermore, we evaluate the technique of medium access control to avoid collisions in multi-readers scenarios using Network Simulator (NS2).

Finally, we present a CSMA-based MAC protocol to avoid reader-reader and reader-tag collisions in a dense RFID network.

2. Recall

RFID systems consist of the following components (Simson Garfinkel et al., 2005) (Thomas Huault, 2006):

2.1 RFID tag

RFID tag consists of a microchip programmed with information about a product and a coupling element - an antenna. Most tags are only activated when they are within the interrogation zone of the interrogator.The size of the tag depends on the size of the antenna, which increases with range of tag and decreases with frequency.

As schowing in figure 1 the architecture of RFID tag is constituted by modulation / demodulation bloc, a local memory containing information about product stored in data base, and a micro-controller that represent the intelligent part of tag.
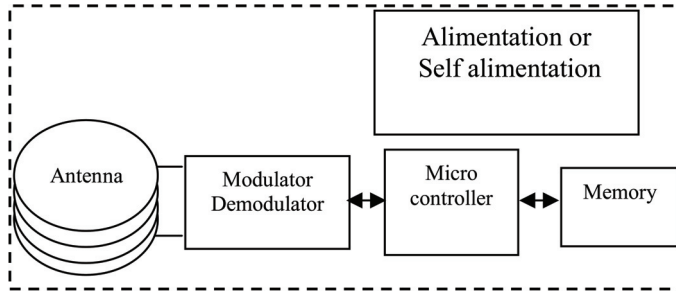
Fig. 1. Architecture of RFID tag

2.2 RFID interrogator

Depending on the application and technology used, some interrogators not only read, but also remotely write to, the tags. For the majority of low cost tags, the power to activate the tag microchip is supplied by the reader through the tag antenna when the tag is in the interrogation zone of the reader.

Generally the reader is constituted by (figure 2):

- An analog part regrouping:
    - A local oscillator accorded on the frequency of a transmitted signal.
    - A modulator/demodulator to transmit or to receive the numeric messages.
    - An amplifier adapted on the antenna of emission / reception.
- A numeric part regrouping:
    - A micro-controller for the management of communication protocols, collisions…
    - A communication interface.
    - A local memory.
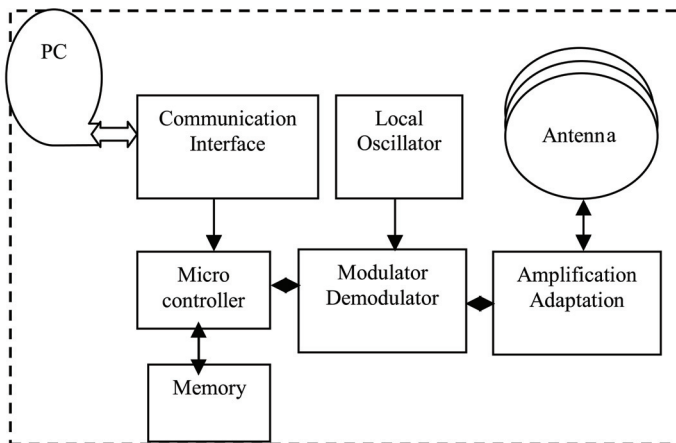
Fig. 2. Architecture of RFID integrator

2.3 Unit of collection and management of information

This unit is the interface needed between the interrogator and the existing company databases and information management software.It permit:

– Filtering and validation of raw data
– Fusion of data sent by different sensors
– System Management (monitoring, service levels, ...)
– Self-healing

The middleware RFID is constituted by informatics equipments and software of management, which convert multiple inputs in data of identification.

3. Different types of RFID tags

In RFID systems, the tags that hold the data are broken down into two different types (Cristina TURCU, 2009): Passive and Active. Passive tags do not have batteries and have indefinite life expectancies. Active Tags are powered by batteries and either have to be recharged, have their batteries replaced or be disposed of when the batteries fail.

RFID systems can use a variety of frequencies to communicate, but because radio waves work and act differently at different frequencies, a frequency for RFID system is often dependant on its application.So it is not a technology where 'one size fits all' applications.

Three primary frequency bands are being used for RFID(Thomas Huault,2006):

• Low Frequency (125/134KHz) – used for access control, animal tracking and asset tracking.
• High -Frequency (13.56 MHz) – Used where medium data rate and read ranges up to about 1.5 meters are acceptable. This frequency also has the advantage of not being susceptible to interference from the presence of water or metals.
• Ultra High-Frequency (850 MHz to 950 MHz) – offer the longest read ranges of up to approximately 3 meters and high reading speeds.

In the same contexte There are two basic types of chips available on RFID tags: Read-Only and Read-Write: Read-only chips are programmed with unique information stored on them that can not be changed . in Read-Write chips, the user can add information to the tag or write over existing information when the tag is within range of the reader. Read-Write chips are more expensive that Read Only chips.

The table below highlights the characteristics these different tags(Gérard-André Dessenne, 2005):

Active or passive	Other Classifications

Passive (no battery)
    Smaller, Lighter
    Shorter range (<3m)
    Smaller data storage
    Lower cost
	Data storage (Programming)
	    Read Only
	    Write once
	    Read/write

Active (with battery)
    Larger, Heavier
    Longer range (up to 100m)
    Larger data storage
    Higher cost
	Frequencies
	    Low –135 kHz
	    VHF –13.5 MHz
	    UHF –860MHz
	    Microwave –2.4 GHz

Table 1. RFID Tags Types

4. Physical survey and modeling of the RFID antenna

4.1 Physical principle

The physical principle of the RFID technology is based on the propagation of electromagnetic wave in the aerial environment T o illustrate this principle, we consider an oriented spindly circuit C, traveled by a permanent current of I intensity.

It creates in a M, point of the space a magnetic induction B (figure 3). According to the laws of Biot and Savart, if dl is an element of the circuit in P point, we can calculate the magnetic induction B in M(Patrick PLAINCHAULT, 2005).
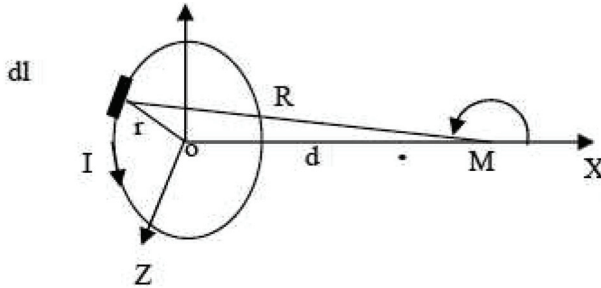
Fig. 3. Principle of magnetic fields
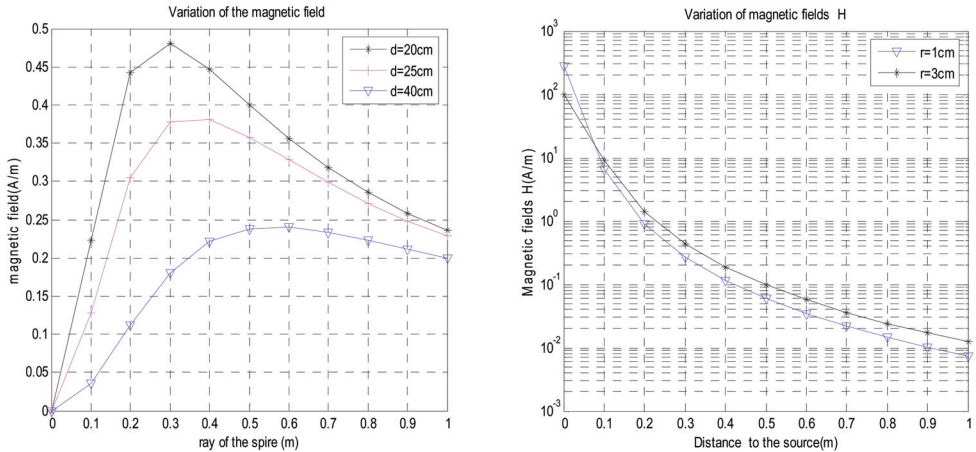
Fig. 4. Variation of the magnetic field vs distance to the source and the ray of spire

The magnetic field is expressed by:

$$\vec{B}(Tesla) = \frac{\mu_0}{4\pi} \oint \frac{\vec{I} \wedge \vec{U}}{R^2} \, dl \tag{1}$$

$$\vec{B} = \mu_0 \vec{H} \tag{2}$$

$$B = \frac{\mu_O . N.I}{2} \cdot \frac{r^2}{(r^2 + d^2)^{32}} \tag{3}$$

N: the number of spire
I: current (A)
d: distance from source (meter)
r: ray (meter)
Under figure 4, we deduct that:
– For low range of communication the magnetic field in the middle of the antenna will be more intense for a low ray.
– To establish a communication for long distances it's necessary to use an antenna of a greater ray.
– The optimal ray (r) for which the magnetic field is maximal for stationary d: $r=d\,\overline{\boxed{2}}$

In order to improve the gotten results, in the next part we are going to present the equivalent electronic circuit of the antenna tag. Then, we present an approach for estimating and determination the Power consumption.

4.2 Electronic modeling of the antenna of a RFID tag

One of the major constraints is the attenuation of signals due the bad choice of antenna parameters. For thus, it is necessary to give an electronic model of the antenna that approaches to the reality. Then anticipate with accuracy the behavior of antenna by the use of simulation tools.

In this subsection, we discuss modifications done to the equivalent circuit of the RFID tag antenna.

Generally the equivalent electronic circuit of the tag antenna is composed of a pure inductance due to the constitution of a coil (L2s), a purely ohmic resistance (R2s), and a generator of tension in presence of a fields magnetic (Patrick PLAINCHAULT,2005)(Paret D.,2003):
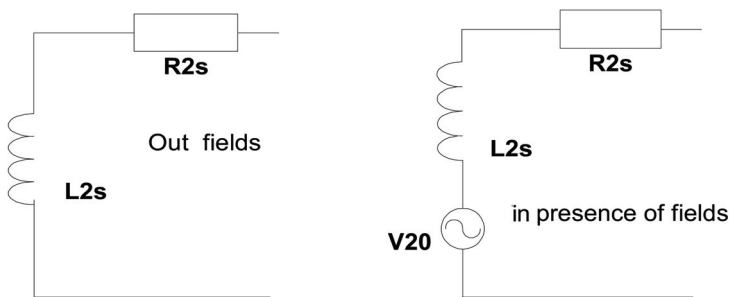
Fig. 5. Equivalent Circuit of antenna

The proper frequency of resonance of this circuit is:

$$L2s \times R2s \times w2 = 1. \tag{4}$$

The quality coefficient is:

$$Q2s = \frac{L2s \times w}{R2s} \tag{5}$$

The V20 (t) tension:

$$V20(t) = -\frac{d\varphi_2(t)}{dt} = -\frac{d}{dt}\int_{S_2} B.dS_2 = -\mu \int_{S_2} H.dS_2 \tag{6}$$

With:

$$\varphi_2(t) = M.I_1(t) \tag{7}$$

M: mutual inductance between the reader and the tag;
I 1 (t): current traveling the reader's antenna;
The value of the mutual M is:

$$M = \mu \frac{r^2}{2(r^2+d^2)^{3/2}}.N_1.N_2.S_2 \tag{8}$$

If the coils of the antenna are accorded to a capacity in parallel, the equivalent circuit of the antenna is showing in figure 6:
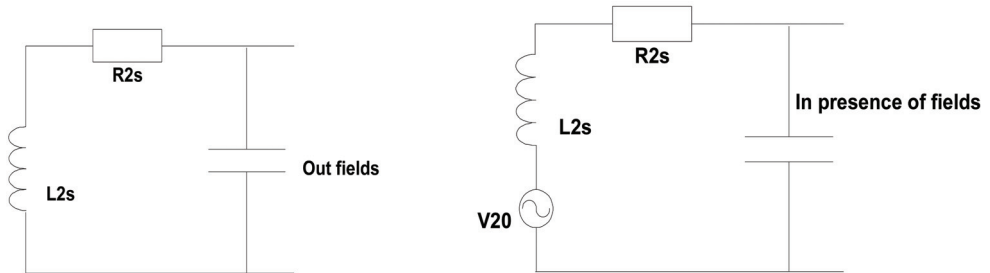
Fig. 6. Accorded antenna of RFID tags

This circuit is equivalent to an active dipole constituted by a generator of tension V20(t), and an internal impedance of Zie given by the following formula(Nejah NASRI et al.,2008):

$$z_{ie} = \frac{(R_{2s} + j(L_{2s}.w)).\dfrac{1}{jCw}}{R_{2s} + j(L_{2s}.w) + \dfrac{1}{jCw}} = \frac{R_{2s} + j(L_{2s}.w)}{(1 - L_{2s}.w^2.C) + jR_{2s}.C.w} \tag{9}$$

If the tag is accorded on the frequency of resonance fc:

$$L_{2s}.C.w_c^2 = 1 \tag{10}$$

As a result:

$$z_{ie} = \frac{1 + j(\dfrac{L_{2s}.w}{R_{2s}}).w_c}{jC.w_c} \tag{11}$$

However:

$$Q_{2s} = \frac{L_{2s}.w}{R_{2S}} \tag{12}$$

This value is always very big in relation to 1; it comes therefore:

$$z_{ie} = \frac{jQ_{2s}}{jCw_c} = Q_{2s}(L_{2s}.W_c) \tag{13}$$

Finally the equivalent circuit of the complete assembling of a RFID tag "antenna accorded with integrated circuit is given by figure 7:
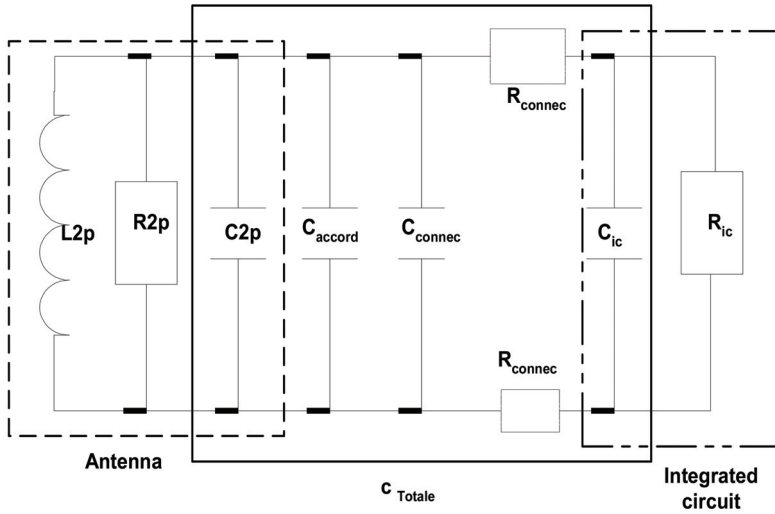
Fig. 7. Complete antenna of a RFID tag

We consider that L2p=L2s, Cp=Caccord+Cic+Cconnec+C2p
With:
C2p: Parallel capacity of the spool of the antenna;
Caccord: Okay capacity;
Cconnec: Parallel capacities of connection;
Cic: Capacity of entrance of the circuit integrated;
Ric : Resistance of input of the circuit integrated;
The value of tension vic applied to the integrated circuit is given by the following formula:

$$v_{ic} = \frac{R_{ic}//C_p}{Z_{L_2p} + (R_{ic}//C_p)} v_{20} = \frac{1}{1 + (R_{2s} + jL_2s.w)(\dfrac{1}{R_{ic}} + jC_p.w)} v_{20} \tag{14}$$

With:

$$v_{20} = -jw.M.I_1 = -jw.B_d.N_2.s_2 \tag{15}$$

Therefore:
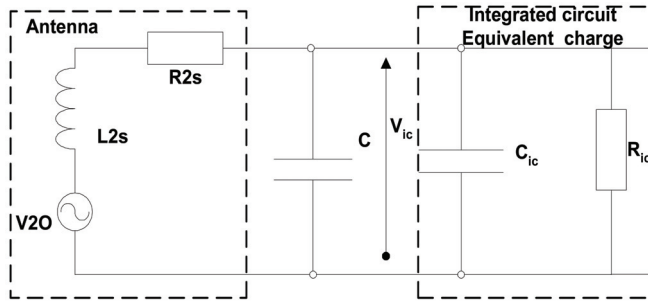
Fig. 8. Induced tension v_{ic} in the transponder

$$v_{ic} = \frac{-jw.M.I_1}{1+(R_{2s}+jL_{2s}.w)(\frac{1}{R_{ic}}+jC_p.w)} = \frac{-jw.B_d.N_2.s_2}{1+(R_{2s}+jL_{2s}.w)(\frac{1}{R_{ic}}+jC_p.w)} \quad (16)$$

$$v_{ic} = \frac{-jw.M.I_1}{\sqrt{(1-+L_2s.C_p.w^2+\frac{R_{2s}}{R_{ic}})^2+(\frac{L_2s.w}{R_{ic}}+R_{2s}.C_p.w)^2}} = f(w) \quad (17)$$

This equation summarizes the reality of relations that exists mathematically between the various elements of equivalent circuit of antenna.
The coefficient quality is given by the following formula:

$$Q_{2s} = \frac{L_{2s}.w}{R_{2S}} = \frac{1}{R_{2s}.C.w} \quad (18)$$

Figure 9 shows the variation of tension induced in the transponder versus the inductance of the antenna and coefficient of coupling. Curves have been traced for the following values: I1 = 0.5 A; R_{ic} = 2 kQ; R2s = 1Q; L1 = 1µH;f=13,56 MHz
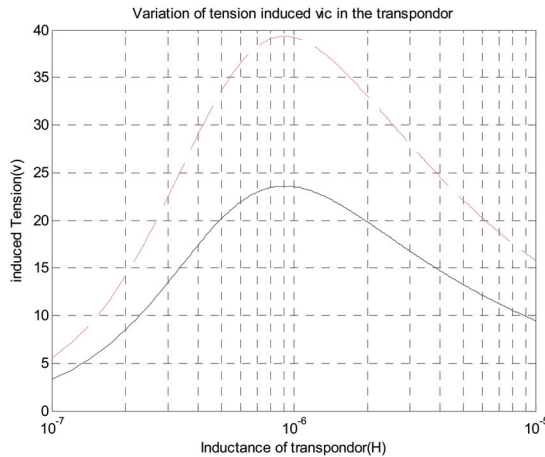
Fig. 9. Variation of tension induced v_{ic} in the transponder

According to this curve we notice that: the induced Tension in the transponder is maximal for a certain value of the inductance.

This type of simulation permits us to determine the optimal value of the inductance of the antenna.

5. Power consumption

For the design of RFID systems, the power consumption has to be taken into account. For thus, to minimize the losses of energy provided by the reader and to get important range of working, it's necessary that the impedance of the integrated circuit of the RFID tag (Ric), be equal to the value of the impedance of the source providing the energy (Zie)(Nejah NASRI, 2008). The following figure presents the condition of impedance adaptation:
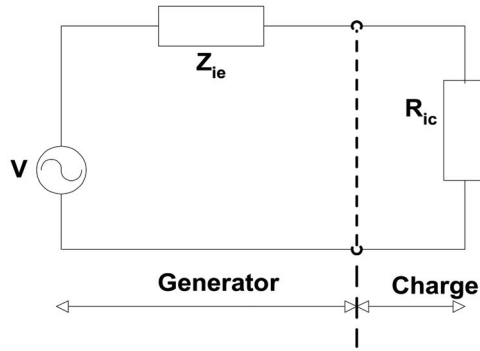
Fig. 10. Condition of power adaptation

As:

$$L_{2s} = L_{2p} \tag{19}$$

$$Z_{ie} = R_{ic} = (L_{2s}.w)Q_{2s} \tag{20}$$

So:

$$L_{2s} = \frac{R_{ic}}{w.Q_{2s}} \tag{21}$$

It is necessary to have a global capacity parallel Cp therefore, as:

$$L_{2p}.C_p.w = 1 \tag{22}$$

5.1 At the level of transponder

RFID tag (passive or semi passive) must provide the sufficient power to produce a signal of the return that the reader can detect. Therefore, the range transmission of a passive system depends on:

Pr: Power of the reader (typically 1 watt).

Gr: gain of the reader's antenna (typically 6 dBi).

Gt: gain of the tag's antenna (1 dBi).

Et: efficiency of the modulator (typically -20dB)
Pt: necessary power for the tag (typically 100 mW or -10 dBm).
RFID system well conceived will be limited by the power available to the tag. This power is given by the following formula:

$$P_t = P_r.G_r.G_t.\left(\left(\frac{\lambda}{4\pi d}\right)\right)^2 \tag{23}$$

5.2 At the level of Reader
Considering the power radiated known as Pa. This radiated power is dissipated in the equivalent resistance of the antenna. The radiated power is expressed by (Nejah NASRI, 2008):

$$P_a = \frac{1}{2}.R_{ant}.I_{a2} \tag{24}$$

$$R_{ant} = \frac{320.\pi^4}{\lambda_{p4}}.(N_1.S_1)^2 \tag{25}$$

With
Rant: Equivalent radiance resistance.
I_1: The current crossing this equivalent resistance.
N_1: Number of spires of the reader's antenna.
S_1: The surface of the reader's antenna.
λ_P: the length of wave of the bearer
As a result:

$$P_a = \frac{320.\pi^4}{\lambda_{p4}}.\pi^2.N_1^2.r_1^4.I_{a2} \tag{26}$$

While taking account of the magnetic induction to the center of the antenna for α = π/2.

$$B_0 = \frac{\mu_0.N.I_a}{2}.\frac{1}{r_1} \tag{27}$$

The power becomes:

$$L_{2p}.C_p.w = 1 \tag{28}$$

$$P_a = \frac{320.\pi^6.\mu_{04}}{\lambda_{p4}}.\frac{N_1^6}{(2.B_0)^4}..I_{a6} \tag{29}$$

To the resonance, the dissipated power in the charges is:

$$P_1 = \frac{L_1.w_P}{Q_1}.I_a^2 \tag{30}$$

To the resonance, the dissipated power in the charges is:

$$P_1 = \frac{L_1.w_P}{Q_1.N_1^2} \cdot \sqrt[3]{\frac{P_a}{\frac{320.\pi^6}{\lambda_{P4}}}} \cdot (2\frac{B_0}{\mu_0})^4 \tag{31}$$

Or the current that must be provided by the reader's amplifier is:

$$I_1 = \frac{1}{N_1} \cdot \sqrt[6]{\frac{P_a}{\frac{320.\pi^6}{\lambda_{P4}}}} \cdot (2\frac{B_0}{\mu_0})^4 \tag{32}$$

For a transponder operating in 13, 56 MHz:
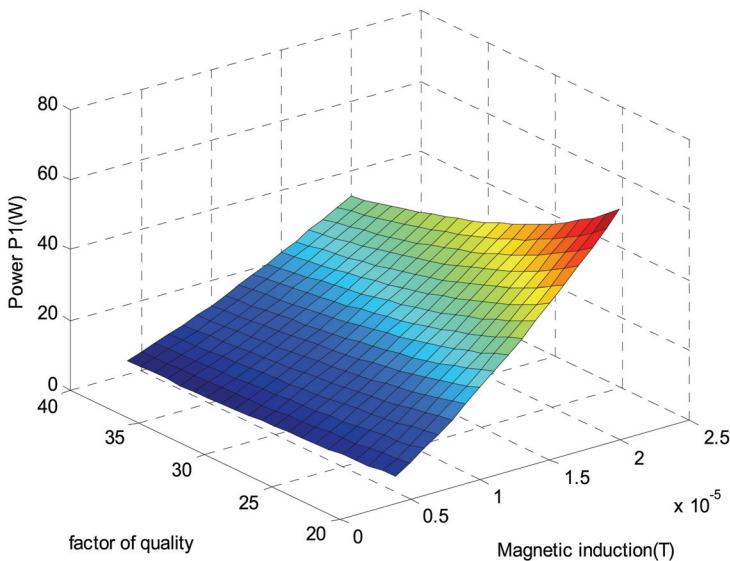
Fig. 11. Variation of the electric power in the reader's antenna according to the field to the center of the antenna

We notice that existed a minimal magnetic field B assuring the necessary tension to the working of the electronics of the transponder .in fact to get 0.4 A/ms we must arrange a field to the center of 0,5 T ,so a power of emission equal to 1 Watt .

6. Protocol survey of RFID network

6.1 Introduction
The protocols governing access to the physical layer and managing potential conflicts have a great importance in wireless networks, in which all users can transmit and receive at any time(Dan Tudor Vuza, 2009). These protocols are based on two mechanisms of allocation:

static and dynamic. A static allocation mechanism assigns a communication channel permanently, while dynamic mechanism is flexible to the nodes numbers.

6.2 Comparison between the techniques of sharing radio frequency medium

After a comparative study between different access techniques we have established a tree that describes the different methods of medium access(Christer Englund et al., 2004) (L. Zhong et al.,2001) (Jong-Hoon Youn et al., 2001)(figure II.14):
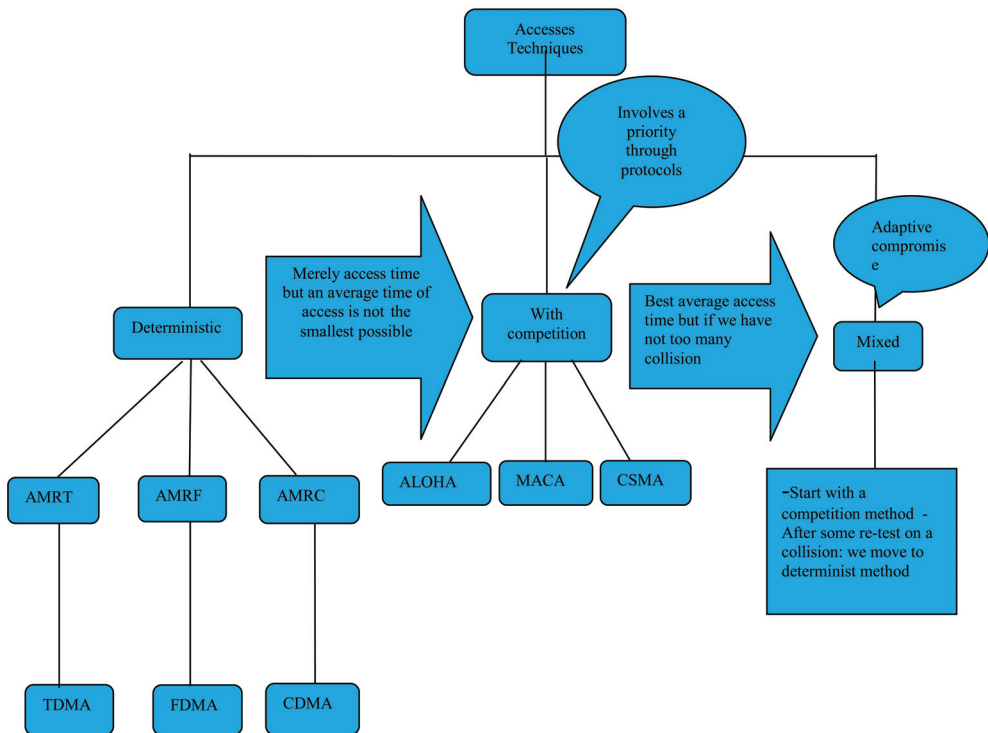
Fig. 12. Tree of accesses techniques
AMRT: Temporal Repartition Multiple Accesses
AMRF: Frequencies Repartition Multiple Accesses
AMRC: Code Repartition Multiple Accesses
TDMA: Time Division Multiple Access
FDMA: Time Division Multiple Access
CDMA: Time Division Multiple Access
MACA: Multiple Accesses with Collision Avoidance
CSMA: Carrier Sense Multiple Access

RFID is an innovative technology. Indeed, techniques for sharing the transmission medium used in other wireless communication systems are not functional in RFID technology. In summary we conclude that:
–   Temporal access techniques require a synchronization time circuit between a reader and tag so a high cost of manufacture.

– Frequency access techniques do not require frequency synchronization between a reader and tag, but in against part we will have a permanent allocation of frequency band (transmission medium).
– Code division multiple accesses suffer from NEAR FAR problem where the labels are mobile.
– The dynamic access techniques are most suitable for RFID technologies. They are flexible on the variation of tags number and for different network topologies.

Overall, the static accesses techniques are not suitable for RFID technology. Dynamic techniques accesses are the most proponents for dense RFID networks. For thus in the following chapter we present a survey of the CSMA-MAC protocol based on the network simulator (NS2).

6.3 Collisions in RFID systems

Simultaneous transmissions in RFID systems has led collisions problem, as readers and tags operate on the same channel. Three types of collisions are possible (Shweta Jain et al., 2006)(EPCTM,2006):

1. Collision Tag-Tag

The collision of Tag-tag occurs when multiple Tag transmit signal in wireless medium at the same time. Due to the arrival of multiple signals at the same time, the reader can not detect any tag. This problem prevents the reader to detect tags in its interrogation zone.

2. Collision reader-tag

The reader-tag collision occurs when the signal interferes with the neighbor's response tag which was received by other readers.

3. Collision reader-reader

A reader-reader collision occurs when a tag receives a signal from multiple readers simultaneously. In this situation, the tag may not be able to satisfy all readers.

6.4 Solution to reduce collisions in RFID networks

In this work we use an access method based on CSMA to solve the problem of collision. Indeed most of the solutions using a classic technique provide access problems so:

– TDMA requires a synchronization circuit therefore high cost of manufacturing.
– FDMA requires a large number of frequencies hopping.
– CDMA sulfur problem Near-Far.

We simulate a network that adopts the RFID services at the MAC layer by varying each time the integration of RTS / CTS on the level Configuration Protocol CSMA.

We notice from Fig.13:

– The number of packets successfully transmitted on the total number of packets generated decreases when the load offered by area increases.
– -Between 0.5 and 10 packets per second per node the reports decreases rapidly and then stabilizes beyond 15 packets per second.
– When the offered traffic load is low, we have maximum contribution because there are fewer collisions between different nodes.

From fig.14:

– The curves show the average number of data packets successfully transmitted (payload) based on the total load of the network.

- The payload increases proportionally with the speed of traffic and stabilizes at a fixed value; this stability is the result of the problem of collisions.
- To present the interest of the mechanism CSMA / CA with RTS / CTS we performed a simulation with and without RTS / CTS, these two simulations have the same configurations. Indeed in low load the two mechanisms have the same performance. As against when traffic load increases the mechanism RTS / CTS becomes more efficient.
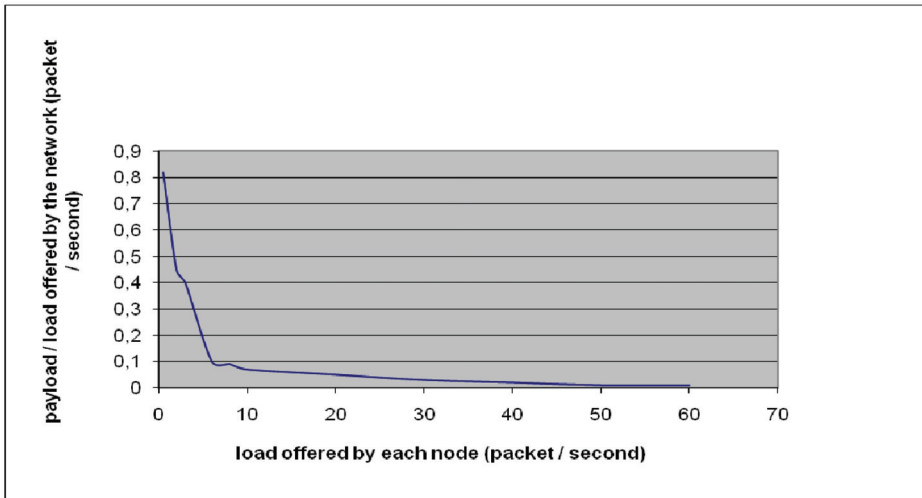
Fig. 13. Relationship between the load generated by the nodes in the coverage area and the payload
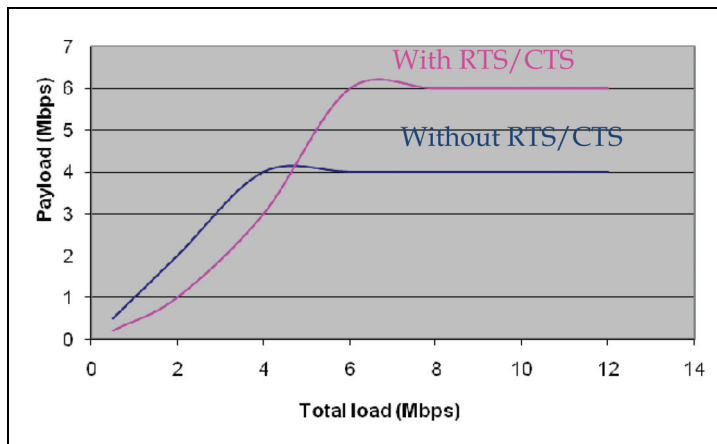
Fig. 14. Comparison of the payload with RTS / CTS and without RTS / CTS

7. Conclusion

In this chapter we detailed the RFID technology and we making the extraction of pattern from the electronic modules comprising the RFID system (base station and transponder). Finally we presented a comparison study on the MAC layer of the OSI model. Especially we have presented a tree of accesses method for wireless networks and we have modeled CSMA based o MAC protocol for RFID networks in NS2.

8. References

rami khouri.(Mai 2007). these de doctorat de l'INP grenoble, *modélisation comportementale en vhdl-ams du lien RF pour la simulation et l'optimisation des systèmes RFID UHF et microondes,* page 31.

Sok-Won Lee.(June 2005). Thesis, *A Multiple Access Algorithm for Passive RFID tags*, p 4. School of Electrical and Electronic Engineering College of Engineering Yonsei University.

Simson Garfinkel; Henry Holtzman.(june 2005). *understanding RFID technology*, garfinkel.book.

Thomas Huault.(2005-2006). *Systèmes RFID* , Master recherche optique et radio fréquence.

Cristina TURCU. (February 2009).Development and Implementation of RFID Technology, In tech BOOK. www.ni.com.*Advanced RFID Measurements: Basic Theory to Protocol Conformance Test*.

Gérard-André Dessenne. *Etat de la normalisation RFID au 15-10-2005,*par du Pôle Traçabilité.

M. Patrick PLAINCHAULT. (février 2005). Thèse de doctorat de l'institut national polytechnique de toulouse, *sécurisation de la conduite par communication véhicule infrastructure a base de transpondeurs*.

Paret D(2003). *Application en identification radiofréquence et cartes à puce sans contact*, Dunod, Paris.

Nejah NASRI. (2008). *Radio Frequency IDentification (RFID)Working,design considerations and modelling of antenna*, 2008 5th International Multi-Conference on Systems, Signals and Devices.

Dan Tudor Vuza (February 2009). *A Low Cost Anticollision Reader*, 1Institute of Mathematics of the Romanian Academy.www.intechweb.org.

Christer Englund and Henrik Wallin(April 2004). *RFID in Wireless Sensor Network*, Communication Systems Group Department of Signals and Systems CHALMERS UNIVERSITY OF TECHNOLOGY GÄoteborg, Sweden.

Jong-Hoon Youn and Bella Bose.(Oct 2001). *An energy conserving medium access control protocol for multihop packet radio networks*. In IEEE International Conference on Computer Communications and Networks, pages 470-475. ICCCN.

L. Zhong, R. Shah, C. Guo, and J. Rabaey.(May 2001). *An ultra-low power and distributed access protocol for broadband wireless sensor networks*. In IEEE Broadband Wireless Summit, Las Vegas, NV.

Shweta Jain , Samir R. Das.(September 29, 2006). *Collision Avoidance in a Dense RFID Network*, WiNTECH'06, Los Angeles, California, USA.

EPCTM. (2006). *Radio-Frequency Identification Protocols Class-1 Generation-2 RFID Protocol for Comunications at 860 MHz – 960 MHz Version 1.10*, EPCglobal Inc.

MAC Protocols for RFID Systems

Marco Baldi and Ennio Gambi
Università Politecnica delle Marche
Italy

1. Introduction

Radio Frequency Identification (RFID) has become widespread thanks to its important advantages over traditional identification technologies, like barcodes. Compared to this technology, RFID is, in fact, able to cover larger distance and does not require line-of-sight, that represent important improvements in the considered field of application.

An RFID system is formed by a set of *n* tags, that represent clients in the identification process, and a tag reader, that is the identification server. Each tag is associated with an identifier (ID), that must be transmitted to the reader upon receipt of a suitable identification query. Tags can be active, i.e. provided with an independent power supply (like a battery), or passive. In the latter case, tags depend on energy provided by the tag reader through its queries (Want, 2006). For this reason, active tags can have some data processing ability, while passive tags are limited to doing only elementary operations and replying to the reader's queries.

An important issue in Radio Frequency Identification systems concerns the reading of co-located tags, that must be managed through suitable Medium Access Control (MAC) protocols, specifically designed for low power devices. Efficiency of MAC protocols for RFID systems directly influences the time needed by the tag reader for completely identifying a set of co-located tags, so it has great impact on the whole system performance. A deep analysis of the MAC technologies adopted in RFID is the aim of this chapter.

We denote by $T_{tot}(n)$ the time needed by the tag reader for completely identifying a set of *n* tags. Under ideal conditions, it should be $T_{tot}(n) = nT_{pkt}$, where T_{pkt} is the time needed to transmit one identification packet. However, in order to ensure collision-free transmission to each tag, a MAC protocol is needed that, inevitably, produces a time waste with respect to the ideal condition. The time actually needed for identification depends on several factors, like the technology adopted, the working frequency, etc. So, RFID systems can exhibit very different reading rates, typically ranging between 100 Tag/s and 1000 Tag/s.

The most common MAC protocols used in RFID systems can be grouped into two classes: *deterministic protocols* and *stochastic protocols*. Deterministic protocols basically coincide with tree traversal algorithms: all RFID tags form a binary tree on the basis of their identifiers, and the reader explores the tree in a systematic way, by repeating queries based on bit masks. Randomness is only in the tree structure (due to the choice of the co-located tag set), while the algorithm execution is pre-determined.

Stochastic MAC protocols are instead based on the framed slotted Aloha (FSA) algorithm, that requires each tag to make a constrained pseudo-random choice of an integer number in order to reduce the probability of collisions.

Both deterministic and stochastic MAC protocols for RFID systems have some advantages and disadvantages. binary tree (BT) protocols have the advantage of very low tag complexity, since there is no need of implementing pseudo-random number generators within tags (except for singulation, when tags with the same identifier can be co-located). Furthermore, binary tree does not require the estimation of the number of co-located tags, that yields an additional effort before reading.

On the other hand, though needing a quite accurate estimation of the tags number, the FSA protocol can be more efficient than the binary tree protocol for large sets of co-located tags. Moreover, FSA does not need any particular bit coding of the tags identifiers and is intrinsically able to resolve ambiguity in the case of multiple tags with the same identifier.

Another important issue in RFID systems concerns power consumption, that influences the tags' lifetime. In fact, the same (possibly short) identification time can be achieved at the cost of many collisions or with a small number of collisions. In the latter case, power consumption is obviously minimized, with the effect of a prolonged tags' lifetime. In general terms, stochastic protocols are recognized to be more power efficient with respect to deterministic ones, due to the reduced number of collisions they produce (Namboodiri & Gao, 2007).

Both deterministic and stochastic MAC protocols have been included in standards and specifications for RFID systems. For example, EPCglobal Class 0 and Class 1 Generation 1 specifications adopt two different binary tree algorithms for the reading of co-located tags, and the same occurs in the first versions of the ISO 18000-6 standard for RFID systems (ISO/IEC, 2003). The more recent EPCglobal Class 1 Generation 2 specification introduced a new inventory technique based on the FSA protocol, that has also been included in the ISO 18000-6 Type C standard.

Several alternative solutions have been proposed in the literature for the implementation of anti-collision algorithms targeted to RFID applications (Cha & Kim, 2005), (Feng et al., 2006), (Lee et al., 2005), (Myung et al., 2006), (Park et al., 2007). For many practical and commercial applications, however, a fundamental requirement is that RFID tags must be very simple and inexpensive devices, often designed for single use. So, it is of main importance to develop low complexity anti-collision protocols able to solve the issues related to the shared medium while considering power and cost constraints.

This chapter studies both deterministic and stochastic MAC protocols for RFID systems proposed in standards, specifications and recent literature. Their principles are described and their performance is assessed and compared through theoretical and numerical arguments.

2. The binary tree protocol

The binary tree protocol is one of the most simple arbitration protocols, and it is based on the random splitting of the whole group of clients into two subgroups each time a collision occurs. This way, clients are progressively separated into smaller groups, until no more than a single client remains in each group. This is equivalent to put the clients on the nodes of a tree having maximum nodal degree 2.

In the binary tree protocol implementations used for medium access control in RFID systems, the binary splitting of tags into subgroups is based on the value of their IDs, that have fixed length and are supposed to be unique.

The tag reader is responsible for the management of the tree traversal procedure. The algorithm starts when the tag reader announces the tree traversal and transmits a binary

value. All tags having that value as the first bit of their ID reply by transmitting back the same value, while the other tags exit from the traversal and wait for another query (with different initial value).

The reader receives the transmitted values for the next bit, and it may or not detect a collision. In fact, it may happen that some tags transmit the same value, but the reader is not able to distinguish if transmission was from a single tag or more than one. In both cases, when a reply is received, the reader goes on with the binary splitting by choosing and transmitting a binary value for the next bit, until completion of the tag ID. Actually, according to the ISO 18000-6 standard, sending a null value corresponds to no transmission, that helps to reduce the power consumption.
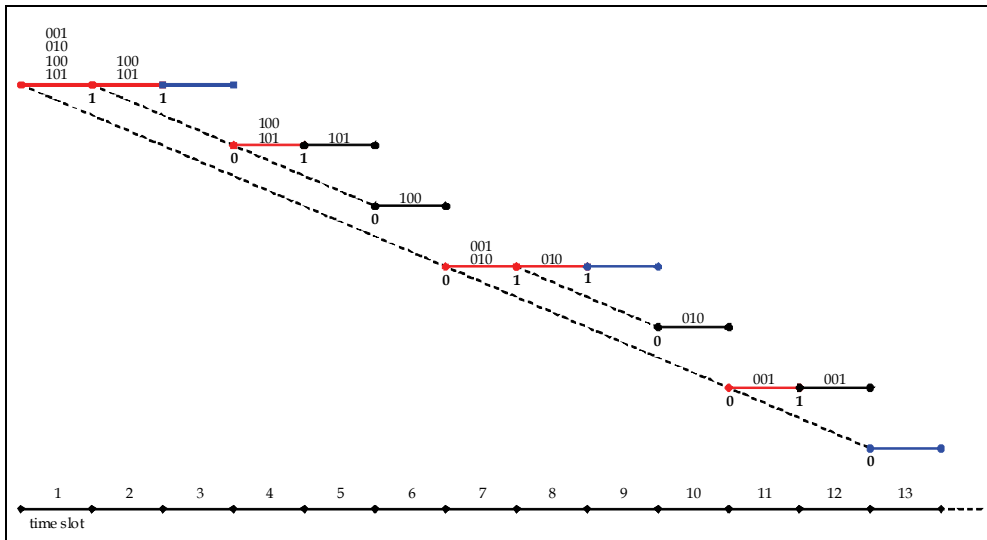
Fig. 1. Example of binary tree protocol with n = 4 tags.

An example of binary tree protocol used for reading co-located RFID tags is reported in Fig. 1. We suppose there are n = 4 tags with the following identifiers: 001, 010, 100 and 101. The time axis is divided into time slots; each time slot begins when the tag reader makes a new query for the value of a bit. The first time slot begins with the announcement of a multiple read query by the tag reader. All tags reply when such command is issued. The identifiers of the tags responding to each query are reported in the time slot that follows the query.

After the first time slot, each tag replies to the query if and only if the next bit of its ID coincides with the queried value; otherwise, it goes to sleep mode. When more than one tag reply in the same time slot, a collision occurs and the corresponding time slot is marked in red in Fig. 1. When the bit queried is not the last one, the tag reader is not able to tell a single reply from a collision, and must continue with the traversal. So, single replies at all bits except the last are equivalent to collisions (this occurs for the tags with IDs 010 and 001 in the figure). When no tag replies to a query, we have an *idle* time slot, marked in blue in the figure. Successful identification is instead accomplished when the last bit is queried and only one tag replies. The corresponding time slots are marked in black in the figure and labelled with the corresponding tag identifier.

An important feature of the binary tree protocol exemplified in Fig. 1 is that queries that are interrupted are then restarted exactly from the same point. In other terms, the tag reader must be able to store the status of each branch of the tree. This way, each edge of the tree is travelled only once, and queries are never restarted from the beginning. This version of the algorithm is with memory, and it is opposite to *memoryless* versions, whose efficiency is reduced due to repeated queries within the traversal (Bo et al., 2006).

Due to its simplicity, the binary tree protocol is suitable for being modelled analytically, and theoretical arguments can be used to predict the value of its most important parameters, that are (Janssen & De Jong, 2000): the number of tree levels required for a random contender to have success, the total number of tree levels and the number of contention frames required to complete the algorithm. Other relevant parameters, as throughput and delay, can also be estimated through analytical modelling of the protocol (Cappelletti et al., 2006).

The total number of tree levels obviously depends on the number of clients n, due to the assumption that, at the lowest tree level, each node must be associated, at most, to one client. The mapping between clients and tree nodes is stochastic, so the allocation of the tree nodes is not optimal. The total number of tree levels (D_n) can be lower bounded by considering the optimal distribution of clients on tree nodes. This occurs when even size groups of tags are split into equal subgroups, while odd size groups are split into subgroups having sizes that differ by one. In this case, it is simple to observe that:

$$D_n \geq \lceil \log_2(n) \rceil + 1,$$
(1)

where function $\lceil \cdot \rceil$ gives the smallest integer greater than or equal to its argument. In practice, due to the statistic nature of collisions, the number of levels is usually higher. In (Janssen & De Jong, 2000) it is proved that, for large n, the average number of tree levels is

$$D_n \simeq 2\log_2(n).$$
(2)

Another important parameter to evaluate the time needed by the binary tree protocol to complete the identification and to be compared with other arbitration protocols is the total number of time slots as a function of n. In order to estimate it for finite values of n (not necessarily large), we can resort to some simple theoretical arguments (Park et al., 2007).

First, we consider that each collision generates two edges, corresponding to the two possible choices for the bit under analysis. So, the total number of time slots required by the binary tree (I_{tot}) to completely identifying a set of n tags is simply twice the number of collisions (C_{bin}), augmented by one (to consider the first time slot):

$$I_{tot}(n) = 2C_{bin}(n) + 1$$
(3)

If we focus on the i-th level of the tree, the number of time slots is $m = 2^i$, and each tag must reply to a query in one of them. The probability that a tag does not reply in a time slot is:

$$p(m) = 1 - \frac{1}{m}$$
(4)

and the probability that the time slot is idle (that is, no tag replies to a query in that time slot) is $p(m)^n$. So, the average number of idle time slots at level i is:

$$Q(n,m) = m \cdot p(m)^n = m \cdot \left(1 - \frac{1}{m}\right)^n. \tag{5}$$

We have reported in Fig. 2 the value of $Q(n, m)$ expressed by (5), as a function of the tree level (i), for different values of the number of tags (n). As expected, the average number of idle time slots quickly converges to the total number of time slots, that is, 2^i.
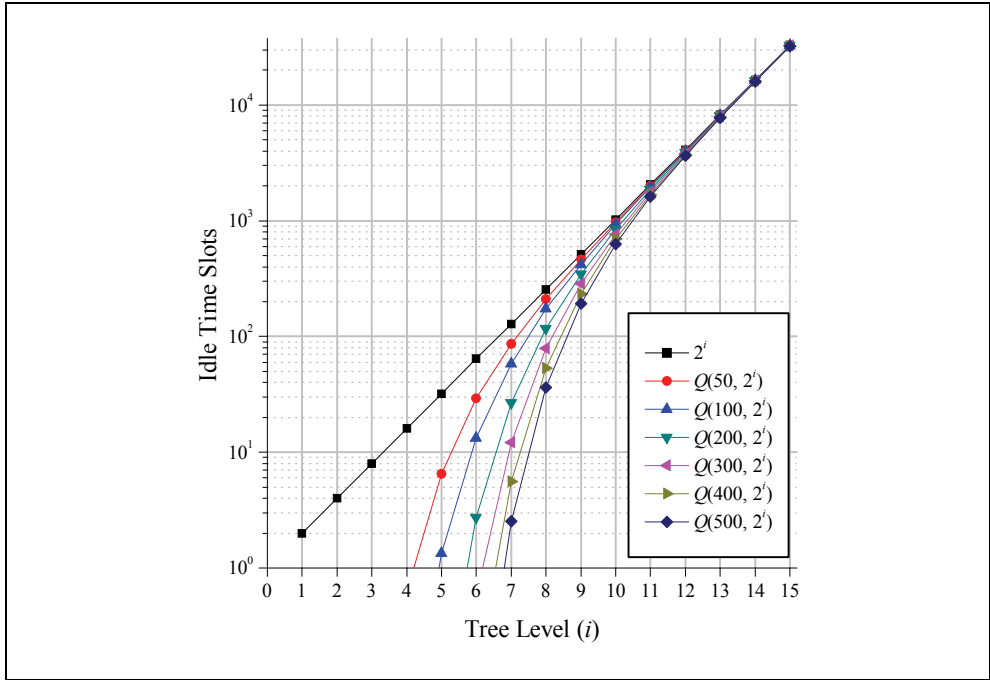
Fig. 2. Average number of idle time slots as a function of the tree level.

With similar arguments, we can consider that a time slot at level i is successful if it is used by a single tag to reply to a query. So, the average number of successful time slots at the tree level i can be estimated as follows:

$$S(n,m) = m \cdot n \cdot p(m)^{n-1}\left[1 - p(m)\right]. \tag{6}$$

Fig. 3 reports the average number of successful time slots as a function of the tree level, for the same choices of the number of tags, calculated by means of (6). In this case, it is immediate to observe that the number of successful time slots converges to the total number of tags n.

Starting from the expressions (5) and (6) for $Q(n, m)$ and $S(n, m)$, respectively, the average number of collisions at the tree level i can be estimated as the number of non-idle and non-successful time slots, i.e.:

$$C_{\text{bin}}(n,m) = m - Q(n,m) - S(n,m). \tag{7}$$
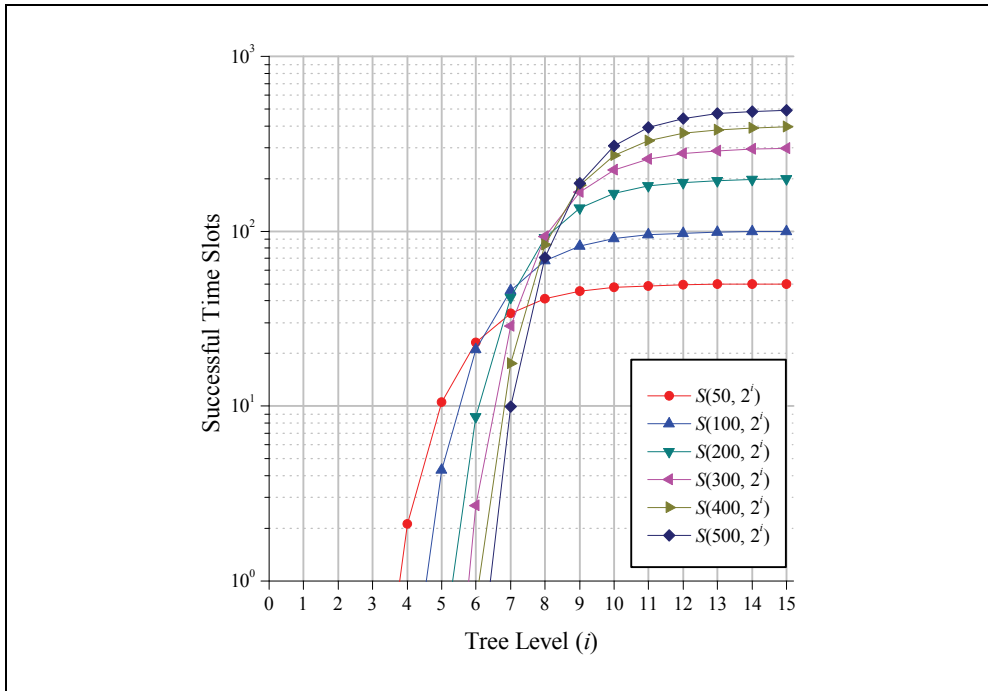
Fig. 3. Average number of successful time slots as a function of the tree level.

Based on these considerations, it follows that the average number of time slots with collisions rapidly goes to zero (a negative number of collisions obviously has no sense). For better evidence, the average number of collisions, expressed by (7), is reported in Fig. 4, for the same choices of n, as a function of the tree level. We observe that, for the initial tree levels, the number of time slots with collisions coincides with the total number of time slots (2^i). Then, the number of collisions becomes smaller than 2^i and, after reaching a maximum value, begins to decrease monotonically.

The total number of collisions in the binary tree protocol can be found by summing the average number of collisions at each tree level, that is:

$$C_{\text{bin}}\left(n\right) = \sum_{i=0}^{\infty} C_{\text{bin}}\left(n, 2^i\right). \tag{8}$$

The series surely converges because $C_{\text{bin}}(n, 2^i)$ becomes null for the values of i exceeding a given threshold. By substituting (5), (6) and (7), equation (8) can be rewritten as follows:

$$C_{\text{bin}}\left(n\right) = \sum_{i=0}^{\infty} m\left[1 + \left(n-1\right) p\left(m\right)^n - n \cdot p\left(m\right)^{n-1}\right]. \tag{9}$$

Expression (9) allows to determine analytically the total number of collisions and, through (3), we can then estimate the total number of time slots needed by the binary tree algorithm to completely identifying the set of n tags. As we will see in the following, such analytical estimation gives results that are very close to those of numerical simulations.
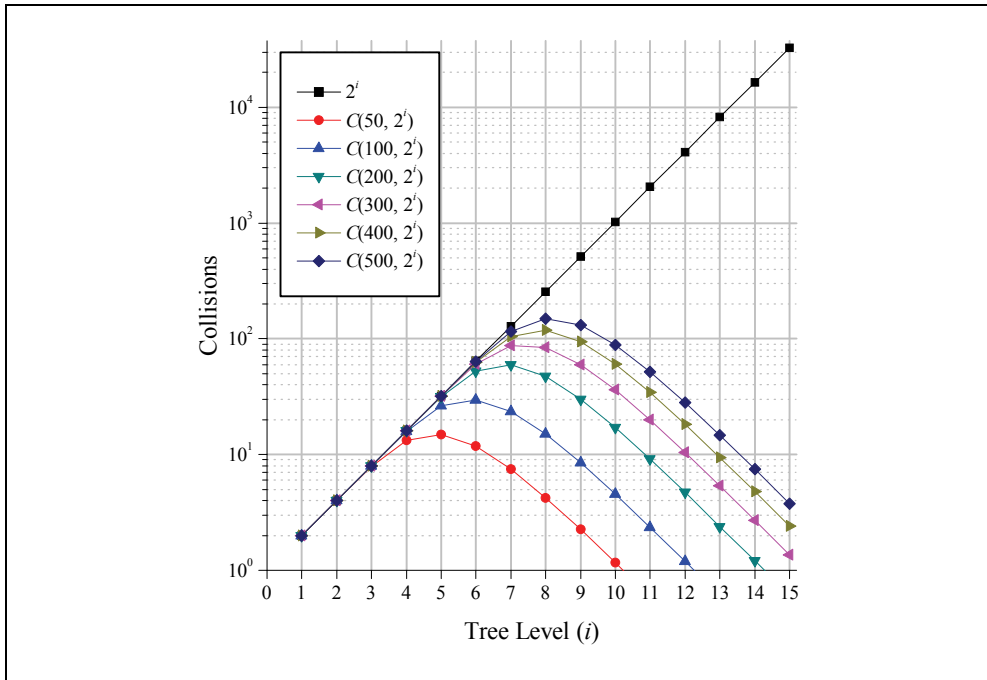
Fig. 4. Average number of time slots with collisions as a function of the tree level.

3. The framed slotted Aloha protocol

As we have seen in the previous section, the binary tree protocol for medium access control in RFID systems exploits binary splitting of the tags into subgroups on the basis of their identifiers, that are fixed and known a priori. For this reason, the binary tree and other similar deterministic protocols are opposed to stochastic protocols, mostly based on the framed slotted Aloha algorithm.

In slotted Aloha protocols, the time axis is divided into time slots. Each tag synchronizes its transmission with the beginning of a time slot, in such a way that concurrent transmissions collide completely. This is the main difference between slotted Aloha protocols and the pure Aloha one, in which instead the time axis is not discretized, so partial collisions can occur as well.

In the framed version of the slotted Aloha protocol, time slots are grouped into groups of L, and each group coincides with a frame. Each tag can transmit only once in each frame, and frames are repeated until the end of the identification procedure.

At the beginning of a frame, each tag randomly selects a time slot within the frame for transmitting its ID. The tag then transmits at the chosen time slot; if a collision occurs, colliding tags wait the end of the current frame and repeat the procedure in the following frame. The advantage of the introduction of frames is due to the limitation in the transmission rate imposed by the fact that each tag only transmits once in a frame. This allows to reduce the number of collisions in the initial phase of the protocol, when all tags try to communicate. This can result in a significant performance improvement with respect to slotted Aloha, on condition that the frame length is properly chosen.

In standard FSA, the frame length must be fixed a priori and is kept constant until completion of the algorithm. When the number of tags significantly exceeds the frame size, efficiency of the FSA protocol with fixed frames decreases. On the other hand, the algorithm efficiency could be kept high by adjusting the frame length on the basis of the number of active tags. In this case, however, such number must be estimated, that instead is not necessary in classic FSA.

A first solution to the problem of estimating the number of tags in the FSA protocol is to adopt dynamic versions of the FSA (Cha & Kim, 2005), (Lee et al., 2005). These approaches exploit the dependence of the probability of collision on the frame size and the number of tags. Such dependence can be expressed in analytical terms through theoretical arguments similar to those used in the previous section for the analysis of the binary tree protocol.

Let P_{idle}, P_{succ} and P_{coll} represent the probability that a time slot is idle, used for a successful transmission or occupied by a collision, respectively. Similarly to (5) and (6), we can express P_{idle} and P_{succ} as follows:

$$\begin{cases} P_{idle} = \left(1 - \dfrac{1}{L}\right)^n \\ P_{succ} = n\dfrac{1}{L}\left(1 - \dfrac{1}{L}\right)^{n-1} \end{cases}. \tag{10}$$

Starting from (10), P_{coll} can be calculated as:

$$P_{coll} = 1 - P_{idle} - P_{succ}, \tag{11}$$

so n can be estimated from the knowledge of L and the estimate of P_{coll}. However, it has been observed that the estimate of n so obtained can be inaccurate, since, for high values of the collision probability, small errors in the estimation of P_{coll} may produce significant deviations of the estimated n from its actual value (Park et al., 2007).

Another important result that can be derived from (10) is that the optimal frame size in the FSA algorithm exactly coincides with the number of tags n. So, FSA becomes less and less efficient when the gap between L and n increases.

For this reason, in Dynamic FSA (DFSA), the probability of collision is used to obtain an estimate of the number of tags that try to access the shared medium. This is repeated at each frame, in such a way that the frame length is dynamically adjusted on the basis of the actual number of contending tags. As anticipated, the estimated number of tags can be inaccurate. We will denote by α the ratio between the estimated number of tags and its exact value (thus, $\alpha = 1$ represents the ideal behaviour).

3.1 FSA with robust estimation and binary selection

An efficient approach for estimating the number of contending tags in the FSA protocol has been proposed in (Park et al., 2007), where the variant denoted as "FSA with Robust Estimation and Binary Selection", or EB-FSA, has been introduced.

The EB-FSA protocol begins with an estimation phase that has the purpose of estimating the number of tags n and to adjust the frame size L consequently. The estimation phase proposed in (Park et al., 2007) is robust, in the sense that it solves the issues due to high sensitivity of the estimated n to estimation errors on P_{coll}, in (11), for high values of the collision probability.

Estimation in EB-FSA starts by fixing an estimation frame size L_{est} and a target P_{coll} threshold ($P_{coll-th}$), that corresponds to a threshold number of tags (n_{th}) through (10) and (11). The tag reader estimates the value of n only when P_{coll} becomes smaller than $P_{coll-th}$, in such a way to reduce inaccuracy on the estimate of n (n_{est}). For this purpose, at each iteration of the estimation phase, the tag reader reduces the number of tags polled by a factor f_d, using a bit mask in the query frame.

Estimation of the tags number is made only when P_{coll} becomes smaller than $P_{coll-th}$, i.e., after a number of estimation frames equal to $i^*(n)$, that coincides with the smallest i such that $n/f_d^{i-1} < n_{th}$. In formula:

$$i^* \left(n \right) = \underset{\substack{i \in \mathbb{N} \\ \frac{n}{f_d^{i-1}} < n_{th}}}{\arg\max} \left(\frac{n}{f_d^{i-1}} \right). \tag{12}$$

Thus, in the EB-FSA protocol, the initial estimation phase requires $I_{est} = i^*(n)L_{est}$ time slots. After such initial phase, tags randomly choose an integer between 1 and n_{est} for transmission of their ID, and a frame with length n_{est} is transmitted. Differently from FSA, when a collision occurs, colliding tags do not wait for the next frame to retransmit their ID. On the contrary, a binary selection mechanism is implemented, that works as follows:

- non colliding tags increment their counters by 1;
- colliding tags randomly choose a binary value;
- colliding tags that chose 0 try retransmission at the next time slot;
- colliding tags that chose 1 try retransmission after one time slot;
- if another collision occurs, the procedure is repeated within the new set of colliding tags.

The binary selection mechanism avoids the need for subsequent frames, since each collision is necessarily solved through the splitting procedure. The protocol succeeds when all the tags have been identified, that is, after I_{iden} time slots. So, the total number of time slots needed by the EB-FSA protocol for completing its task is:

$$I_{tot} = I_{est} + I_{iden} = i^*(n)L_{est} + I_{iden}. \tag{13}$$

As it will be evident through numerical simulations, the EB-FSA approach can achieve a significant performance improvement with respect to FSA and DFSA.

4. Protocols comparison

In order to assess and compare the considered protocols for medium access control in RFID systems, we report in this section the results of numerical simulations that model different scenarios.

We are interested in estimating the time needed by the considered protocols to complete the identification phase, in order to compare their efficiency in arbitrating the channel use in groups of tags with different size. The actual identification speed depends on technology issues, so we refer to the number of time slots instead of real time.

We consider, as a starting point, the classic implementation of the framed slotted Aloha protocol, with fixed frame size. We consider two common values of frame size, that are $L = 128$ and $L = 256$, and estimate by simulation the total number of time slots needed to complete the identification procedure (I_{tot}). The results obtained are averaged over a number of simulations sufficiently high to ensure a satisfactory level of statistic confidence.
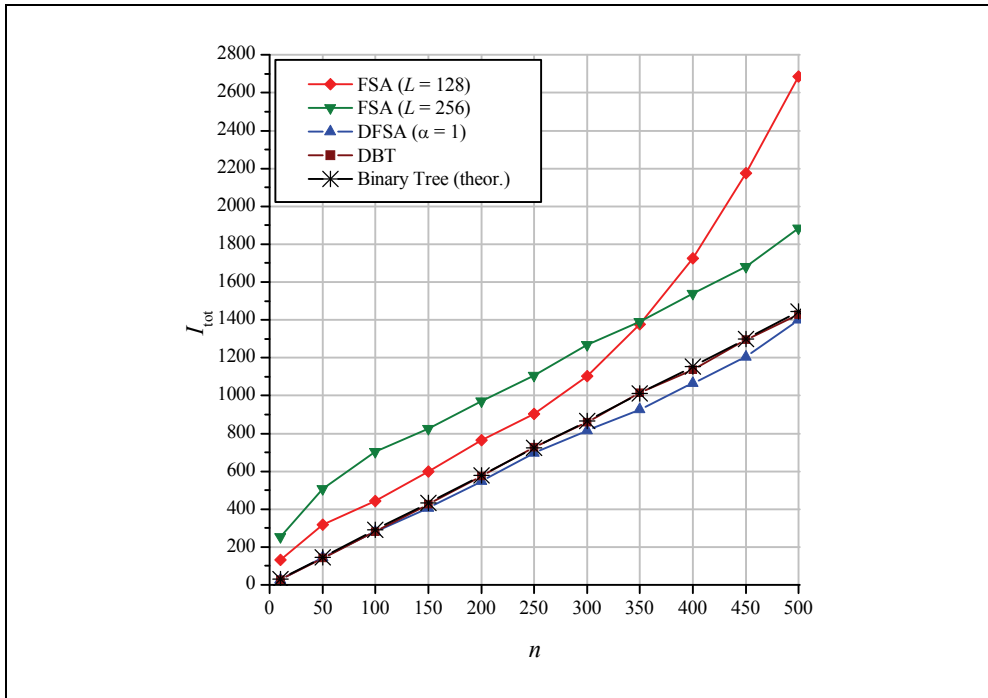
Fig. 5. Comparison of binary tree and framed slotted Aloha protocols.

The values of I_{tot}, so obtained, are reported in Fig. 5 as a function of the total number of tags (n). As we observe from the figure, the classic FSA protocol becomes less and less efficient for an increasing number of tags. The curve corresponding to $L = 128$ exhibits a parabolic behaviour starting from n on the order of 300. When L is increased up to 256, the protocol is less efficient for a small number of tags (n between 0 and 350), but its performance is improved for higher n. The parabolic behaviour of the curve for $L = 256$ is not apparent in the figure, since occurs for higher values of n with respect to the simulation scope.

In Fig. 5, classic FSA is compared with Dynamic FSA, in which the frame length is changed dynamically in such a way to coincide always with the number of contending tags. When the estimation of the number of tags is exact ($\alpha = 1$), the DFSA protocol is able to significantly improve the performance of classic FSA. As we observe from the figure, the improvement is on the order of 200 time slots with respect to FSA with $L = 128$ and n up to 250. When n increases, the advantage of adopting DFSA instead of FSA becomes more and more relevant.

As an example of the binary tree algorithm, we consider a distributed binary tree (DBT) protocol that is self-adjusting, and that is directly managed by tags (Baldi et al., 2008). It recalls the classic version of the binary tree traversal, in which, when a collision occurs, each client randomly chooses a binary value. This is the same principle at the basis of the binary selection phase in the EB-FSA protocol. In DBT, the reader sends its query and all tags randomly choose a binary value. Tags that chose 0 try transmission at the first time slot available, while the others try transmission at the following time slot. If a collision occurs,

the same procedure used in EB-FSA is adopted. So, colliding tags randomly select another binary value, while all the others increment their counters by 1.

Such implementation of the BT protocol is independent of the bit coding of the tags IDs (that instead must be suitably chosen in the RFID standard BT protocol). Moreover, a fundamental role in RFID standard binary tree is played by the tag reader, that must perform the splitting procedure based on the tags IDs. On the contrary, in DBT the tags are able to manage the protocol autonomously, without the reader's queries. This way, the tag reader is not required to store the status of forked queries to avoid travelling each edge more than once. On the other hand, a drawback of DBT is that it requires tags to perform some processing (as for generation of pseudo-random binary values), so it could be difficult to implement with passive tags.

As we see from Fig. 5, performance of the DBT protocol is very close to the theoretical expectation, expressed by (9). DBT is able to improve significantly the performance of standard FSA and, for a number of tags up to 500, gives a moderate performance loss with respect to DFSA.

As a further assessment, we can compare the performance of the DBT protocol with that of EB-FSA. A simple example of application of the two protocols is reported in Fig. 6, where we consider the case of $n = 5$ tags. We observe from the figure that the only difference between the two protocols consists in the distribution of the initial values of the tag counters: in EB-FSA each tag must know the frame size ($L = 5$, in this case) and chooses its random value accordingly. In DBT, instead, each tag starts by choosing a binary value, without any knowledge on the frame size. However, even without needing any information on the number of tags, the DBT protocol is able to achieve the same performance as the EB-FSA, in the considered example, since both protocols complete identification in 8 time slots. Moreover, contrary to EB-FSA, DBT does not require any estimation phase before identification.

On the other hand, it should be observed that the DBT protocol produces a higher number of collisions with respect to EB-FSA, due to the fact that the initial values chosen by the tags are only binary. In EB-FSA, instead, tags can select initial values in the range between 1 and n_{est}. For these reasons, the DBT protocol is less efficient than EB-FSA under the power consumption viewpoint.

DBT

	1	2	3	4	5	6	7	8
Counter Tag1	1	2	1	2	1	0 (C)	1	0 (S)
Counter Tag2	0 (C)	1	0 (C)	1	0 (S)			
Counter Tag3	0 (C)	1	0 (C)	0 (S)				
Counter Tag4	1	2	1	2	1	0 (C)	0 (S)	
Counter Tag5	0 (C)	0 (S)						
Time Slot	1	2	3	4	5	6	7	8

EB-FSA

	1	2	3	4	5	6	7	8
Counter Tag1	2	1	0 (C)	1	0 (C)	0 (S)		
Counter Tag2	0 (S)							
Counter Tag3	2	1	0 (C)	1	0 (C)	1	0 (S)	
Counter Tag4	2	1	0 (C)	0 (S)				
Counter Tag5	3	2	1	2	1	2	1	0 (S)
Time Slot	1	2	3	4	5	6	7	8

Fig. 6. Example of application of DBT and EB-FSA protocols.

When the number of tags increases, the advantage of having many possible initial random values in EB-FSA becomes more and more relevant, yielding a performance improvement

with respect to the DBT protocol. This is shown in Fig. 7, where DBT is compared with EB-FSA through numerical simulations, for a number of tags up to 500.

As we observe from the figure, under the hypothesis of perfect estimation of the number of tags, the EB-FSA protocol outperforms the DBT one. However, we can take into account the number of time slots needed by the initial estimation phase of EB-FSA, I_{est}, calculated on the basis of (12). The value of I_{est} has been found by considering, for the estimation phase, the same choice of the parameters proposed in (Park et al., 2007), that is, $L_{est} = 64$, $P_{coll-th} = 0.7$ and $f_d = 4$. By considering the estimation phase, the performance gain achieved by EB-FSA becomes smaller and the two protocols have almost the same performance for a number of tags up to 300. So, the DBT protocol could still represent a valid choice, since it does not require the initial estimation phase, that has some drawbacks under the complexity viewpoint.
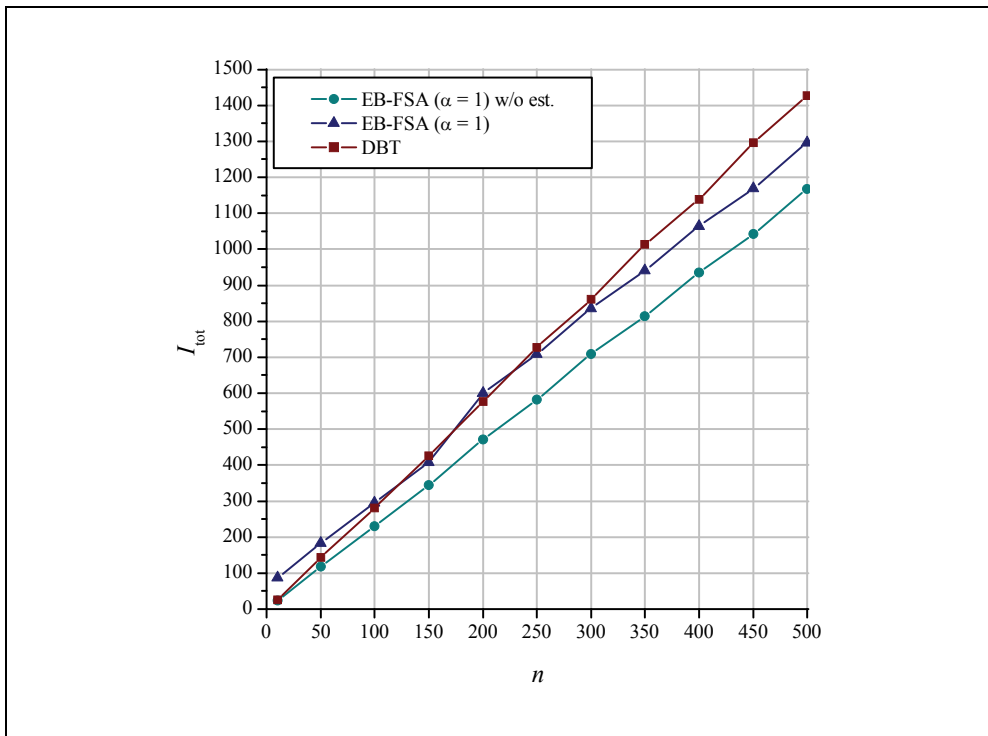
Fig. 7. Comparison of DBT and EB-FSA with perfect estimation ($\alpha = 1$).

Another important aspect that must be taken into consideration is that, in the EB-FSA protocol, the estimation phase could be inaccurate, so the performance gain with respect to DBT could be further reduced.

We consider two different cases, in which we suppose that the reader estimates a number of tags equal to 0.5 and 1.5 times the actual number. The results of numerical simulations of the EB-FSA protocol with inaccurate estimation are reported in Fig. 8, where they are compared with those of the DBT algorithm.

We observe that the DBT protocol achieves almost the same performance as the EB-FSA in both the considered cases with inaccurate estimation. The overhead due to the initial estimation phase in EB-FSA has been also taken into account.

So, for a number of tags up to 500 (that is of interest for many applications), the DBT protocol (or, equivalently, the binary tree protocol based on tags IDs) is able to guarantee a rather good collision arbitration. Its performance compares with that of optimized stochastic algorithms, as the EB-FSA.

However, as we notice from the figure, the DBT curve has a higher slope with respect to those of EB-FSA and intersects them at $n \approx 300$. This confirms that, when the number of tags increases, the advantage of EB-FSA becomes more and more relevant.
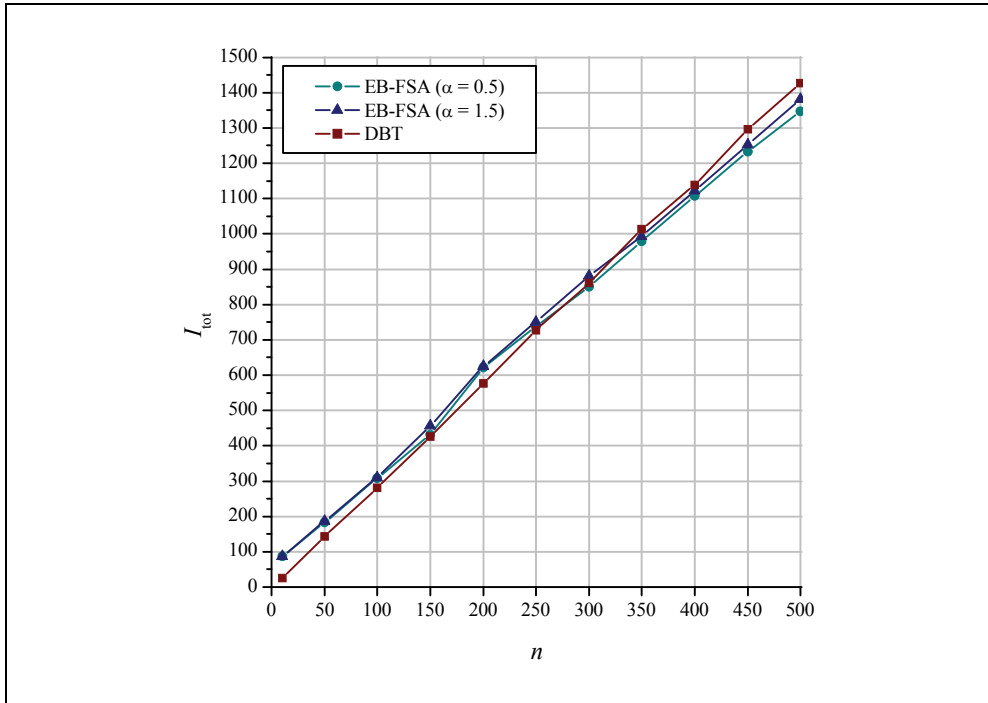
Fig. 8. Comparison of DBT and EB-FSA with inaccurate estimation (α = 0.5, 1.5).

5. Conclusion

A very common requirement in RFID systems is the reading of co-located tags, that is necessary when multiple tags are found simultaneously in the coverage area of the tag reader. Due to the low latency and low power constraints of these systems, the availability of efficient protocols able to arbitrate collisions and guarantee shared access to the transmission medium becomes of fundamental importance.

This chapter has described several anti-collisions protocols for RFID systems, that can be grouped in the two main categories of deterministic and stochastic protocols. We have seen that deterministic protocols, as the binary tree algorithm, can outperform classic stochastic

protocols as the framed slotted Aloha with fixed frame length. By considering more efficient versions of stochastic protocols, like the Dynamic FSA and the EB-FSA, the performance in terms of identification speed can be improved in a significant manner.

All these protocols, however, require estimation of the number of contending tags. So, the BT algorithm could still represent a good solution for resolving collisions without the need of tags estimation. We have seen that the BT protocol can also be implemented in a distributed manner, in such a way to be managed directly by tags and to be independent of the bit coding of the tags identifiers. This could represent an alternative to the RFID standard BT protocol (with centralized coordination) when intelligent tags are available.

6. References

Baldi, M., Morichetti, S. & Gambi, E. (2008). "A distributed binary tree protocol for medium access control in RFID systems", in *Proc. SoftCOM 2008*, Split, Dubrovnik, Croatia, 25-27 Sep. 2008, pp. 228-232.

Cappelletti, F., Ferrari, G. & Raheli, R. (2006). "A simple performance analysis of multiple access RFID networks based on the binary tree protocol", in *Proc. Intern. Symp. Commun. Control Signal Proc. (ISCCSP '06)*, Marrakech, Morocco, Mar. 2006.

Cha, J.-R. & Kim, J.-H. (2005). "Novel Anti-Collision Algorithms for Fast Object Identification in RFID Systems", in *Proc. ICPADS 2005*, Fukuoka, Japan, Jul. 2005, vol. 2, pp. 63–67.

Feng, B., Li, J.-T., Guo, J.-B. & Ding, Z.-H. (2006). "ID-Binary Tree Stack Anticollision Algorithm for RFID", in *Proc. IEEE ISCC '06*, Cagliari, Italy, Jun. 2006, pp. 207–212.

ISO/IEC 18000–6 (2003). "Information technology automatic identification and data capture techniques - radio frequency identification for item management air interface – part 6: parameters for air interface communications at 860-960 MHz", Nov. 2003.

Janssen, A. & De Jong, M. (2000). "Analysis of Contention Tree Algorithms", *IEEE Trans. Inform. Theory*, vol. 46, no. 6, pp. 2163–2172.

Lee, S.-R., Joo, S.-D. & Lee, C.-W. (2005). "An Enhanced Dynamic Framed Slotted ALOHA Algorithm for RFID Tag Identification", in *Proc. MobiQuitous 2005*, San Diego, CA, Jul. 2005, pp. 166–172.

Myung, J., Lee, W. & Srivastava, J. (2006). "Adaptive Binary Splitting for Efficient RFID Tag Anti-Collision", *IEEE Commun. Lett.*, vol. 10, no. 3, pp. 144–146.

Namboodiri, V. & Gao, L. (2007). "Energy-Aware Tag Anti-Collision Protocols for RFID Systems", in *Proc. IEEE PerCom '07*, White Plains, NY, Mar. 2007, pp. 23–36

Park, J., Chung, M. Y. & Lee, T.-J. (2007). "Identification of RFID Tags in Framed-Slotted ALOHA with Robust Estimation and Binary Selection", *IEEE Commun. Lett.*, vol. 11, no. 5, pp. 452–454, May 2007.

Want, R. (2006). "An Introduction to RFID Technology", *IEEE Perv. Comput.*, vol. 5, no. 1, pp. 25-33.

Stochastical Model and Performance Analysis of Frequency Radio Identification

Yan Xinqing[1], Yin Zhouping[2] and Xiong Youlun[2]
[1]School of Information Engineering, North China University of
Water Conservancy and Electric Power,
[2]State Key Laboratory of Digital Manufacturing Equipment and Technology,
Huazhong University of Science and Technology,
China

1. Introduction

RFID (Radio Frequency Identification) can assign a unique digital identifier to each physical item, and provide an efficient, cheap and contactless method for gathering the information of the physical items to enable their automatic tracking and tracing(Finkenzeller 2003). RFID technology serves as the back stone of the "Internet of Things"(Engels 2001), and is reviewed as a main enabler of the upcoming "Pervasive Computing"(Stanford 2003). RFID systems have been widely adopted in quite a lot applications, ranged from "smart box" to world-wide logistics management systems.

A typical RFID system is consisted of some RFID tags, one or more RFID readers and the backend information system. Each RFID tag holds a unique identifier and is attached to a physical item. RFID reader is used to collect the identifiers stored in the RFID tags located in its vicinity and is often connected with the backend information system. During identification, The RFID reader asks the RFID tags to modulate their binary identifiers into signals and transmit these signals back to the reader through the air interface, which is a wireless communication channel for the RFID tag and reader to exchange information. Afterwards, The RFID reader sends the data gathered to the backend information system for further processing and dispatching to various applications.

One of the main issues that affect the universal deployment and application of the RFID system is the collisions occurred during RFID tag identification(Wu 2006). The simultaneous modulated signals broadcasted by the RFID reader and transmitted from the RFID tags will interfere in the air interface, in which case, what the receivers can get is only a collision signal but no useful information. Collisions occurred in the RFID system can be categorized as the reader-reader, reader-tag and tag-tag collisions(Shih 2006).

When two or more RFID readers try to broadcast messages through the air interface simultaneously, reader-reader collision occurs. Due to that they are often connected with the computer system and can be equipped with enough resource to monitor the air interface, RFID readers can detect the collision and coordinate with each other in advance. Reader-reader collision can be avoided and resolved completely with some deliberate designed protocols, such as the ColorWav(Waldrop 2003) and others(Leong 2006).

Reader-tag collision can also be avoided easily by asking the RFID reader and RFID tags to broadcast message and transmit identifiers in different time, so that the signals broadcasted by the RFID reader and transmitted from RFID tags will never collide in the air interface and reader-tag collision will never occur.

When two or more RFID tags try to transmit their identifiers simultaneously through the air interface, tag-tag collision will occur. Due to the extreme constraints on computation, communication and energy supply put on RFID tags, especially that in passive RFID system, RFID tag can only get power supply through the reflection of the waveforms broadcasted by the RFID reader, tag-tag collision cannot be resolved easily using existed collision resolution methods, such as CDMA (Code Division Multi Access), FDMA (Frequency Division Multi Access), SDMA (Space Division Multi Access) and TDMA (Time Division Multi Access), proposed in other communication systems(Theodore 2006).

Proposed protocols for RFID tag collision resolution can be classified as the probabilistic frame slotted ALOHA based protocols, the deterministic splitting tree based protocols, and some hybrid protocols, such as the slotted tree protocol (Bonuccelli 2007). The deterministic splitting tree based RFID tag collision resolution protocols suffer from scalability, and perform clumsily in resolving the collision caused by a large amount of RFID tags, while the hybrid protocols are seldom adopted in real RFID systems, so these collision resolution protocols will not be discussed any further in this chapter.

Due to that in a frame, each RFID tag can only choose a slot to transmit its data, the RFID tag collision resolution process using the frame slotted ALOHA based protocols can be viewed as a binomial distribution process, the identification accuracy and the efficiency of the protocol depends seriously on the estimation and choice of some key parameters.

In this chapter, for the probabilistic frame slotted ALOHA based RFID tag collision resolution protocol, based on the binomial distribution model, the accurate estimation of the RFID tag population and the optimal choice some key parameters adopted in the collision resolution protocol are analyzed, the Markov chain and its corresponding transition matrix for RFID tag collision resolution are proposed to determine the amount of frames needed in the identification, and our research is verified by numeric simulations.

The remaining sections of this chapter is organized as follows: section 2 presents the basic assumption we hold in this chapter and reviews briefly the frame slotted ALOHA based RFID tag collision resolution protocols. Section 3 discusses the stochastical distribution model for RFID tag collision resolution based on the binomial distribution and the Markov chain, and some key parameters that affect the performance of the collision resolution protocol are analyzed. Section 4 describes and analyzes the result of the numeric simulations performed to verify our research. And finally in Section 5, we conclude.

2. Basic assumptions and the frame slotted ALOHA based protocols

2.1 Basic assumptions

In this chapter, as presented in (Kaplan 1985) for the analysis of multiple-access protocols, we hold the following basic conventions in the discussions:

- Time is slotted, each time slot can be either a command slot for the RFID reader to broadcast a message or a data slot for the RFID tags to transmit their binary identifiers.
- One RFID tag group is interrogated in a data slot.
- The air interface is perfect, and no signal transmission error or lose occurs in it.
- The air interface is ternary, the interrogation of a tag group reveals the presence of *zero, one* and *two or more* RFID tags.

But unlike (Kaplan 1985), in this chapter, it is assumed that the air interface is instantaneous, not delayed, due to the limited distance between the RFID reader and RFID tags. However, short time intervals are needed for the RFID reader and tags to modulate and transfer a bit through the air interface. As other research work on RFID tag collision resolution protocols, it is assumed that RFID tags remain stable in a collision resolution cycle, neither newly arrived RFID tag enters nor does existed RFID tags leave the interrogation zone of the RFID reader during an identification cycle.

2.2 The frame slotted ALOHA based RFID tag collision resolution protocols

The ALOHA protocol for resolving the collision occurred in wireless communication was originally proposed by N. Abramson from the Hawaii University in the 1970s to enable the terminals distributed in isolated islands to exchange information with the mainframe computer system(Abramson 1970). In this protocol, each terminal can choose a time interval randomly to transmit its data to the mainframe, and if the time interval is occupied solely by the terminal, the data can be received by the mainframe successfully. Otherwise, if the time interval is occupied by two or more terminals and collapses, the data signals from these terminals will interfere, and collision will occur, and each terminal is acknowledged with the collision and will choose randomly another time interval afterward for retransmission.

An improvement of the ALOHA protocol is the slotted ALOHA protocol (Roberts 1975), in which the time is slotted, each terminal can only choose randomly a whole time slot, start data transmission at the beginning of the time slot and finish transmission at the end of it. In such a way, a lot of collisions occurred in the wireless communication channel can be avoided.

Due to its simplicity and easiness of implementation, the slotted ALOHA protocol was introduced to the RFID system to resolve the tag-tag collisions, which are caused by that two or more RFID tags try to transmit their identifiers simultaneously through the air interface, and various frame slotted ALOHA based RFID tag collision resolution protocol have been suggested, such as the standard frame slotted ALOHA protocol, the dynamic frame slotted ALOHA protocol, the extended frame slotted ALOHA protocol and etc. Some frame slotted ALOHA protocols have been adopted as international or industrial standards. In all these protocols, the overall process that a RFID reader tries to collect the identifiers stored in the RFID tags within its vicinity is called a collision resolution cycle (or an identification cycle), which is consisted of a series of frames. And in each frame there is a command slot and a series of data slots.

In the command slot of a frame, the RFID reader broadcasts a command message to RFID tags in its interrogation zone to indicate the number of data slots (frame length), *s*, adopted in this frame. Each RFID tag, upon receiving this message and decoding the frame length *s*, randomly generates an integer *i* in the range *0..s-1*, modulates its binary identifier into signals and transmits the signals back to the RFID reader in the *i*th data slot through the air interface. Due to the constraint on computation put on RFID tags, *s* is often chosen as a integer mean of 2 and in the range *[2,4,8,16,32,64,128,256]*.

Afterwards, the RFID reader gathers information contained in the data slots of the frame. If in a data slot, no RFID tag chooses to transmit its identifier, the data slot is called an idle slot. Else if in a data slot, there is one and only one RFID tag choosing to transmit its identifier, the data slot is called a success slot, the identifier is gathered and the RFID tag is identified successfully. Otherwise, two or more RFID tags choose to transmit their identifiers in the data slot, collision will occur and the data slot is called a collision slot, in such case, what the RFID reader can get is only a collision signal but no other useful information.

If after a frame, the desired identification accuracy of RFID tags specified by the application system is achieved, the current collision resolution cycle can be terminated, and the RFID reader will report the result to the backend information system for further processing and dispatching. Otherwise, another collision resolution frame is needed, and the same identification process is repeated.

3. The stochastical model for collision resolution of RFID tags

3.1 The binomial distribution model for RFID tag collision resolution

In a collision resolution frame, due to that each RFID tag can only randomly choose one data slot to transmit its digital identifier, this procedure can be viewed as a typical binomial distribution process.

Suppose that the population of RFID tags within the vicinity of the RFID reader is t and the frame length is s, the probability that n RFID tags choose a common data slot to transmit their identifiers can be calculated with the binomial distribution as

$$B_{s,\frac{1}{t}} = \binom{t}{n}\left(\frac{1}{s}\right)^n\left(1-\frac{1}{s}\right)^{t-n} \tag{1}$$

where $\binom{t}{n} = \frac{n!}{t!(n-t)!}$. And the mathematical expects of this binomial distribution can be calculated with

$$E\left[\left[B_{t,\frac{1}{s}}(n)\right]\right] = s\binom{n}{t}\left(\frac{1}{s}\right)^n\left(1-\frac{1}{s}\right)^{t-n} \tag{2}$$

Suppose that μ_r is a random variable representing the amount of data slots that r RFID tags chooses the data slot to respond, where $r \in [0,1,..,t-1]$, the distribution of μ_r, according to (Feller 1970), is

$$P(\mu_r = m) = \frac{\binom{s}{m}\prod_{k=0}^{m-1}\binom{t-k}{r}G(s-m,t-rm)}{s^t} \tag{3}$$

where $G(M,m) = M^m + \sum_{k=1}^{\left\lfloor\frac{m}{r}\right\rfloor}\left\{(-1)^k\prod_{j=0}^{k-1}\left\{\binom{m-jr}{r}(M-j)\right\}(M-k)^{m-kr}\frac{1}{k!}\right\}$.

The mathematical expects for the number of idle, success and collision data slots, $C_{0,t,s}$, $C_{1,t,s}$, and $C_{k,t,s}$ achieved in the frame can be calculated as

$$C_{0,t,s} = s\left(1-\frac{1}{s}\right)^t \approx s\,e^{-\frac{t}{s}}$$
$$C_{1,t,s} = t\left(1-\frac{1}{s}\right)^{t-1} \approx t\,e^{-\frac{t}{s}} \tag{4}$$
$$C_{k,t,s} = s - c_{0,t,s} - c_{1,t,s} \approx s\left(1-\left(1+\frac{t}{s}\right)e^{-\frac{t}{s}}\right)$$

The values of $C_{0,t,s}$, $C_{1,t,s}$ and $C_{k,t,s}$ for the identification of different amount of RFID tags with fixed frame length $s=256$ are shown in Fig. 1. From Fig. 1, it can been observed that for the collision resolution protocol with fixed frame length, as tag population increases, the amount of collision slots also increases rapidly and approaches to the frame length, and the

amount of idle slots deacreses rapidly and approaches to 0, while the amount of success slots, after reaches a maximum value, will also decrease rapidly and approach to 0 finally.
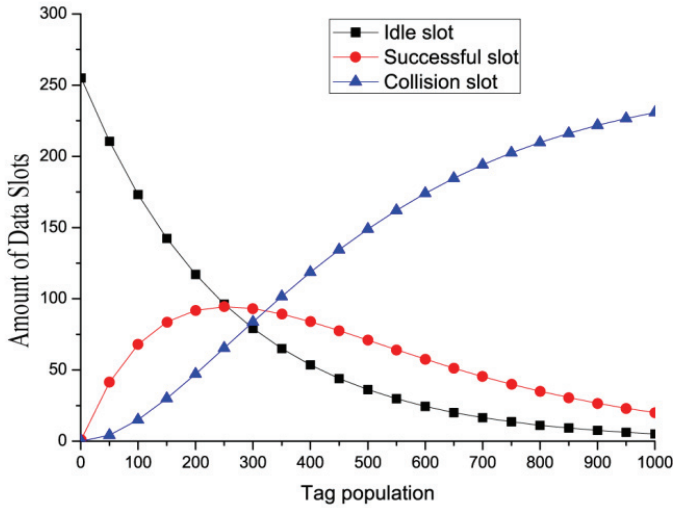
Fig. 1. The Values of $C_{0,t,s}$, $C_{1,t,s}$ and $C_{k,t,s}$ for Different Tag Population and Fixed Frame Length s=256

3.2 Estimation of RFID tag population

In typical RFID applications, the population of RFID tags within the vicinity of the RFID reader is usually unknown in advance. For the frame slotted ALOHA based RFID tag collision resolution protocols, accurate estimation of the RFID tag population is a necessity for the calculation of the identification accuracy achieved after a frame and the termination of the current collision resolution cycle.

Proposed methods for the estimation of the RFID tag population adopted in the frame slotted ALOHA based protocols, according to the name of the proposer, can be categorized as the Vogt-1, the Zhen-1, the Cha-1, the Cha-2 and the Vogt-2 methods.

The Vogt-1 method (Vogt 2002) refers to that after an identification frame, if the amounts of idle, successful and collision slots are a_0, a_1, and a_k, due to that a_1 RFID tags respond in the successful slots and that every collision is occupied by the identifiers from at least 2 RFID tags, the overall population of RFID tags that respond in the frame can estimated as t directly with

$$t = a_1 + 2a_k \qquad (5)$$

The Zhen-1 method (Zhen 2005) uses the probability that collision occurs in a data slot to estimate the overall population of RFID tags in the vicinity of the RFID reader. The probability that a RFID tag may collide with other RFID tags in a data slot can be calculated as

$$C = \frac{P_{col}}{1 - P_{suc}} = 1 - \frac{(1 - \frac{1}{s})^t}{1 - \frac{t}{s}(1 - \frac{1}{s})^{t-1}} \tag{6}$$

where P_{col} and P_{suc} refer to probabilities that a data slot result in collision and success. According to the law of large number, the stable of value of C can be achieved when $t \to \infty$, and in such case, C can be calcuated as $C=0.418$. So the overall population of RFID tags that transmits their identififers in the frame can be estimated with

$$t = a_1 + \frac{a_k}{C} = a_1 + 2.392a_k \tag{7}$$

Another method proposed in (Cha 2005) is that the overall population of RFID tags within the vicinity of the RFID reader should be estimated as $t=2.392a_k$, and this method is called the Cha-1 in this chapter.

As proposed in (Cha 2006) according to the binomial distribution of the frame slotted ALOHA based RFID tag collision resolution protocols, the mathematical expects for the amounts of idle, successful and collision slots can be calculated with Eq. 3, if after a frame, the actual number of collision slots is a_k, for the equation $a_k = s\,(1 - \left(1 + \frac{t}{s}\right) e^{-\frac{t}{s}})$, for known s, the value of t can be calcuated with the Newton or other literation methods.

This calculation is time consuming, so to ease the calculation, for the framel length s adopted in the protocol, we can calcuated the value of $C_{k,t,s}$ for different t, and compare a_k with it to find the approximate RFID tag population t. That is, through seaching t to minimize the $|a_k - C_{k,t,s}|$, the appropriate value of RFID tag population can be founded. This method is called Cha-2, and also has been proposed in (Kodialam 2006).

It should be noticed that the search range of t should be limited to $[a_1+2a_k, 2(a_1+2a_k)]$, for that (a_1+2a_k) is the low limit of the tag population, and numeric simulation presented in section 4 shows that the chance is rare for actual RFID tag population exceeds $2(a_1+2a_k)$.

As proposed in (Vogt 2002), accroding to the *Chebyshev's inequality*, the result for random experiment with random variable X is most likely results in the mathematical expects of X, and to resolve the collision caused by different number of RFID tags t with frame length s, the mathematical expects of $C_{0,t,s}$, $C_{1,t,s}$ and $C_{k,t,s}$ achieved in a frame can be calculated in advance. And if after the frame, if the actual amounts of idle, success and collision slots are a_0, a_1, and a_k, the population of RFID tags t can be calculated by minimizing the difference between the tuples $< a_0,\ a_1,\ a_k,>$ and $<C_{0,t,s},\ C_{1,t,s},\ C_{k,t,s}>$. That is to find the RFID tag population t, which satisfies

$$Min(f) = Minize \begin{vmatrix} C_{0,t,s} - a_0 \\ C_{1,t,s} - a_1 \\ C_{k,t,s} - a_k \end{vmatrix} \tag{8}$$

The search range of RFID tag population t can also be limited to the range $[(a_1+2a_k), 2(a_1+2a_k)]$, as discussed above.

These methods estimate the population of RFID tags within the interrogation zone of the RFID reader from different views, and the estimation accuracy achieved in each method needs to be examined with further numeric simulations.

3.3 The calculation of the optimal frame size

In the frame slotted ALOHA based RFID tag collision resolution protocols, once the population of RFID tags is known or can be estimated, the choice of the frame length adopted in the protocol affects the efficiency of the protocol and the latency of a collision resolution cycle. The choice of the optimal frame size should take into consideration of both the throughput of the protocol and the efficiency of RFID tag identification.

The throughput of the collision resolution protocol reflects the efficient use of the air interface, and is defined as

$$e_{th} \; = \; \frac{c_{1,t,s}}{s} = \frac{t(1 - 1/s)^{t-1}}{s} \tag{9}$$

where t is the RFID tag population, and s refers to the frame length adopted.

For e_{th} to achieve its maximize value, we need to fix t, and let $\frac{de_{th}}{ds} = 0$. It can be found that when $s=t$, e_{th} is maximinzed to be $\left(1 - \frac{1}{t}\right)^{t-1}$. Similarly, according to the law of large number, the stable maximum value of e_{th} can be calcuated as

$$max\,(e_{th}) \; = \lim_{t\to\infty}\left(1 - \frac{1}{t}\right)^{t-1} = e^{-1} = 0.368 \tag{10}$$

An alternative is to view this collision resolution process as a Poisson distribution process. The probability that t RFID tags transmit their identifiers back to the RFID reader in a time interval $[0\,,\,\tau]$ is in accordance with the Poisson distribution, and can be calculated with

$$p(X(\tau) = k) \; = \; \frac{(\lambda\tau)^k}{k!}e^{-\lambda\tau} \tag{11}$$

where $\lambda = \frac{t}{s}$.

Due to that the frame slotted ALOHA based RFID tag collision resolution protocols divide an identification frame into a series of discrete data slots, and each slot can be viewed as one time unit, if only one RFID tag chooses the time unit to transmit its identifier, no collision occurs and the RFID tag is identified successfully, so the throughput of the frame slotted ALOHA based collision resolution protocol can viewed as $p(X(1) = 1) = \lambda e^{-\lambda}$, and when $\lambda = 1$, p is maximized to be *0.368*. This also verifies that when $s=t$, the throughput of the protocol is maximized.

The throughputs achieved by the frame slotted ALOHA based RFID tag collision resolution protocols with different frame length in the identification of different amount of RFID tags are depicted in Fig. 2.

In the research of frame slotted ALOHA based RFID tag collision resolution protocols, throughput is often used to determine the optimal frame size adopted in the protocol. But we think that although throughput in an important issue to measure the efficient use of the communication channel, another key factor should be taken into consideration for the calculation of the optimal frame length is to consider the performance of the collision resolution protocol using the identification ratio of RFID tags achieved in a frame, which can be defined as $e_{s,t}$ and calcuated with
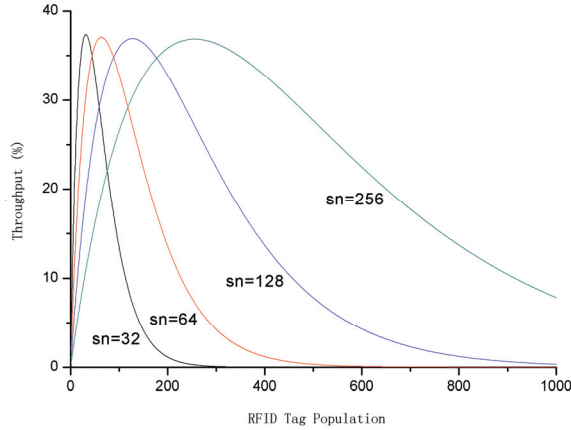
Fig. 2. The Throughputs Achieved by the Frame Slotted ALOHA Based RFID Tag Collision Protocols with Different Frame Length.

$$e_{s,t} = \frac{c_{1,t,s}}{t} = (1 - 1/s)^{t-1} \tag{12}$$

To find the maximum value of the identification ratio $e_{s,t}$, we also need to fix s, calculate $\frac{de_{s,t}}{ds}$, and let $\frac{de_{s,t}}{ds} = 0$, we get

$$
\begin{aligned}
\frac{de_{s,t}}{ds} &= \left(1 - \frac{1}{s}\right)^{t-1} + t\left(1 - \frac{1}{s}\right)^{t-1} ln\left(1 - \frac{1}{s}\right) \\
&= \left(1 - \frac{1}{s}\right)^{t-1} \left(1 + tln\left(1 - \frac{1}{s}\right)\right) = 0
\end{aligned} \tag{13}
$$

and then $s = \frac{1}{1 - e^{-\frac{1}{t}}} = 1 + \frac{1}{e^{\frac{1}{t}} - 1}$.

According to the discussion presented above for the identification of different amount of RFID tags in the vicinity of the RFID reader, the corresponding optimum frame length for the frame slotted ALOHA based protocol to achieve best identification ratio can be calculated. Due to that the frame legnth adopted in the protocol can only be chosen in the range of *[2,4,8,16,32,64,128,256]*, for the identification of *t* RFID tags, the appropriate frame length *s* should satisfy:

- $e_{s,t} > 2e_{\frac{s}{2},t}$, which means that the amount of RFID tags identified in a frame with frame length *s* should be more than that identified in two frames with frame length $\frac{s}{2}$, and

- $2e_{s,t} > e_{2s,t}$, means that the amount of RFID tags identified in two frames with frame length *s* should be more than that identified in a frame with frame length *2s*.

3.4 Collision resolution process based on the Markov chain

Suppose that in a collision resolution cycle of the frame slotted ALOHA based RFID tags collision resolution protocol, after the *i*th frames, the amount of identified RFID tags is *f(i)*,

then after the next frame, the amount of RFID tags identified should be $f(i+1)=f(i)+t_i$, where t_i is the amount of RFID tags which are newly identified in the frame $i+1$ but have not been identified in the previous frames. This specifies that the amount of RFID tags identified after frame $i+1$ depends solely on the amount of RFID tags identified after frame i, and this process can be viewed as a homogenous Markov chain.

The Markov chain is often defined using the transition matrix to specify the probability that a state changes to another. The elements of this Markov chain transition matrix for the identification of t RFID tags using the frame slotted ALOHA protocols can be calculated with

$$
q_{ij} = \begin{cases} 0 & (j < i) \\ \sum_{r=0}^{i} P(\mu_1 = r) \dfrac{\binom{i}{r}}{\binom{t}{r}} & (j = i) \\ \sum_{r=j-i}^{i} P(\mu_1 = r) \dfrac{\binom{t-i}{j-i}\binom{i}{r-j+i}}{\binom{t}{r}} & (j > i) \end{cases}
\tag{14}
$$

Each element q_{ij} specifies the probability that the amount of identified RFID tags changes from i to j after a frame.

The first situation specified in Eq. 14 will never occur due to that it is impossible that after a new frame the total amount of RFID tags identified is less than that identified before the frame.

The second situation specifies that the amount of RFID tags newly identified in the frame is 0, which means that all RFID tags which are identified without collision in this frame have been identified in the previous frames, and the current collision resolution cycle should be terminated because that the probability that new RFID tags can be detected in the following frames is also 0. The coefficients for such transition can be calculated with the equation $q_{ii} = 1 - \sum_{j=0,j\neq i}^{t} q_{ij} = 1 - \sum_{j=i+1}^{t} q_{ij}$.

For the third situation, of all t-i RFID tags not identified in the previous frame by the RFID reader, j-i RFID tags choose the success data slot to respond and are identified newly in the frame.

The values for elements in the first row of the transition matrix specifies the initial state of a collision resolution cycle, and should be set to $q_{0j} = \{1,0,\dots0\}$.

The Markov chain and corresponding transition matrix specifies the condition that a collision resolution cycle can terminate, and can be used to calculate the number of frames needed for the identification of t RFID tags.

3.5 The deployment of multiple RFID readers

Usually in a dense RFID tag environment, multiple RFID readers are deployed to facilitate the RFID tag identification cycle. Suppose that there are n readers deployed, and each reader resolves the RFID tag collision independently and reader-reader collision is resolved. For the overall identification accuracy α required by the application system, the accuracy γ which each RFID reader should achieve can be calculated as

$$
(1 - \gamma)^n \leq 1 - \alpha
\tag{15}
$$

and we have

$$\gamma \geq 1 - \sqrt[n]{1 - \alpha} \tag{16}$$

Table 1. shows that if overall identification accuracy required by the application systems is 99.0%, and multiple readers are deployed, the identification accuracy which each RFID reader should achieve. From Table 1, we can see that the deployment of multiple RFID reader decreases the accuracy requirement for each reader significantly, which will in return, facilitate the identification cycle greatly.

Number of RFID readers deployed	Identification accuracy required for each RFID reader
1	99.0%
2	90.0%
3	78.5%
4	68.4%
5	60.2%

Table 1. Identification Accuracy for Each RFID Reader

4. Numeric simulation and result analysis

4.1 The numeric simulation environment

To verify the research work presented in this chapter, numeric simulations and evaluations are performed. In the simulation, 100 randomly generated data sets are used, in each data set, there are 1000 randomly generated binary strings, and each of which represents the binary identifier of a RFID tag encoded with SGTIN-96 schema. The standard frame slotted ALOHA based RFID tag collision resolution protocols with different frame length are implemented and simulated with the C# programming language in Microsoft Visual Studio .NET 2005 for the measurements of their performances in resolving the collision caused by different amount of RFID tags contained in each data set, the results are recorded and averaged with the 100 data sets.

4.2 The accuracy of RFID tag population estimations

To find the accuracy for RFID tag population estimation of various methods discussed in section 3.1, simulations are performed, in which the frame size of the frame slotted ALOHA protocol is fixed to 256. The accuracies of the RFID tag population estimation methods presented in section 3.2 are measured with the mathematical means and variances of their estimation error ratios achieved in the simulations.

The mathematical means of the estimation error ratios for a RFID tag population estimation method is calculated as

$$\mu_{err} = \frac{\sum_{i=1}^{R} \dfrac{\hat{t} - t}{t}}{R} = \frac{\sum_{i=1}^{R} \hat{t}}{Rt} - 1 \tag{17}$$

And the mathematical variance of the estimation error ratio for a RFID tag population estimation method is calculated as

$$\sigma_{err} = \sqrt{\frac{\sum_{i=1}^{R}\left(\frac{\hat{t}-t}{t}-\mu_{err}\right)^2}{R-1}} \tag{17}$$

where t and $\hat{t}$ represent the actual and estimated RFID tag populations. R is the number of data sets used the simulation, and in this example, and is fixed to 100.

Fig. 3. shows the mathematical means of the RFID tag population estimation error ratios of the Vogt-1, Vogt-2, Cha-1, Cha-2 and Zhen-1 methods, from which it can be concluded that the Vogt-2 method performs better than other methods with stable means of error ratios around 0.

Fig. 4. shows the mathematical variances of the estimation error ratios of these methods, from which it can also been seen that although the variance of the tag population estimation ratios for Vogt-2 is the greatest, but is still within a satisfactory range.

For the tag population estimation using Vogt-2 and Cha-2, as we have discussed, search on tag population t is needed to find the minimal value of the evaluation function, and the search can be limited in the range [$a_1 + 2a_k$, $2(a_1 + 2a_k)$]. In the simulations, we examine the probability that the actual tag population is in the range, and the result is shown in Figure 6. From these simulations, we have observed that if the tag population is less than *3.2* times of the frame size, this upper limit *2(a_1 + 2a_k)* has never been exceeded.
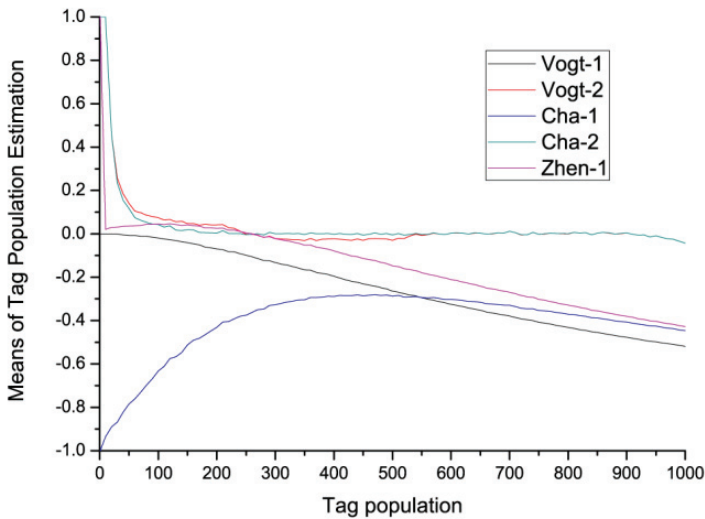
Fig. 3. Mathematical Means of the Tag Population Estimation Error Ratios
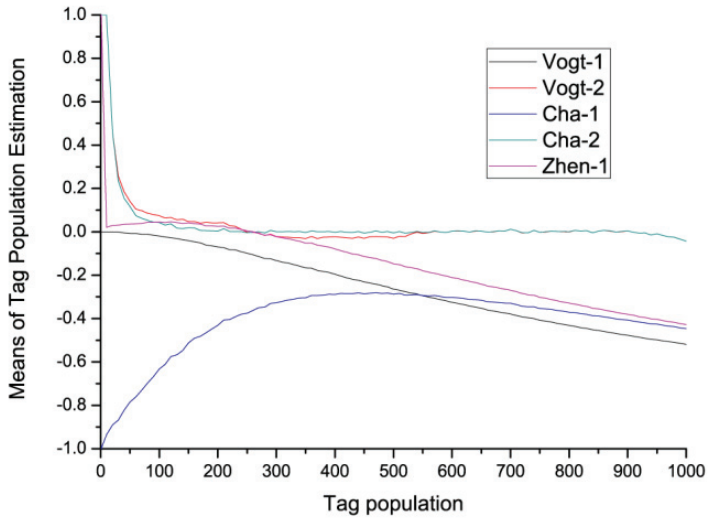
Fig. 4. Mathematical Variances of the Tag Population Estimation Error Ratios
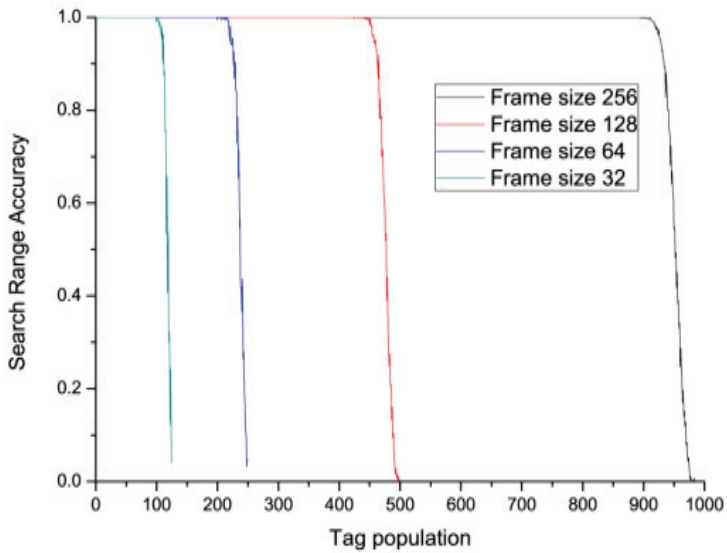
Fig. 5. The Probability that the Tag Population is within the Range

4.3 The efficiencies of the frame slotted ALOHA protocol and analysis

Fig. 6 shows the efficiency of the frame slotted ALOHA protocols with different frame length in resolving the collision caused by different amount of RFID tags. For the convenience of comparison, the protocol with frame length *s* is performed *256/s* frames, for example, the collison resolution protocol with frame size 16 is performed 16 frames. The efficiency is defined as the identification ratio of RFID tags in these frames, calculated with the number of RFID tags actually identified divided by the actual number of RFID tags.

From Fig. 6, it can be observed that as the population of RFID tags increase, the efficiency of frame slotted ALOHA protocol decreases rapidly.
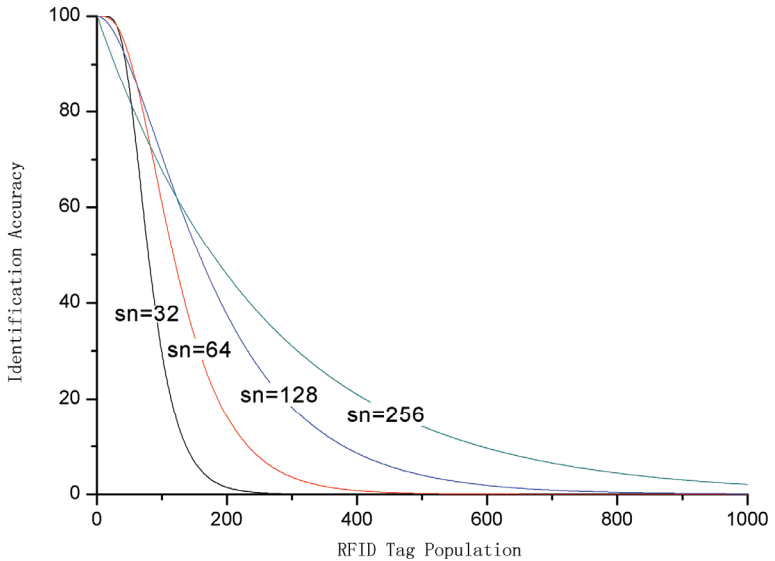
Fig. 6. The Efficiencies of Frame Slotted ALOHA Protocols with Different Frame Length

According to the calculation and simulation, the optimal frame length which the frame slotted ALOHA protocol should adopt in resolving the collision caused by different number of RFID tags is shown in Table 2.

RFID Tag Population	1-14	15-30	31-61	62-124	124~
Optimal Frame Length	16	32	64	128	256

Table 2. Optimal Frame Length for the Identification of Different Number of RFID tags.

4.4 Simulation and analysis of the identification process

Fig. 7 shows the amount of frames needed in resolving the collision caused by different amount of RFID tags using the frame slotted ALOHA based protocols with different frame length. It can been seen that as the RFID tag population increases, the amount of frames needed by these protocol will increase rapidly in exponential order.
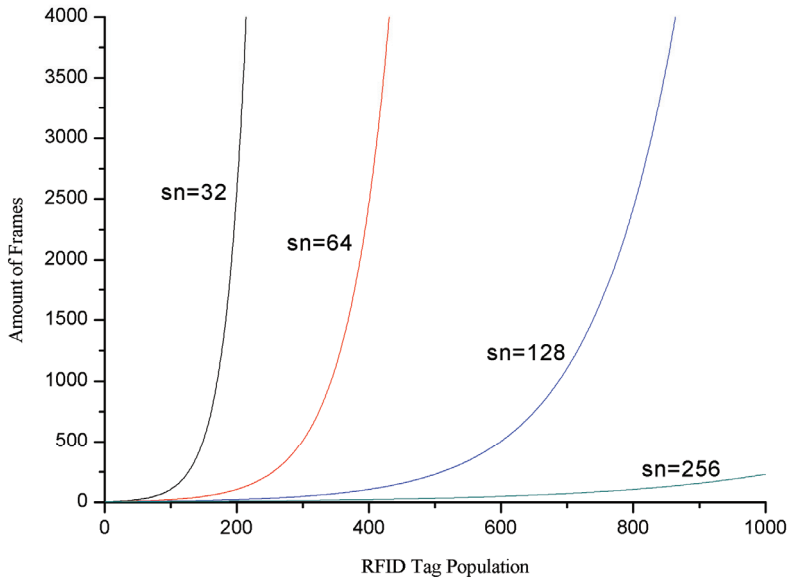
Fig. 7. Amount of Frames Needed for the Frame Slotted ALOHA Protocol with Different Frame Length

5. Conclusion

RFID holds the promise to enable human being to monitor the physical world with much fine granularity and bridge the huge gap between the physical item world with the virtual digital space. However, the collision occurred during the identification of multiple RFID tags prevents this promise to become a reality.

In this chapter, the frame slotted ALOHA based RFID tag collision resolution protocols are investigated, the stochastical distrubution model based on the binomial distrubution and the honomgenous Markov chain for the collision resolution process are proposed, the transisition matrix for the Markov chain is estabilished, vairous methods proposed for the estimation of RFID tag population within the vicinity of the RFID reader are examined and evalutaed. Some key factors that affect the performance of the protocols are evaluated and examined. Numeirc simulations are performed to verify the research presented in this chapter.

6. Acknowledgement

7. References

Abramson, N. (1970). The ALOHA system - another alternative for computer communications. in Proceeding of the 37th American Federation of Information Processing Societies Computer Conference: 281-285.

Bonuccelli, M. A., Lonetti, F., & Martelli. F. (2007). "Instant collision resolution for tag identification in RFID networks." Ad Hoc Networks 5(8): 1220-1232.

Cha, J. R., & Kim, J. H. (2006). Dynamic framed slotted ALOHA algorithms using fast tag estimation method for RFID system. in Proceeding of the 3rd IEEE Conference on Consumer Communications and Networking: 768-772.

Cha, J. R., & Kim, J. H. (2005). Novel anti-collision algorithms for fast object identification in RFID system. in Proceeding of the 11th International Conference onParallel and Distributed Systems: 63-67.

Engels, D. W., Foley. J. , Waldrop, J., Sarma, S., Brock, D. (2001). The networked physical world: an automated identication architecture. In Proceedings of the Second IEEE Workshop on Internet Applications.: 76-77.

Feller, W. (1970). An introduction to probability theory and its applications, Wiley Press.

Finkenzeller, F. (2003). RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification, John Wiley & Sons.

Kaplan, M. A. G., E. (1985). "Analytic Properties of Multiple-Access Trees." IEEE Transactions on Information Theory IT-31(2): 255- 263.

Kodialam, P. M., & Nandagopal, P. T. (2006). Fast and reliable estimation schemes in RFID systems. in Proceedings of the 12th annual international conference on Mobile computing and networking: 322-333.

Leong, K. S., Ng, M. L., Grasso, A. R.,& Cole, P. H. (2006). Synchronization of RFID Readers for Dense RFID Reader Environments. in Proceeding of the International Symposium on Applications and the Internet Workshops: 48-51.

Roberts, L. G. (1975). "ALOHA packet system with and without slots and capture." ACM SIGCOMM Computer Communication Review 5(2): 28-42.

Shih, D. H., Sun, P. L., Yen, D. C. & Huang, S. M. (2006). "Taxonomy and Survey of RFID Anti-collision Protocols." Computer Communications 29(1): 2150-2156.

Stanford, V. (2003). "Pervasive Computing Goes the Last Hundred Feet with RFID Systems." Pervasive Computing 2(2): 9-14.

Theodore, S. R. (2006). Wireless Communications: Principles and Practice, Addison Wesley/Pearson Publisher.

Vogt, H. (2002). Efficient Object Identification with Passive RFID Tags. in Proceeding of the International Conference on Pervasive Computing: 98-113.

Vogt, H. (2002). Multiple Object Identification with Passive RFID Tags. in Proceedings of IEEE International Conference on Systems, Man and Cybernetics: 1854-1858.

Waldrop, J., Engels, D., & Sarma, S. (2003). Colorwave: an Anti-collision Algorithm for the Reader Collision Problem. In Proceeding of the IEEE Wireless Communications and Networking Conference: 1206-1210.

Wu, N. C., Nystrom, M. A., Lin, T. R., & Yu, H. C. (2006). "Challenges to global RFID adoption." Technovation 26(12): 1317-1323.

Zhen, B., & Kobayashi, M., & Sgunuzy, M. (2005). "Frame ALOHA for Multiple RFID Objects Identification." IEICE Transactions on Communications 88(3): 991-999.

Anti-collision Algorithms for Multi-Tag RFID

GENG Shu-qin, WU Wu-chen, HOU Li-gang and ZHANG Wang
VLSI and System Lab, Beijing University of Technology, Beijing 100022,
P. R. China

1. Introduction

RFID is one of automatic technology to identify and collect object data quickly through RF digital signals. RFID increases productivity and convenience. RFID is used for hundreds, if not thousands, of applications such as preventing theft of automobiles and merchandise; gaining entrance to buildings; automating parking. But one of the largest disadvantages in RFID system is its low tag (transponder) identification efficiency by tag collision.

Collisions are divided into interrogator collisions and tag collisions. Interrogator collisions occur when neighbouring interrogators interrogate a tag simultaneously. Tag collision is the event that the interrogator (reader) cannot identify the data of tag when more than one tag occupies the same communication channel simultaneously. The reason is that whenever two or more users are transmitting on the shared channel simultaneously, a collision occurs and the data cannot be received correctly. This being the case, packets may have to be transmitted and retransmitted until eventually they are correctly received.

As the most RFID systems use passive tags, frame sizes are limited in the framed slotted ALOHA algorithm. Especially, since low-functional passive tags can neither detect collisions nor figure out neighboring tags, a tag collision gives rise to the need for a tag anti-collision protocol that enables the recognition of tags with few collisions and also executes in real-time. Active RFID tags contain an on-board battery. They can communicate with interrogator in far distance. Active tags can provide anti-collision by using various combinations of some methods including time scope and frequency scope. When the number of tags is large, for the conventional RFID anti-collision algorithm, the number of slots required to read the tags increases exponentially as the number of tags does. Some methods can solve this problem with complex algorithm consuming long communication time.

Based on the analysis above, a good tag collision arbitration protocol for RFID tags should have the following characteristics: First, a interrogator ought to identify all the tags inside its own reading range. Since the interrogator cannot estimate the number of tags precisely, the guarantee of recognizing all tags must be taken into consideration in the design of the tag hard system and anti-collision protocol. Second, a tag should be identified while consuming a small amount of resource, since the tag has low power. Thus, the tag anti-collision protocol must load the tag with the least possible communication time.

This paper presents an improved dynamic framed slotted aloha algorithm (IDFSA) that may solve this problem by dividing frequency of tags that is grouping the tags in different

frequency channel, reducing the number of slots and saving the communication time of grouping with estimation. The interrogator requests every frequency in turn to check the tags. In every frequency channel, the optimal frame size was set to enhance the system efficiency. This Algorithm has been used in the 433MHz RFID system. The system identification efficiency shows good performance.

2. Overview of several RFID anti-collision algorithms

In general, tag anti-collision protocols can be grouped into two broad categories: aloha-based protocols and tree-based protocols. The former is composed of such as aloha, slotted aloha, and frame slotted aloha that reduce the occurrence probability of tag collisions since tags transmit at distinct times. The later is composed of such as the binary tree protocol and the query tree protocol, based on the collision resolution algorithm studied in.

2.1 Tree-based RFID protocols
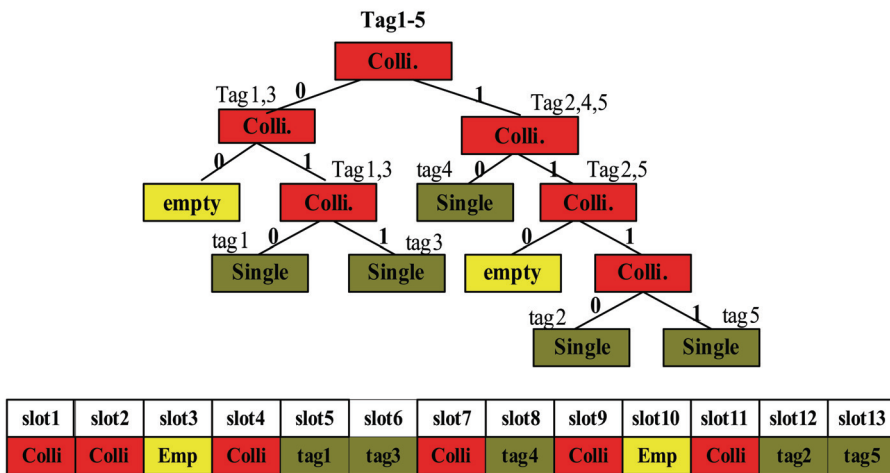
Fig. 1. An example of binary tree algorithm.

In tree-based RFID protocols, many protocols use binary tree algorithm. In this protocol, if a collision occurs in a timeslot, the colliding tags are randomly separated into two subgroups by independently selecting 0 or 1, until all tags are identified. The tags that select 0 transmit their IDs to a interrogator right away. If a collision occurs again, the collided tags are split again by selecting 0 or 1. The tags that select 1 wait until all the tags that select 0 are successfully identified by the interrogator. And if all the tags that select 0 are resolved, the tags that select 1 send their IDs to the interrogator. This procedure is repeated until there is no further collision.

An example presented in figure1 illustrates the process of the anti-collision scheme adopting the binary tree protocol. In the first timeslot, all tags select 0 or 1 randomly due to the collision. And tag 1 and 3 select 0. Both tags send their IDs at the next timeslot and are collided again. Tag1and 3 randomly select 1, no one select 0, then at the following timeslot,

it is empty. At the fourth timeslot, it is collided again. Tag1 transmits its ID at the fifth timeslot successfully by selecting 0, and the interrogator can then read the tag 3 because of no collision at the next timeslot. After the collision resolution of tag 1 and 3, tag2, 4 and 5 are collided at the seventh timeslot. Next, tag 4 selects 0 and tag 2and 5 select 1. Tag4 sends its ID at the eighth timeslot. Thus tag 2 and 5 send at the twelfth and thirteenth timeslot, respectively. Due to the no further collision, an interrogator finishes an identification process.

Figure 2 shows the procedure of query tree searching algorithm. At t0, the interrogator starts the anti-collision sequences by sending broadcast frame. Then at t1, the interrogator sends '0' to receive a tag's UID of the first bit equal to '0'. At stage t2, the interrogator sends '00' which is an accumulated UID stream that it is searching. By sending this accumulated UID stream, the tags are free for counting the stage information. Moreover, the only operations at tags are comparator or exclusive-OR operation. At stage t3, the interrogator receives '00XX' where 'X' means a collision. It sends '000' firstly, and then receives the first complete tag information '0000'. Again the reader sends '001' which results an identification if UID '0010'. This algorithm takes 8 stages to get the whole 4 UID stream. The de-activation frame transmission is omitted for the simplicity.

		Interrogator						
		t1	t2	t3	t4	t5	t6	t7
		Broad cast	0	00	000	001	01	1
Tag1	0000							
Tag2	0010							
Tag3	0101							
Tag4	1100							
Iterrogator	receive	xxxx	0xxx	00xx	0000	0010	0101	1100

Fig. 2. Sequences of the query tree searching scheme.

When the number of tag is small, tree-based protocols exhibit a reasonable performance. If the number of tags is large, at the early stage, they may experience poor performance because they might waste timeslots due to many collision slots until all tags are identified.

2.2 Basic framed slotted Aloha algorithm

BFSA algorithms use a fixed frame size and do not change the frame size until the process of tag identification is over. When an RFID interrogator attempts to read tags, the interrogator offers necessary information to the tags, such as the frame size and the random numbers. Receiving this information, tags transmit their IDs at the computed timeslots in the frame. If a timeslot has collision, the tags retransmit in the next read frame.

Figure 3 presents a process where tags are identified by BFSA. We assume that the frame size and the number of tags are 4 and 5, respectively. Firstly, Tag 4 transmits its ID at timeslot 1 of the frame 1. It is successfully identified. At the following timeslot, since a collision occurs, the interrogator can not read the tags correctly. Neither tag 3 nor tag 5 is identified by the interrogator due to the same reason. Thus, in the next frame, tag 1, 2, 3 and 5 must repeat the procedure until all tags are identified.

	T1	Frame1				T1	Frame2			
		Slot1	Slot2	Slot3	Slot4		Slot1	Slot2	Slot3	Slot4
	Que.	single	Colli.	Em.	Colli.	Que.	single	Colli.	single	Em.
Tag1										
Tag2										
Tag3										
Tag4										
Tag5										

Fig. 3. Basic framed slotted Aloha algorithm

Because of the fixed frame size of BFSA, implementation is rather easy. If there are too many tags, most of timeslots experience collisions, and none of tags may be identified during long time. And many timeslots may be wasted by idle slots if the number of timeslots in the frame is much larger than that of tags. Thus, it exhibits low performance of tag identification.

2.3 Dynamic framed slotted Aloha algorithms (DFSA)

Time Separation based anti-collision uses two or more different ID tags in which different tags have reply signals that occur in differing time positions. There are several methods of changing the frame size. One of the popular dynamic framed slotted ALOHA algorithm (DFSA) is that the interrogator regulates the number of slots of next frame using the last frame slots with collision, the number of the empty slots, and the slots filled with one tag.

In an RFID system, the interrogator can dominate the multiple-access procedure, including initiating communication, controlling read process, and receiving responses from tags. In a dynamic frame length ALOHA anti-collision algorithm, the interrogator initiates a read cycle by broadcasting a request command to all tags under its coverage. This request command also includes a dynamic parameter, called the frame length, by which each tag randomly selects one of the available time slots and transmits its ID at the selected time slot. For a given time slot, there are only three possible outcomes: idle, successful transmission (the slots filled with one tag), and collision. The channel is idle if no tag transmits its ID in the time slot. A successful transmission means one tag only sends it's ID. If two or more tags transmit in the same time slot, the interrogator suffers from collision and no tag can be read. After a read cycle, the interrogator can observe empty slots, singly occupied (or successful) slots, and collision slots. If the number of collision slots is greater than zero, the interrogator needs to estimate the number of tags that are present at the beginning of the read cycle according to the triple parameter and then to forecast the number of unread tags. According to the number of unread tags, the interrogator then determines an appropriate frame length for the next read cycle. When the number of slots with collision is over the upper threshold, the interrogator increases the number of slots. If the collision probability is smaller than the lower threshold, the interrogator decreases the number of slots. The read process stops when there is no collision in the read cycle. In the presence of a large amount of collision slots, it is reasonable to assume that the number of tags is great. In this case, the number of empty slots should be very small. In contrast, a large amount of empty slots means that just a few tags are present.
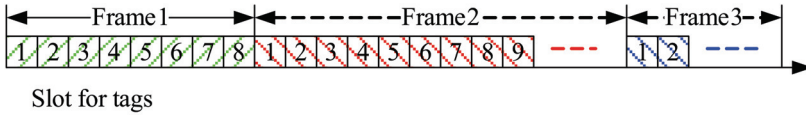
Fig. 4. Slots of Dynamic Framed Slotted ALOHA

DFSA algorithm can enhance channel usage efficiency and identify the tag efficiently because the interrogator regulates the number of slots according to the number of tags (see figure4). When the number of tags is small, DFSA algorithm can identify tags efficiently. However the maximum frame size for a concrete system is definite. When there are a number of tags, changing the frame size alone must be limited to the maximum frame size. So it is not fit for large tags system.

2.4 Enhanced dynamic framed slotted Aloha (EDFSA) algorithm

Collision efficiency is a function of the number of communicating tags presented within the interrogator communication range.

According Chebyshev's inequality, the outcome of a random experiment involving a random variable X is most likely somewhere near the expected value of X. Thus estimation function (1) measures the difference between the real results and the expected values to estimate the number of tags for which difference becomes minimal.

$$\varepsilon_{vd}(N, C_0, C_1, C_c) = \min \left| \begin{pmatrix} a_0^{N,n} \\ a_1^{N,n} \\ a_c^{N,n} \end{pmatrix} - \begin{pmatrix} C_0 \\ C_1 \\ C_c \end{pmatrix} \right| \tag{1}$$

The number of tags is estimated using both the number of slots N used in the read cycle and the results of the previous read cycle as a triple of numbers $< C_0, C_1, C_c >$ that quantify respectively the empty slots, slots filled with one tag, and slots with collision as Equation (1). In Equation (1), $< a_0^{N,n}, a_1^{N,n}, a_{\geq 2}^{N,n} >$ respectively denote the empty slots, slots filled with one tag, and slots with collision where the number of slots is N and the number of tags is n. Given N slots and n tags, the number 0, 1, r of tags in one slot is binomially distributed, and the expectation value for them is given by the follow eqation

$$a_r^{N,n} = N \binom{n}{r} \left(\frac{1}{N} \right)^r \left(1 - \frac{1}{N} \right)^{n-r} \tag{2}$$

When n is large, the optimal number of slots can be obtained by

$$N \approx n + 1, n \gg 1 \tag{3}$$

The above equation tells us that when the number of tags and the number of slots are approximately the same, the system efficiency becomes the maximum. According this, if the number of unread tags is sufficiently large, the tags can be grouped and allowing only one group to respond. The number of groups can be obtained by Modulo operation.

$$M = unread\ tags/N \tag{4}$$

In a word, when the number of unread tags is large, EDFSA divides the tags into groups with estimation. However, in practical system, when EDFSA based estimation grouping the number of unread tags is used, the time of interrogator command is long that can prolong the time of communication, which will influence the number of slots in a frame. So a simple easily realized method that improved dynamic framed slotted aloha algorithm (IDFSA) is presented as follows.

3. Improved dynamic framed slotted ALOHA (IDFSA) algorithm

This system experiment is based upon the assumptions that (a) Lots of tags are presented in the interrogator's field at the same time, the number of tags being present is not known in advance. The number of tags for every test is not known in advance. (b) Capture effect is not taken into consideration. (c) Experiment is trying to identify all tags presented in the field of the interrogator.

3.1 The description of IDFSA

For a practical system, the maximum time of one tag communication can be known, and the maximum number of slots in a frame can be calculated. The maximum total number of tags can be known too. If the number of tags is large, from equation (3), when the frame size N is equal to or close to the number of tags, the system efficiency becomes the maximum. In practical system, many RF chips have many frequency channels (e.g. nRF905). The tags can be divided into groups in different frequency channel to enhance the identification efficiency and to save the time of the command of the EDFSA. Grouping the tags can be accomplished in the system design period. Every group of tags has their own frequency. The number of frequency channels can be gotten as follows

$$G = n_{total} / N_{max} \qquad (5)$$

Where n_{total} is the number of system maximum total tags; N_{max} is the number of system maximum frame size. G is the number of frequency channels.

The maximum number of tags in every group is approximate to the maximum frame size. In one frame, according to the number of identified tags, C_1 the number of slots given one tag can be known. The collision C_c can be known by the difference of number of address match (AM) and data ready (DR). C_c is divided by frame size N_i, and then collision efficiency P_r can be gotten. Next frame size N_{i+1} can be known from (4). If 15%< C_c/ N_i <40 %, next frame size N_{i+1} does not change. If C_c/N_i<15%, next frame size N_{i+1} is $N_{i/2}$. If C_c/N_i>40%, next frame size N_{i+1} is $2N_i$. Until the interrogator identifies all tags in one channel, another channel can start to check.

$$N_{i+1} = \begin{cases} N_i / 2, & C_c / N_i < 15\% \\ N_{i,} & 15\% < C_c / N_i < 40\% \\ 2N_i & C_c / N_i > 40\% \end{cases} \qquad (6)$$

The frequency channel group can be made in the system design period not in the communication period, and the real-time estimation method is not used by the IDFSA. It not only saves the time of grouping with estimation during the communication, but also enhances the identification efficiency.

3.2 Performance analysis of IDFSA algorithm

For example, this system has total 210 tags; the maximum number of a frame size is 64 (see table 1). (3) is used in the condition that the number of tag is very large. According (3) the number of frequency channels is 210/64≈3.

In this system, the frequency channels of tags are 433 MHz, 433.4 MHz and 433.9MHz. For every frequency channel, the number of real time slots can be decided by IDFSA. The interrogator requests every frequency by turns to check different frequency tags. This can enhance the system efficiency.

n_{total}	N_{max}	$G_{channel}$
210	64	3

Table 1. The total system tags vs. maximum number of a frame size

Figure 5 is the system efficiency vs. groups and tags number. With the number of tag increasing, it can be seen that system efficiency of 3groups is higher than that of 2 groups; System efficiency of 2groups is higher than that of 1 groups.

In figure 4, it can be seen that the line groups 1, 2, 3 have two crossing point A, and B. According this, n_A and n_B can be obtained by

$$a_1^{N,n} / N = a_1^{N,n/2} / N \tag{7}$$

$$a_1^{N,n/2} / N = a_1^{N,n/3} / N \tag{8}$$

When N is 64 slots, n_A =88 and n_B=155.
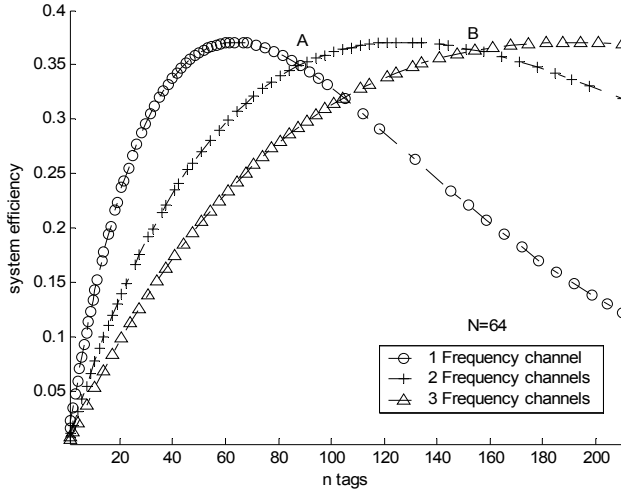
Fig. 5. System efficiency vs. frequency channels

When N is 64 and 89≤n≤154, to achieve the optimal system efficiency, the number of frequency channels can be 2. Similarly, when N is 64 and 155≤n≤218, to achieve the optimal system efficiency, the number of frequency channels can be 3. The result can be seen in table 2.

N_{total}	G	N/G	P_r
…	…	…	…
156~219	3	64	0.19516~0.31621
88~155	2	64	0.15061~0.34476
45~87	1	64	0.15606~0.40053
23~44	1	32	0.16073~0.40157
…	…	…	…

Table 2. Tags、frequency channels、the number of slots and collision efficiency
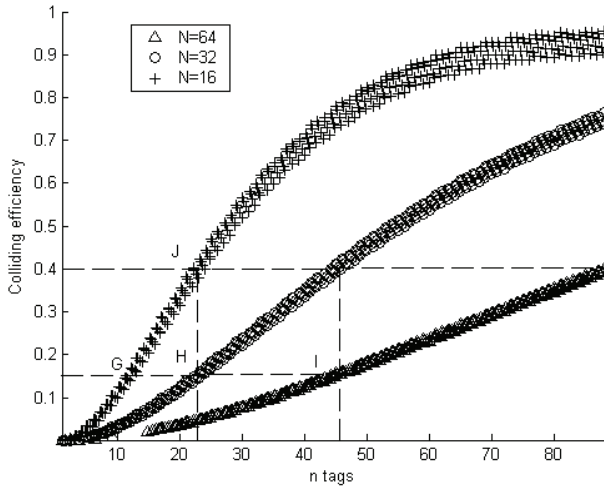
Fig. 6. The collision of slots number is $2N_i$、N_i、$N_i/2$

Figure6 is the collision efficiency of $2N_i$, N_i and $N_{i/2}$. When the collision efficiency is 15%, the number of tags is near to the down threshold the same as the table 1. When the collision efficiency is 40%, the number of tags is near to the upper threshold the same as the table 1. System identification efficiency is between 34.94% ~37.085% in one frame once a time.

Figure 7 is the collision efficiency and identification efficiency. The collision efficiency of the traditional method is between 30%-70%, and the system identification efficiency is the line between EF in figure 3. The collision efficiency of IDFSA is between 15%-40%, and the system efficiency is between 34.94% ~37.085% in one frame once a time. It is the line between CD in figure 7. It can be seen that system identification is higher than the traditional method.

4. Conclusion

It is an important problem to enhance the tag identification efficiency. When the number of tags is large, for the conventional RFID anti-collision algorithm the number of slots required to read the tags increases exponentially as the number of tags does. The proposed IDFSA algorithm may solve this problem by grouping the tags in different frequency channel, saving the time of grouping with estimation. In every frequency channel, DFSA is used to

set the optimal frame size to enhance the identification efficiency. This Algorithm is used in the 433MHz RFID system, tags anti-collision shows good performance.
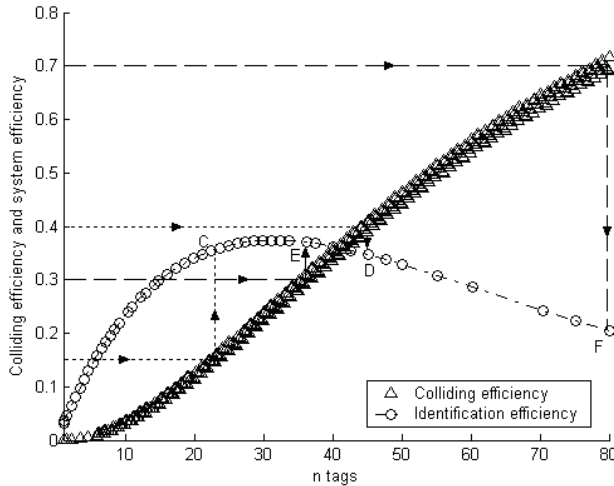
Fig. 7. Collision efficiency and identification efficiency

5. References

Engels, D. & Sarma S. (2001). The Reader Collision Problem, Technical Report MIT-AUTOID-WH007, Auto-ID Center, Nov. 2001.

Engels, D. et al, (2003). An Anticollision Algorithm for the Waldrop Reader Collision, *Proceedings of IEEE Int'l Conf. Comm.*, pp. 1206-1210, ISSN: 05361486, Anchorage, AK, United states, May 2003, Institute of Electrical and Electronics Engineers Inc., NJ

Finkenzeller, K. (2003). *RFID handbook - Second Edition,* John wiley & sons, ISBN: 0470844027, England

Haifeng, L. et al, (2006). A Modified Dynamic Binary Search Anti-collision Algorithm, *IET Conference Publications*, pp. 78, ISBN-10: 0863416446, Hangzhou, China, Nov. 2006, Institution of Engineering and Technology, SG1 2AY, United Kingdom.

Jae-Min, S. & Seong-Whan, K. (2006). Collision-Resilent Multi-state Query Tree Protocol for Fast RFID Tag Identification, *Conf. Rec. 2006 Int. Conf. Computational Intelligence and Security*, pp. 1159-1162. ISBN: 1-4244-0605-6, Guangzhou, Nov. 2006, Guangzhou

Junbong, E. & Tae-Jin, L. (2007). Framed-Slotted ALOHA with Estimation by Pilot Frame and Identification by Binary Selection for RFID Anti-collision. *2007 International Symposium on Communications and Information Technologies*, pp. 1027-1031, ISBN-13: 978-1-4244-0976-1, Sydney,. NSW, Australia, Oct. 2007, Inst. of Elec. and Elec. Eng. Computer Society, NJ 08855-1331

Landt, J. (2005). History of RFID. *IEEE Potentials*, Vol.24, No. 4, (Oct.-Nov. 2005) pp. 8 – 11, ISSN: 0278-6648

MIT Auto-ID Center (2003). Draft protocol specification for a 900MHz Class 0 Radio Frequency Identification Tag, http://www. epcglobalinc.org/, Feb., 2003. (binary tree)

Myung, J. et al, (2006). Adaptive Binary Splitting for Efficient RFID Tag Anti-Collision. *IEEE Comm. Letters*, vol. 10, no.3, (March 2006) page numbers (144-146), ISSN: 10897798

Myung, J. et al, (2006). Tag-splitting : Adaptive Collision Arbitration Protocols for RFID Tag Identification. *IEEE transactions on parallel and distributed systems*, Vol. 18, NO.6, (June 2007), page numbers (763-765), ISSN: 1045-9219Philips Semiconductors, UCODE, http://www.semiconductors. philips.com, 2005.

Sangho, S. & Sin-Chong, P. (2008). Efficient RFID Anti-collision scheme with multi-collision reflected frame request. *2009 6th IEEE Consumer Communications and Networking Conference,* pp. 1-5, ISBN-13: 9781424423095, Las Vegas, NV, United states, 1,2008, Inst. of Elec. and Elec. Eng. Computer Society, NJ 08855-1331, United States.

Sarma, S. et al, (2001). Radio Frequency Identification and the Electronic Product Code. *IEEE Micro*, Vol. 21, No. 6, (November/December 2001) pp. 50-54, ISSN: 02721732

Sarma, S. et al, (2002). RFID Systems and Security and Privacy Implications, *Proceedings of Workshop Cryptographic Hardware in Embedded Systems,* pp. 454-470, ISBN-10: 3 540 00409 2, Redwood Shores, CA, USA, Aug. 2002, Springer-Verlag, Berlin

Song-sen, Y. et al, (2007). RFID Anti-collision algorithm Based on Bi-directional Binary Exponential Index. *Proceedings of the IEEE International Conference on Automation and Logistics*, pp.2917-2921, Jinan, China, August 2007, Inst. of Elec. and Elec. Eng. Computer Society, NJ 08855-1331

Su-Ryun L. et al, (2005). An Enhanced Dynamic Framed Slotted ALOHA Algorithm for RFID Tag Identificatio, *Proceedings of Second Annual International Conference on Mobile and Ubiquitous Systems -Networking and Services*, pp. 1-7, ISBN-10: 0769523757, San Diego, CA, United states, July 2005, Institute of Electrical and Electronics Engineers Computer Society, Los Alamitos

Vogt, H. (2002). Efficient Object Identification with Passive RFID Tags, *Proceedings of Int'l Conf. Pervasive Computing*, pp. 98-113, ISSN : 15308669, Zurich, Switzerland, Apr. 2002, John wiley and sons Ltd, 2002, Berlin

Vogt.,H. (2002). Multiple Object Identification with Passive RFID Tags. *2002 IEEE International Conference on Systems*, PP. 651-656, ISSN: 08843627, Yasmine Hammamet, Tunisia, October 2002, Institute of Electrical and Electronics Engineers Inc., NJ

Weis, S. et al, (2003). Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems, *Proceedings of First Ann. Conf. Security in Pervasive Computing*, pp. 201-212, Boppard, Germany, Mar. 2003, Springer-Verlag, Berlin

Zhai,J. & Wang, G. (2005). An Anti-Collision Algorithm Using Two-Functioned Estimation for RFID Tags, *Proceedings of Int'l Conf. Computational Science and Its Applications*, pp. 702-711, Singapore, May 2005, Springer-Verlag, Berlin

Applications of RFID Systems - Localization and Speed Measurement

Valentin Popa, Eugen Coca and Mihai Dimian
Faculty of Electrical Engineering and Computer Science
Stefan cel Mare University of Suceava,
Romania

1. Introduction

Many efforts were made in the last years in order to develop new techniques for mobile objects identification, location and tracking. Radio Frequency Identification (RFID) systems are a possible solution to this problem. There are many different practical implementations of such systems, based on the use of radio waves from low frequencies to high frequencies. In this chapter we present a short review of existing RFID systems and an in depth analysis of one commercial development system. We also present a speed measurement application using the same RFID system. The last section of this chapter offers important electromagnetic compatibility (EMC) information regarding the use of high frequency RFID systems. All results are from experiments performed in real life conditions. EMC and speed measurements were performed in a 3 m semi-anechoic chamber using state-of-the-art equipments.

2. RFID locating systems

Localization of mobile objects has become of great interest during the last years and it is expected to further grow in the near future. There are many applications where precise positioning information is desired: goods and assets management, supply chain management, points of interest (POIs), proximity services, navigation and routing inside buildings, emergency services as defined by the E911 recommendations (FCC 1996) in North America and EU countries, etc. There are numerous outdoor solutions, based mainly on Global Positioning Systems (GPS) but there are also so-called inertial systems (INS). Solutions based on cellular phone networks signals are another good example of outdoor positioning service. For GPS based solution the precision of location is dictated by a sum of factors, almost all of them out of user control. Inertial systems can provide continuous position, velocity and orientation data that are accurate for short time intervals but are affected by drift due to sensors noise (Evennou & Marx, 2006). For indoor environments the outdoor solutions are, in most of the practical situations, not applicable. The main reason is that the received signal, affected by multiple reflection paths, absorptions and diffusion (Wolfle et al., 1999), is too weak to provide accurate location information. This introduces difficulties to use positioning techniques applied in cellular networks (time of arrival, angle of arrival, observed time reference, etc.) in order to provide accurate location information inside buildings or isolated areas. Indoor positioning systems should provide the accuracy desired by the context-aware applications that will be installed in that area.

There are three main techniques used to provide location information: triangulation, scene analysis and proximity (Finkenzeller 2003). These three techniques may be used separately or jointly. Indoor positioning systems may be divided into three main categories. First of all there are systems using specialized infrastructure, different from other wireless data communication networks. Second, there are systems based on wireless communication networks, using the same infrastructure and signals in order to obtain the location information. Third, there are mixed systems that use both wireless networks signals and other sources to achieve the goal. There are many implementations, we mention here several of them having something new in technology and/or the implementation comparing with previous systems (Gillieron et al., 2004; Gillieron & Merminod, 2003; Fontana 2008; D'Hoe et al., 2009; Priyantha et al. 2000; Van Diggelen & Abraham, 2001; De Luca et al., 2006; Ni et al., 2003; Bahl et al., 2000):

- Active Badge is a proximity system that uses infrared emission of small badges mounted on the moving objects. A central server receives the signals and provides location information as the positions of the receivers are known;
- Cricket system from MIT which is based on "beacons" transmitting an RF signal and an ultrasound wave to a receiver attached to the moving object. The receiver estimates its position by listening to the emissions of the beacons based on the difference of arrival time between the RF signal and the ultrasound wave;
- MotionStar is a magnetic tracker system which uses electromagnetic sensors to provide position information;
- MSR Easy Living uses computer vision techniques to recognize and locate objects in 3D;
- MSR Radar uses both triangulation based on the attenuation of the RF signal received and scene analysis;
- Pinpoint 3D-iD which uses the time-of-flight techniques for RF emitted and received signals to provide position information;
- Pseudolites are devices emulating the GPS satellite signals for indoor positioning;
- RFID Radar which used RF signals;
- SmartFloor utilizes pressure sensors integrated in the floor. The difference of pressure created by a person movement in the room is analyzed and transmitted to a server which provides the position of that person;
- SpotON is a location technology based on RF signals. The idea is to measure on the fixed receivers the strength of the RF signals emitted by the tags mounted on moving objects to be located.

3. Location applications using a RFID system

3.1 Introduction

RFID systems are still developing, despite the problems and discussions generated by privacy issues. Many commercially available systems using passive or active transponders provide only information regarding the identity (ID), memory content and in very few cases, the position of the transponders relative to a fixed point, usually the main antenna system. Very few progresses were made in the direction of using these systems for real-time position or speed measurements. One development system delivering accurate positioning information for active transponders is the RFID Radar from Trolley Scan.

3.2 RFID radar locating system description

The locating system we used to perform the location measurement tests is a mixed one, based on both ToA - Time of Arrival and AoA - Angle of Arrival methods (Coca & Popa, 2007). It uses a system based on one emitting antenna and two receiving ones. The working principle, mainly based on a tag-talks-first protocol (Coca et al., 2008), is as follows: when a transponder enters the area covered by the emitting antenna, it will send its ID and memory content. The signal transmitted by the transponder is received by two receiving antennas. Based on the time difference between the two received signals and the range data, it computes the angle and the distance information.

We used for our tests active long-range transponders of Claymore type. The system uses a central frequency of 870.00 MHz with a bandwidth of 10 kHz.

3.3 Experimental setup and measurement results

Experimental setup included an anechoic chamber, the RFID system with the antenna system and several transponders as shown in the figure bellow:
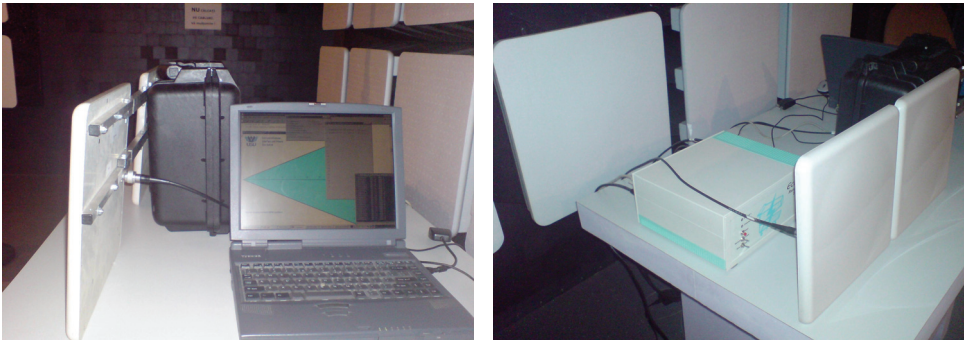
Fig. 1. The RFID system on the turn-table in the anechoic chamber with the control computer connected to the Ethernet network via optical-fibre isolated converters

The diagrams shown bellow are obtained from the signal transmitted between the receiving antennas pre-processor (and the demodulation block) and the digital processing board located inside the reader. The board is made using a Microchip Explorer 16 development board. We used for measurements a LeCroy 104Xi scope and 1/10 passive probes.

A typical signal received by the processing board, when only one active transponder is in the active area of the reader, is represented in Figure 2. When multiple transponders are located in the Radar range, the received signal contains multiple data streams. See, for example, Figure 3, which presents the signal received in the presence of four transponders. The information transmitted by the reader system to the processing board inside the reader is plotted in Figure 4.

The transmission duration for one transponder takes approximately 2.66 milliseconds for 1024 bits. The ID bits from the first part of the transmission, the so-called header, which is shown in the zoomed part at the bottom of Figure 5. The last part of the transmission contains the information regarding the angle and time relative to the receiving antennas.
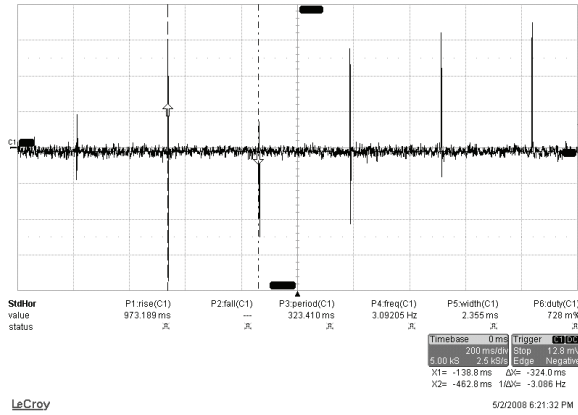
Fig. 2. Reading one transponder every 333 ms
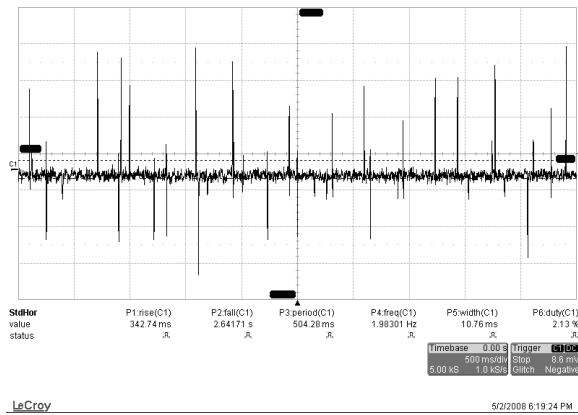
Fig. 3. Four transponders located in reader's range
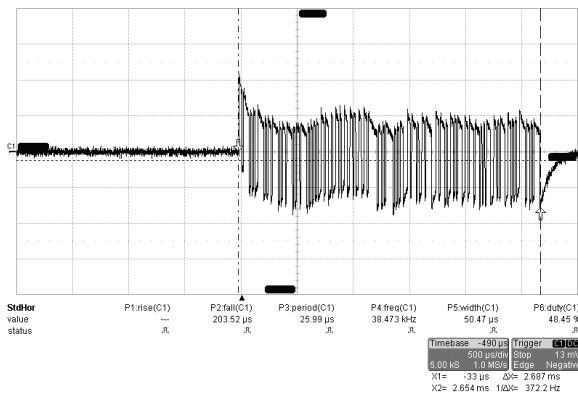
Fig. 4. Reading 1024 bits from one transponder takes 2.66 ms
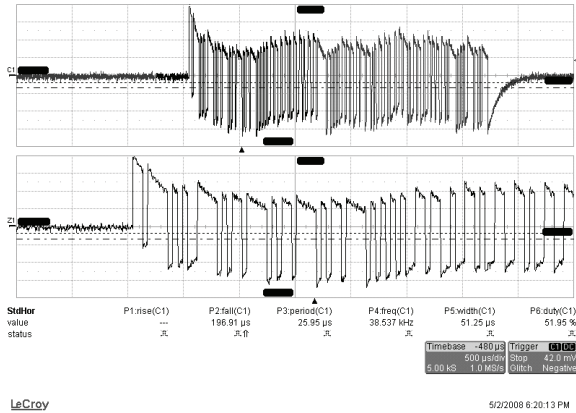
Fig. 5. Header data with one active transponder

As one can see in Figure 6, a bit is transmitted every 26 microseconds.
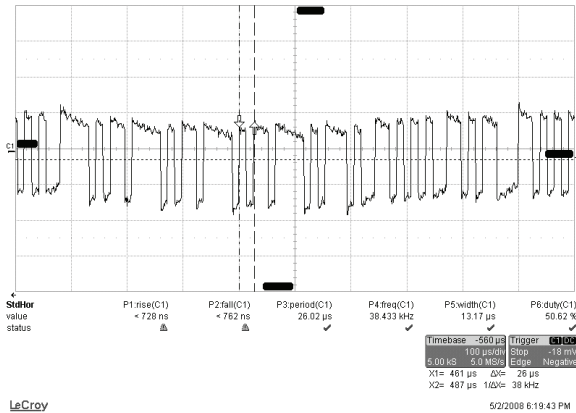
Fig. 6. Every bit takes about 26 μs to be transmitted

We made a series of tests during several days, in different environmental conditions and using various positions for the tags. Before starting the measurement session the receiver itself must be calibrated using, as recommended by the producer, an active tag. The tag was positioned in the centre in front of the antenna system at 9 m distance. The operation is mandatory as the cables length introduces delays in the signal path from the antenna to the receiver. We made a calibration for every site we made the measurements, in order to compensate the influence of antenna, cables and receiver positions.

For the tests we used all three types of tags provided (two active and one passive). The batteries voltages were checked to be at the nominal value before and after every individual test in order to be sure the results were not affected by the low supply voltage. For the first set of tests we used a real laboratory room (outdoor conditions), with a surface of about 165 square meters (7.5 meters x 22 meters). There were several wooden tables and chairs inside, but we did not changed their positions during the experiment. The antenna system was mounted about 1.4 meters height above the ground on a polystyrene stand, with no objects

in front. All tags were placed at the same height, but their positions were changed in front of the antenna. We used a notebook PC to run the control and command software.

We present only the relevant results of the tests and conclusions, very useful for future developments of this kind of localization systems. For the first result presented we used two long range tags, one Claymore (at 10 meters in front of the antenna) and one Stick type (at 5 meters) - Figure 7.
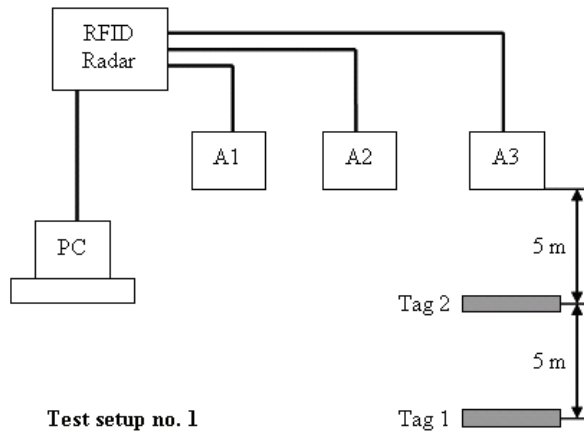
Fig. 7. Test setup for distance measurement from two tags - one at 5 m and the second at 10 m in front of the antenna
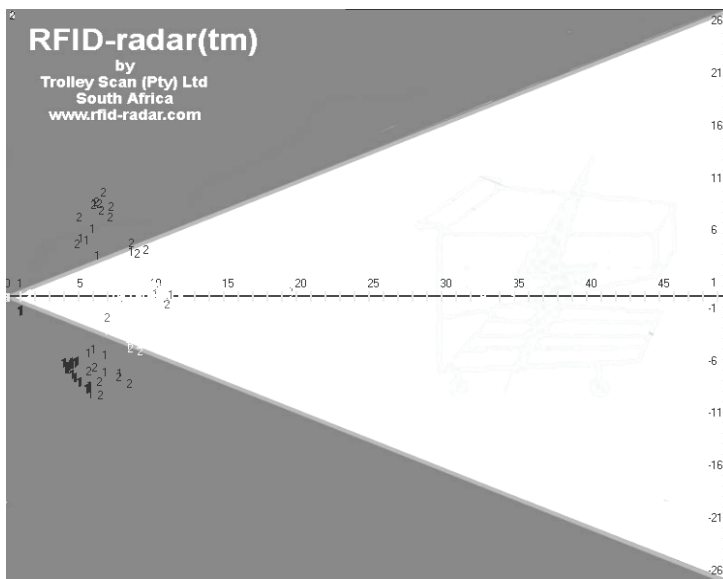
Fig. 8. Results for 2 active tags placed on 5 meters and 10 meters respectively, in front of the antenna system in a room

As one might see in Figure 8, the positions for each individual tag reported by the system were not stable enough in time. We run this measurement for several times using the same spatial configuration for all elements. The test presented here was made for duration of 4 hours. Analyzing the numerical results, we find out that 65% of cases where for the tag located at 5 meters the position was reported with an error less than 10% and for 47% of cases the results were affected by the same error for the tag located 10 meters in front of the antenna.

The second setup was the same in respect of location of the measurement, but one tag was moved more in front of the antenna system, at a distance of 20 meters. The results are practically the same regarding the position dispersion. Only in about 35% of all measurements for the tag situated at 20 meters the results were with an error less than 10%.
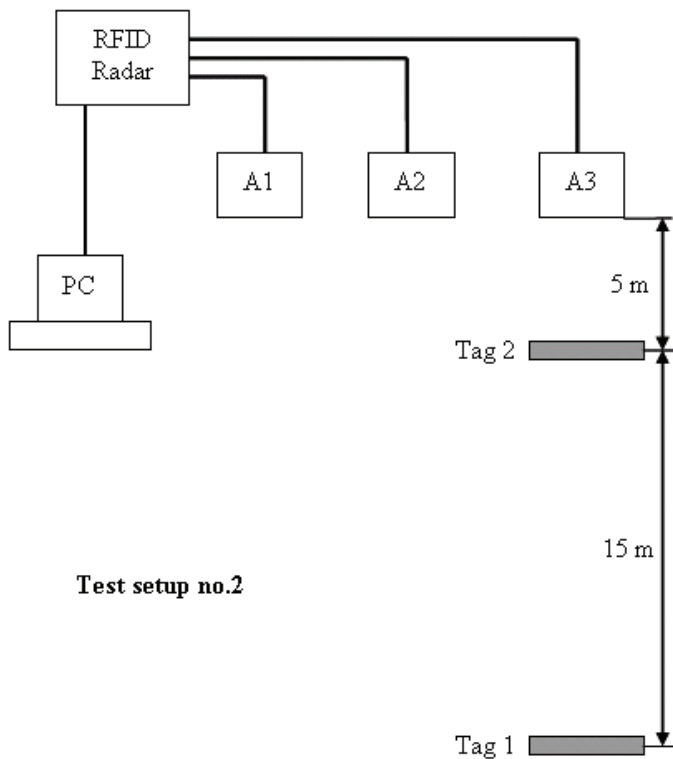
Fig. 9. Test setup for distance measurement for two tags - one at 5 m and the second at 20 m in front of the antenna

The measurements for the third case presented here were made in an open area, with no obstacles between the antenna system and the tags, using a tag placed at 10 meters in front of the antenna. The results obtained (Figure 10) are much better than the results from the measurements done in the laboratory. In this case (Figure 11) about 6 % of the measured distances were affected by an error more than 10 %.
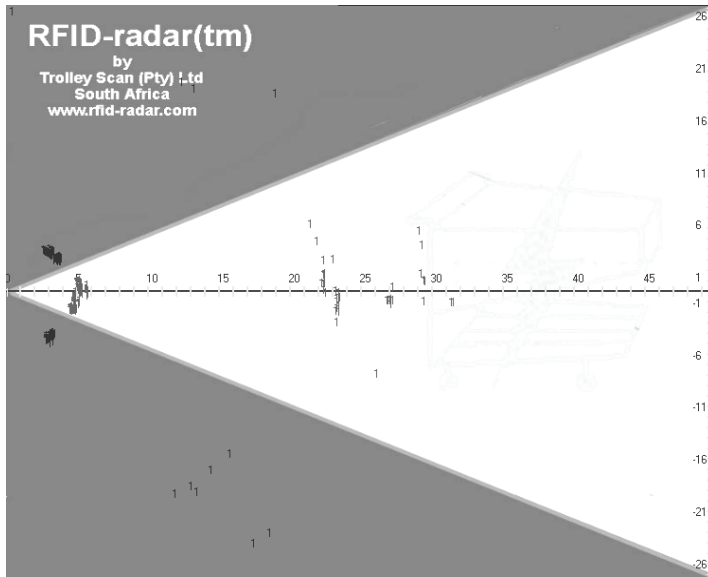
Fig. 10. Results for 2 active tags placed on 5 m and 20 m respectively, in front of the antenna system in a room
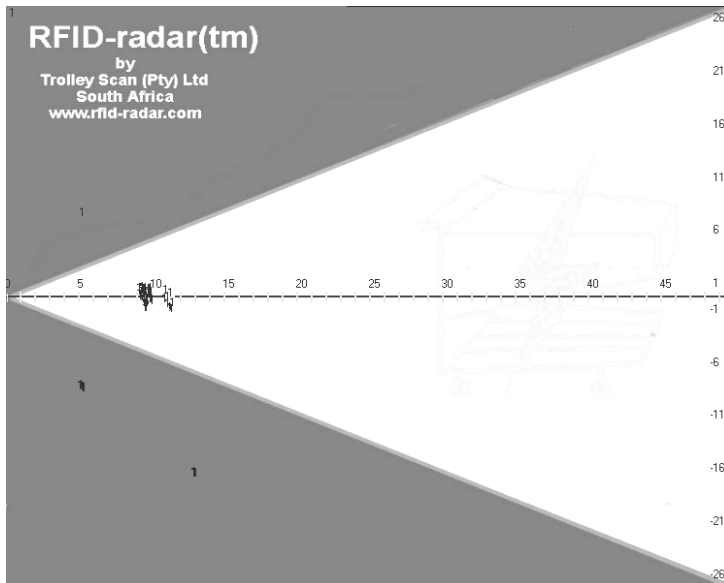
Fig. 11. Results for 1 active tag placed on 10 meters in front of the antenna system in an open-area site

4. Speed measurement applications using a RFID system

4.1 Calculating the speed using distance and angle information

In order to calculate the speed of the moving transponder we need to know the distances and the angles for two consecutive points P1 and P2. Our system provides distance and angle information for transponders in range. We assume the movement between these points is linear, which is a reasonable assumption for small distances.

The equipment computes the distance between the reference point "0" (located in the middle of the antenna system) and the transponder, as well as the angle between the reference axis and the line connecting "0" to the transponder. Let us consider that the moving object is located at points P1 and, respectively, P2, at two consecutive readings. Since the RFID radar provides the values of d1, d2, α1 and α2, one can determine the distance between the two points as it follows.
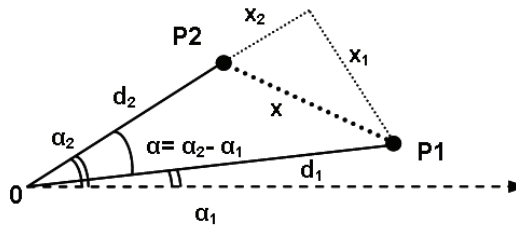
Fig. 12. Calculating the speed from two distances and two angles of two consecutive positions

By taking into account the diagram presented in Figure 12, one can derive the following expressions:

$$x = \sqrt{d_1^2 + d_2^2 - 2.d_1.d_2.\cos\alpha} \tag{1}$$

For the variables in these equations, we have the values determined at two time moments t_1 and t_2, so computing the speed of the object having attached the tag is obvious:

$$v = \frac{x}{\Delta t} = \frac{\sqrt{d_1^2 + d_2^2 - 2.d_1.d_2.\cos\alpha}}{t_2 - t_1} \tag{2}$$

4.2 Software diagram of the speed computing program

We have developed a software program to compute the speed based on the location information provided by the RFID reader and have made various performance tests using a RFID Radar. The program was developed on a platform running Windows XP as an operating system. We used Power Basic for writing and compiling the program, with very good results regarding the processing speed. Data was exchanged with the RFID system by using the RS232C serial interface. Results were delivered in a text box and were written in a text file on the local disk.

Figure 13 presents the software diagram for calculating the speed. The process begins with a system initialization procedure, followed by a calibration routine. After these operations, we
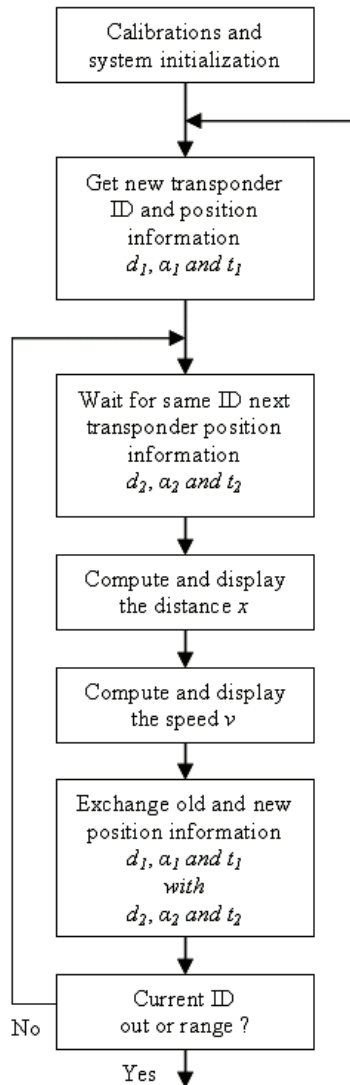
Fig. 13. Software diagram to calculate the transponder speed

wait for a transponder to come in the active range of the antennas. When the transponder enters the range, we get the current information, such as the unique ID, the location and time information. We do not need, and consequently, do not process any information stored in the transponder internal memory. After a delay of about 100 ms, the program enters a routine expecting the next reading. When receiving the same ID, the program gets the new values for location and time information, and then, it computes and displays the distance travelled by the transponder, and its speed.

When the current transponder ID is out of range, the program will acquire a new unique ID to calculate the new speed. If another transponder comes into the active range of the reader while the software is acquiring the speed for one transponder, the last one will not be read.

In Figure 14 one may see the distance calibration process necessary to be made at system initialization, before any speed measurement could be done.


```
BCBBB4581^   08.84 -001.1
BCBBB4581^   08.84 -001.2
BCBBB4581^   08.90 -001.2
BCBBB4581^   08.84 -001.3
CALIBRATE
BCBBB4581^   08.84 -001.3
BCBBB4581^   08.84 -001.2
BCBBB4581^   08.84 -001.3
BCBBB4581^   08.79 -001.3
BCBBB4581^   08.79 -000.1
BCBBB4581^   08.79  000.2
BCBBB4581^   08.83  000.4
BCBBB4581^   08.83  000.2
BCBBB4581^   08.83 -000.2
BCBBB4581^   08.82 -000.8
BCBBB4581^   08.76 -000.9
BCBBB4581^   08.82  000.0
BCBBB4581^   08.84  000.8
BCBBB4581^   08.84  000.0
BCBBB4581^   08.84 -001.1
B-08EA 090B 093B 098A 09C1 -01AE 0202 023A 025B 0267
A-0795 078A 0795 07C8 0883 -0005 001F 0054 00DB 013D
Calibration successful
BCBBB4581^   09.34 -001.1
```

Fig. 14. RFID system calibration using a transponder at 9 m distance from the antennas

A photo of the set-up in the anechoic chamber used for speed measurement tests is shown bellow:

Fig. 15. View of experimental setup in the anechoic chamber for speed measurements

We capture the output screen of the software we developed in Figure 16, showing the results with two active transponders moving in opposite directions with the same very low speed and, in Figure 17, a screen capture and a photo taken in order to compare the speed measured by the RFID system and the K Band radar gun.
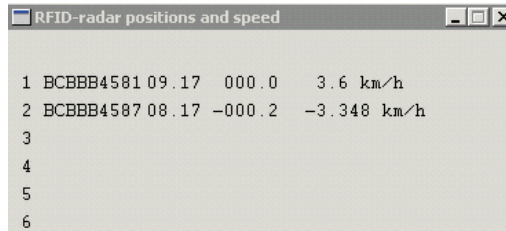
Fig. 16. Measurement screen showing two active transponders moving in opposite directions with the same speed
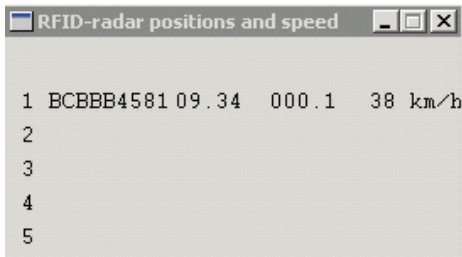
Fig. 17. Comparison between the speeds measured by the RFID system and a K-band radar

4.3 Theoretical and practical limitations for speed measurement

Considering the distance between the two receiving antennas of 31 cm (factory default), the system is able to solve angles between -30 and +30 degrees. The time spacing between two transponder transmissions is, as in Figure 2, about 333 milliseconds (three transmissions per second). Assuming that a transponder is moving such that the distance to the antenna system is constant, one can calculate the maximum theoretical speed that may be measured by using only the angle of arrival information. We also assume that we read two times the transponder in the whole working range of 60 degrees, the minimum information needed to compute the speed. If the reader does not receive the second transmitted signal, due to propagation issues, the speed can not be computed. The software will initiate a new measurement sequence by acquiring a new transponder ID. Table 1 presents a summary of the theoretical maximum speed as a function of the distance from the transponder to the antennas.

Distance to the antenna system (meters)	10	20	30	40	50
Distance traveled by the transponder (meters)	5.8	11	17	23	28
Speed (km/h)	62	124	187	249	311

Table 1. The theoretical maximum speed as a function of the distance between the transponder and the antenna system

In practical cases, more than two transmissions will be necessary in order to compute and have trusted information regarding the speed. Moreover, by reducing the angle between

two transmission points, let us say the system is not able to process the information in a timely manner or the radio signal is disturbed/attenuated due to propagation, the maximum measurable speed is much lower.

For the tests we made in a laboratory-controlled environment, with very low RF noise floor, we obtained the results presented in Table 2.

Distance to the antenna system (meters)	10	20	30	40	50
Speed (km/h)	6	24	32	36	n/a

Table 2. The maximum measured speed as a function of the distance between the transponder and the antenna system

Due to propagation issues generated by multiple reflections, we were not able to measure transponder speeds for distances over 40 meters.

5. Electromagnetic compatibility measurements on the RFID location system

We made a set of two measurements, one using a portable equipment for radiated emissions safety measurements (Narda SRM-3000) and a real life outdoor set-up and one using a certified set-up in an ISO 17025 accredited Electromagnetic Compatibility Laboratory - emclab.ro.

The RFID system we used for location and speed measurements is supposed to use a central frequency of 870.00 MHz with a bandwidth of 10 kHz. The frequency was chosen intentionally in order to be outside the GSM 900 band used in Europe (880.0 MHz - 915.0 MHz / 925.0 MHz - 960.0 MHz).

As we might see in the capture from the spectrum analyzer (see Figure 18), the electric field strength, at distance of 20 m in front of the reader antenna, is about 1.2 V/m, a value sufficiently low to be in accordance with the EMC safety levels in Europe and in the US. There are also visible, above the RF noise floor, the emissions from the GSM base stations (at 940 MHz and 960 MHz) located at about 600 meters from the location the tests were made.

Problems appear right in front and very close to the antenna system. In Figure 19 we have the field strength at a distance of 3 meters in front of the antennas. At this distance the emission level is about 39 V/m, a value high enough to worry. At about 30 cm near the emission antenna the field was about 200 V/m, the maximum value the spectrum analyzer could measure.

Regarding the bandwidth of the signal, we observe to be in the range of 10 to 25 kHz, small enough not to produce interference with other radio spectrum users. If many such devices are to be used simultaneously, on different central frequencies, there will be no problem if the spacing between to channel will be as low as 30 kHz.

A second set of measurements were made in an ISO 17025 accredited laboratory, using a certified set-up. The radiated emissions measurements have been made in a 3 m TDK semi-anechoic chamber using a Rohde & Schwarz - ESU 26 EMI Test Receiver, calibrated antennas and cables. The turntable and the antenna mast were operated by using an in-house made software program. Two international standards specify the emissions level and the performance characteristics of SRD-RFID equipments respectively: EN 55022 (CISPR 22) - "Information technology equipment - Radio disturbance characteristics - Limits and methods of measurements" for the emissions and EN 300-220 - "Electromagnetic
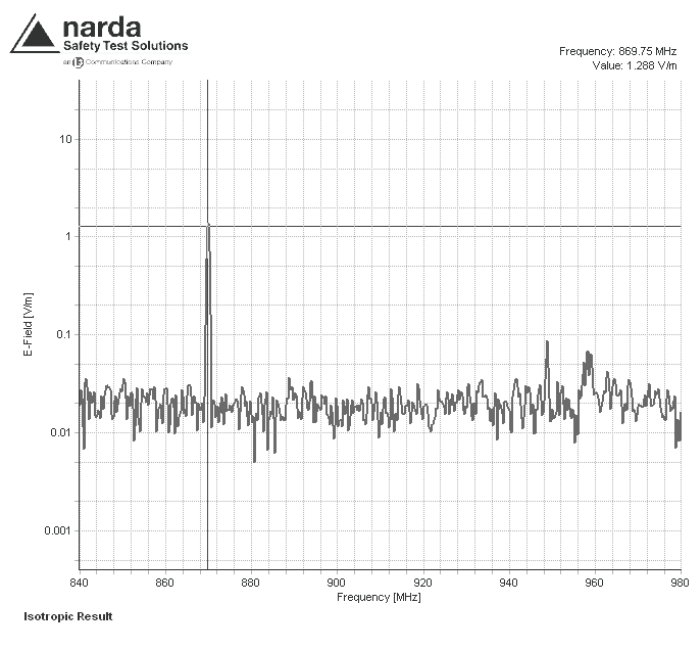
Fig. 18. Electric field magnitude at 20 m distance in front of the antenna
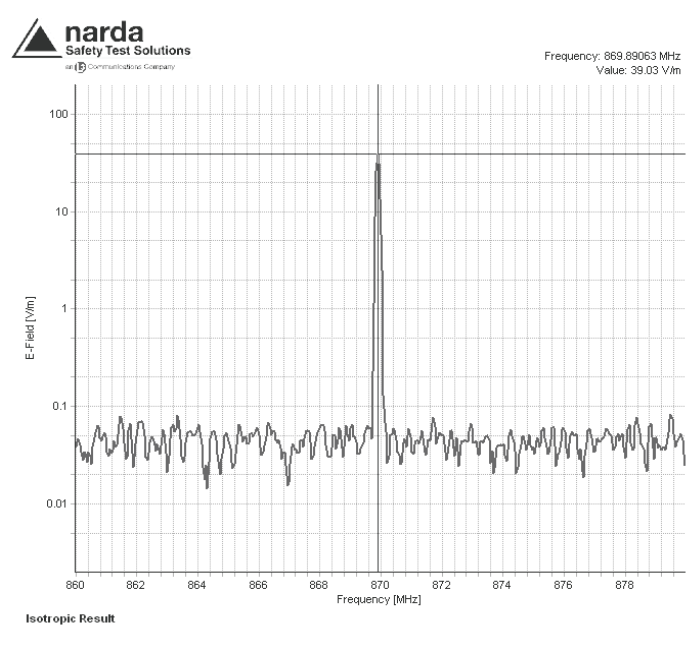
Fig. 19. Electric field magnitude at 3 m distance in front of the antenna

compatibility and Radio spectrum Matters (ERM); Short Range Devices (SRD)" for the operating performances and functional characteristics. A standard configuration was used for the test, as the equipment to be measured (EUT - Equipment Under Test) was positioned on a turn table at 0.8 meters above the ground and at 3 meters distance from the receiving antenna tip. During the measurements, the receiving antenna moved from 1 m to 4 m height and the EUT rotated 360 degrees, to find out the maximum emission level in the 30 to 1000 MHz band (as specified in the standards, in the final scan procedure, the operating frequencies were excluded from the measurement interval). We placed the transponders just in front of the RFID Radar antenna system. As stated in the standards above, the readings were made continuously, one measure per second using quasi-peak and peak detectors for the pre-scan and the final scan measurements respectively.

Table 3 shows the levels measured using this setup (we preserved also the peaks from the operating frequency range in order to compare them with the peaks outside this band and with the results from the first outdoor set-up). The limits used for calculations (QP Margin column) were 40 dB for 30 to 230 MHz and 47 dB for 230 MHz to 1000 MHz (as stated in CISPR 22 for 3 m test distance we have to add 20 dB per decade). We observe that outside the operating frequency band the emissions were below the limits with one notable

Freq (MHz)	Pol.	Tbl. Ang. (deg)	QP (dBuV)	Freq. peak (MHz)	QP Margin (dB)	QP Trace (dB)
188.7	H	65.5	33.20	184.01	-6.80	18.21
202.5	V	44.2	33.98	194.61	-6.02	18.11
865.2	H	18.2	89.00	869.91	42.00	65.36
865.2	V	153.2	72.54	869.91	25.54	48.90
867.0	H	17.7	88.70	869.92	41.70	65.06
867.0	V	150.5	42.38	869.92	-4.62	18.74
868.3	H	18.5	80.43	869.97	33.43	56.79
869.3	H	17.4	72.57	870.00	25.57	48.93
869.3	V	150.9	55.89	870.00	9.11	32.25
869.9	H	18.8	89.46	869.90	42.46	65.82
869.9	V	152.0	72.85	869.90	25.85	49.21
945.6	H	12.6	133.10	945.75	86.10	109.17
945.8	V	62.0	117.61	945.80	70.61	93.68

Table 3. The emission levels measured in the semi-anechoic chamber at 3 meters distance from the RFID Radar.

exception, at 945 MHz, where the electric field magnitude was over the limits specified in the standards. For the main operating frequency band, the emissions were very high, causing possible EMI problems for other electrical equipments operating nearby.

Regarding the safety aspects, there are problems due to very high emissions level, the field intensity measured being well higher than the maximum values permitted by the standard. In ETSI EN 300 220-1 V2.2.1 (2008-04) - Electromagnetic compatibility and Radio spectrum Matters (ERM), the power limit for devices operating between 30 MHz and 1.000 MHz, for all the bands reserved for short range devices, is 500 mW. There are other regulations in the EU where power levels up to 2 Watts are permitted for RFID systems with non/modulated carrier. Due to the operating principle, the RF power generator operating continuously, long time exposure to the EM field produced by the antenna RFID Radar system could be dangerous for humans.

6. Conclusion

RFID location systems for indoor and outdoor positioning are a promise for the future, even the performances of these systems are affected by many factors. We identified here that for a system working in the RF band near 900 MHz, the objects interposed between the antenna system and the tags to be located may have a great influence in terms of accuracy of the measurement results.

In closed areas multiple reflection paths may disturb the measurement systems, a percent of only 40 to 60 of total measurements are enough accurate to locate an object. In such conditions, there are small chances for this kind of systems to be used for high precision indoor applications requiring more than several tens of centimetres accuracy. The results obtained from the measurements we made in open area test sites are more promising, more than 93 percent of total result were not affected by notable errors.

For speed measurement of mobile objects by using RFID systems, we may conclude there are many aspects to solve before such systems may be used in commercial applications. Despite the precision for both passive and active transponders positioning is in the range of 10-30 centimetres for methods based on the time of arrival and angle of arrival, the performances obtained for speed measurements are not good enough when a large number of mobile objects are simultaneously in range. For a single transponder or a reduced number of transponders and small speeds, bellow 40 km/h, the speed measurement errors were below 30 %. For better speed measurement results we must combine the use of a RFID system for reading IDs and transponder internal memory contents with a classical radar system and process the results in a software interface.

Regarding the EMC aspects of this RFID location system, we may say, based on measurements presented here, that the electric field are high enough not to use this system indoors at distances less than 5 meters, if humans are present on a regular basis in that area. For applications in open areas, like access control for auto vehicles and many similar others, this kind of systems are very good.

7. References

Bahl, P.; Venkata, N.; Padmanabhan, N. & Balachandran, A. (2000). "Enhancements to the RADAR user location and tracking systems" *Microsoft Research Technical Report MSR-TR-2000-12*, February 2000

Coca, E. & Popa, V. (2007). "Experimental Results and EMC Considerations on RFID Location Systems", *Proceedings of the 1st International RFID Eurasia Conference*, 4-6

September 2007, Istanbul, Turkey, pp. 279-283, ISBN 978-975-01566-0-1, Digital Object Identifier 10.1109/RFIDEURASIA.2007.4368138

Coca, E.; Popa, V.; Găitan, V.; Turcu, C. O. & Turcu, Cr. (2008). "Speed Measurement of a Moving Object by Using a RFID Location System and Active Transponders", *Electronics and Electrical Engineering*, Lithuania, Nr. 8(88), 2008, ISSN 1392-1215

Van Diggelen, F. & Abraham, C. (2001). "Indoor GPS Technology", *CTIA*, Dallas, Texas, USA, May 2001

Evennou, F. & Marx, F. (2006). "Advanced Integration of WiFi and Inertial Navigation Systems for Indoor Mobile Positioning", *EURASIP Journal on Applied Signal Processing*, vol. 2006

FCC (1996). Docket no. 94-102, "Revision of the commission's rules to ensure compatibility with enhanced 911 emergency calling", *Tech. Rep. RM-8143*, July 1996

Finkenzeller, K. (2003). "*RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification*" John Wiley & Sons, New York, NY, USA, 2nd edition, 2003

Fontana, R. J. (2008). "Recent Applications of Ultra Wideband Radar and Communications Systems", http://www.multispectral.com

Gillieron, P.Y. & Merminod, B. (2003). "Personal navigation system for indoor applications", *Proceedings of the 11th IAIN World Congress*, Berlin, Germany, October 2003.

Gillieron, P.Y.; Buchel, D. & Spassov, I. (2004). "Indoor navigation performance analysis", *Proceedings of the 8th European Navigation Conference* (GNSS '04), Rotterdam, The Netherlands, May 2004

Hightower, J. & Borriello, G. (2001). "A survey and taxonomy of location systems for ubiquitous computing" *Tech. Rep. UWCSE 01-08-03*, University of Washington, Washington, DC, USA, August 2001

D'Hoe, K.; Van Nieuwenhuyse, A.; Ottoy, G.; De Strycker, L.; De Backer, L.; Goemaere, J. & Nauwelaers, B. (2009). "Influence of Different Types of Metal Plates on a High Frequency RFID Loop Antenna: Study and Design", *Advances in Electrical and Computer Engineering*, ISSN Print 1582-7445, ISSN On-line 1844-7600, vol. 9, no. 2, pp. 3-8, 2009. doi: 10.4316/AECE.2009.02001

De Luca, D.; Mazzenga, F.; Monti, C. & Vari, M. (2006). "Performance Evaluation of Indoor Localization Techniques Based on RF Power Measurements from Active or Passive Devices", *EURASIP Journal on Applied Signal Processing*, vol. 2006, Article ID 74796, 11 pages, 2006. doi:10.1155/ASP/2006/74796

Ni, L. M.; Liu, Y. & Patil, A. P. (2003). "LANDMARC: Indoor Location Sensing Using Active RFID", *Proceedings of the First IEEE International Conference on Pervasive Computing and Communications* (PerCom'03), pp. 407-415, 2003

Priyantha, N. B.; Chakraborty, A. & Baladrishnan, H. (2000). "The cricket location-support system", *Proceedings of the 6th Annual International Conference on Mobile Computing and Networking* (MOBICOM '00), pp. 32–43, Boston, Mass, USA, August 2000

Wolfle, G.; Wertz, P. & Landstorfer, F. M. (1999). "Performance, accuracy and generalization capability of indoor propagation models in different types of buildings," in *Proceedings of 10th IEEE International Symposium on Personal*, Indoor and Mobile Radio Communications (PIMRC '99), Osaka, Japan, September 1999

IP-based RFID Location System

Phuoc Nguyen Tran and Nadia Boukhatem
Computer Science and Network Department, Telecom ParisTech
46 rue Barrault, 75013 Paris,
France

1. Introduction

The Radio Frequency Identification (RFID) landscape has been radically changing since decades. It has been widely deployed by commercial and industrial organizations as well as government agencies with a wide range of applications. The RFID technology makes it possible to identify an object, to track it and learn its characteristics remotely, thanks to a label emitting radio waves, integrated or attached to the object. The RFID technology enables reading of labels even without direct line of sight and can pass through thin layers of material (paint, snow, etc.).

In the last few years, the RFID systems have evolved significantly in terms of technology and cost, enabling the RFID systems to stand out as the reference identification technology in numerous fields of applications such as asset tracking, logistics and supply chain management, animal tracking, healthcare, warehouse management, manufacturing engineering, automotive, contactless payments, etc. and mandated by industry giants (e.g. Wall-Mart, Target, Tesco and Albertson , etc.) and various government agencies (e.g. U.S. Department of Defense and Department of Homeland security, etc.).

One of the main advantages of the RFID technology is to provide a low cost and easy to install indoor location system compared to other positioning systems, such as Global Positioning System (GPS), Wi-Fi, Ultra-Wideband (UWB), Infrared (IR), and sensor based systems, etc.

A number of location sensing systems based on RFID technology have been proposed for indoor location services. SpotON [high] supports indoor location service using RFID technology based on radio signal strength analysis. LANMARC [ni] aims at increasing the accuracy in determining the RFID tag location and economizing the deployment cost of the system. To increase the accuracy, the system defines extra fixed location reference tags to help location calibration. In addition, an algorithm which reflects the relations of signal strengths by power level is developed in order to compute accurately the physical distance between the objects and the reader. FLEXOR [sue] is an improvement of LANDMARC to reduce the computational overhead in determining the location of the objects. The system divides the location area into cells which reduce the information used for localization calculation and decreases the computation load for the localization service. FERRET [liu] allows not only locating the RFID tagged objects, but also displaying the objects. The system uses an RFID reader embedded in a camera. FERRET uses also the algorithm which reflects the relations of signal strengths by power level to locate the objects. When the object is

found, the camera is turned on and displays their locations in real-time. In [teso], a sensing surface location system is proposed. The system is capable of tracking the objects within a closed environment. The objects (e.g devices, people, robots, ect.) integrate passive RFID readers. The RFID tags are installed as a grid representing the sensing surface. When the objects are on the surface, their locations are determined by mapping the RFID tag detected by the RFID readers and the physical surface of the RFID tags that it represents.

Besides, some solutions use Wi-Fi based Active RFID tags to expand the coverage zone using the Wi-Fi technology and provide complete wireless asset tracking and monitoring [aero] [ekah].

Considering the RFID management systems, the EPC global network developed by EPCglobal [jud][klau][epc] is the most representative. EPCglobal aims at standardizing the electronic product code (EPC) and the automatic identification system in the specific context of supply chain.

With the target to develop open RFID management systems and ease the integration of existing network services along with RFID location functionality, a number of works have been proposed.

SOA-oriented networked RFID system [zhang] proposes RFID location tracking service using web services. This system enables a distributed deployment of RFID solution which hides the diversity of the RFID hardware and underlying I/O communication protocols. Other works have investigated the use of session initiation protocol (SIP) [sip] as a control protocol for RFID management. SIP-based RFID management system (SRMS) [cho] uses SIP to manage the RFID tags. SRMS enhances the existing SIP architecture to perform RFID tags location registration and tracking procedures.

Our work is motivated by developing an IP-based RFID system management thus enabling low cost and large scale deployment of the RFID technology as well as openness and ease of integration with the existing IP-based services. In particular, a SIP implementation will have the benefit of providing a flexible integration of RFID location with the other corporate network services

Several motivations underpin our work:

- Propose a SIP-based RFID location system for indoor location. The current location of an object is determined by the identity of the reader when the object moves under its coverage zone.
- Integrate the RFID location services to the other IP services of the corporate network. This provides an integrated and flexible solution.
- More and more communication services such as location based services (LBS) are developed using the location information. The RFID based location system constitutes a good basis for providing such customized services.

1.1 Positioning systems

A positioning system allows determining the location of an object in space based on real-time collected information. It is also able to track the current location of an object moving through a space.

GPS system [joy][ivan] is today a widely deployed system. It provides the location of an object on the Earth (e.g. latitude and longitude). The current location of the objects moving through space could be visual using navigating map provided by the GPS providers. The GPS system is consisting of satellites in located geostationary orbit around the Earth and the GPS devices sending the updated location information to the satellites. If GPS seems to be a

good solution for the development of outdoor location systems, it is not able to be deployed inside buildings which impair the signal reception. It performs only in area where path between the GPS receiver and the sky is unobstructed. Moreover, the GPS devices require a dedicated chipset, a ground GPS system to extend signal range in large areas leading to a very costly deployment.

With the widespread adoption of wireless LANs, the Wi-Fi technology has been adopted as a tool for developing indoor positioning systems [joy][aero][ekah]. The Wi-Fi positioning system reuses the existing Wi-Fi infrastructures including the Wi-Fi access points, Wi-Fi-based radio tags integrated in the mobile devices and specific software allowing the system administrators to track the device location and analyze the position accuracy. The location of the devices is detected by measuring the signal strength indicator (RSSI). Although reusing the existing Wi-Fi infrastructure for developing the positioning system economizes the deployment cost, the Wi-Fi network cards and the management system deployment constitutes a non negligible cost.

UWB-based positioning system determines the current location of the object by scanning and continuously monitoring the UWB radio transceivers attached to clients [joy] [edoc]. The UWB-based system uses radio signal in a very wide bandwidth. The position calculation is based on time-of-arrival (TOA) technique. The main advantage of the UWB system is that it can be used at very low energy levels for short-range high-bandwidth communications. The issue is that the battery replacement constitutes a significant cost.

An object can be detected by an IR-based system [edoc] when it is present in the signal range of the IR detectors. The IR-based system enables to make a real-time tracking but it suffers from some shortcomings. First, it is not able to detect the object without direct line of sigh. The IR signal degrades when there is material obstacle such as walls, ceilings, and carton boxes because the signal cannot penetrate opaque materials. The IR tags and the IR detectors have to be installed everywhere to avoid loosing tracked objects. In addition, the IR system suffers from its sensitiveness to sunlight, direct light of sight requirement, cost of installation and maintenance at large scale.

Similar to most other positioning solutions, sensor-based systems [edoc] allow determining the location of the objects (tags) by using the Time Difference of Arrival (TDOA) technique. Each object has to integrate a battery-powered radio module that transmit frequently RF signal of its unique identification number. The sensors are installed to receive the RF signal. The object location is calculated by TDOA using the triangulation method based on the analysis of radio signal strength. However, the triangulation method using TDOA cannot provide an accurate position when the signal from the sensors to the tag is obstructed. Therefore, many sensor based systems are not widely deployed. Moreover, the obligation of battery integration into the tags limits the sensor network deployment capacities in terms of easy installation and cost.

The RFID technology allows locating the RFID tags attached to object at a close distance that use radio frequency (RF). These tags emit messages readable by RFID readers. Each RFID tag contains a unique identification number. There are two general categories of the RFID tags, active and passive, depending on their source of electrical power. Active RFID tags contain usually their own power source. Passive tags are powered from the signal of the readers. The RFID readers are also categorized into two general types: active and passive. Each type of reader can read specific type of tag [wein].

Compared to other positioning systems, the RFID technology provides following advantages:

- *Covers indoor areas* – fewer limitations compared to outdoor positing system such as GPS. In addition, the RFID technology can provide indoor positioning without any considerations of the direct line of sight unlike the other indoor positioning systems such as IR, Wi-Fi and sensor based systems.
- *Quick installation* –the investments can be quickly returned by installing the RFID system in days or weeks rather than months or years.
- *Cost effective* – indoor location systems such as Wi-Fi, UBW, and sensor based require battery installation. The RFID technology through using passive tags economizes the deployment cost.

1.2 RFID management systems

EPCglobal is an industry-driven organization which aims at standardizing the electronic product code (EPC) and the automatic identification system in the supply chain. The EPC code stored in the RFID tag allows uniquely identifying a physical object. EPCglobal defines EPCIS (EPC information system) for object identification. The EPCIS includes several components that allow accessing/exchanging information between the enterprises subscribing to the EPCglobal network. However, EPCglobal network is designed as a middleware solution with a specific goal.

While the Internet today is recognized as a network that is fundamentally changing social, political, and economic structures, the trend is that all network technologies converge to IP (Internet Protocol).

The term "Internet of Things" is a new notion that describes a number of technologies and research disciplines that enable the Internet to reach out into the real world of physical objects [itu]. The RFID technology is at the forefront of the Internet of Things. Today, it is one of the most promising automated identification technologies; by sticking an RFID tag to a physical object, it can be identified as a unique entity in the virtual world making the internet of things a reality.

Location awareness is a key feature of the ubiquitous computing, one of the advanced concepts of the Internet of things.

Many initiatives have been launched to develop open RFID based systems supporting location tracking.

The SOA-oriented networked RFID system [zhang] proposes a decentralized and plate-form independent location-tracking services using web services technology. The system provides a modular and layered application framework allowing scalability and extensibility.

SIP-based RFID management system (SRMS) [cho] uses session initiation protocol (SIP) [sip], which is an Internet standard protocol for session initiation management to manage the RFID tags. SRMS enhances the existing SIP architecture by introducing a surrogate user agent (SUA) and a SRMS name server (SNS). The SUA performs location registration procedures on behalf of RFID tags with limited capabilities, while the SNS provides name resolution services for location registration and tracking of RFID tags. The RFID-enabled location tracking system (SIP-RLTS) [zang] also based on SIP is proposed to support the location management. The SIP-RLTS solution uses the SIP event notification model to support the PUSH and PULL operation needed by the location service.

1.3 Contributions and organization

The contributions of this chapter are as follows:

- Design and specify an IP-based RFID architecture for location management.
- The location service implements two main functions: location and tracking. The location function aims at registering the current location of the RFID objects while the tracking function returns their current location.
- The implementation system defines an interface, which interconnects the RFID system to the existing communication infrastructure and services. With this interface, the location system is notified the RFID objects located in the detection area of the RFID reader, via entering and leaving events.
- The validation of the IP-based RFID location management system using the *Session Initiation Protocol (SIP)* [sip] is presented.

The chapter is organized as follows. Section 2 presents a motivating scenario that shows the benefits of location management services in daily life. In section 3, we identify different requirements and functions of the IP-based RFID architecture. The SIP-based implementation is presented in section 4. Section 5 concludes the chapter with further works.

2. Application scenario

In this section, we present an application scenario to highlight the motivations of the service location development.

Consider a hospital environment where the staff has a business (or access) card that incorporates an RFID tag. An RFID tag can also be added to any medical equipment (defibrillators, portable scanner, etc.). RFID readers are scattered throughout the grounds of the hospital mainly at strategic locations or crossing such as doors. Doctors may have to move between different departments and buildings and thus among several RFID readers. The latter, through the tracking system, update their current location. If a nurse, for example, seeks to reach a doctor, she can use the location system to identify where the doctor is. The same goes for finding medical equipment more quickly.

3. The IP-based RFID architecture

3.1 Architecture requirements

As a first step of our work, we identify the requirements of the IP-based RFID location system. As presented above, the RFID technology is today considered as a cost effective method for indoor location management. However, the RFID management systems are dedicated, relatively expensive and do not inter-operate with the classical communication devices such as PDA, mobile phone, smart-phone, laptop, etc. In our context, we aim at providing a communication infrastructure which integrates both the tagged devices (RFID) and classical devices, and defines a location system based on RFID. From an operational point of view, the communication infrastructure must provide a location service based on RFID and may support the following requirements:

3.1.1 Location function

The location function should allow any objects to indicate their current location. The RFID readers play a significant role in detecting the tagged objects under their detection zone.

We should distinguish two types of location. *Network location* - which indicates the IP address of the RFID reader the tagged object is under coverage area. In our system the reader IP address of the servers also as an identity of the reader. *Geographical location* -

which indicates where, geographically, the object is. The geographical location indicate the name of the room where the RFID reader is (e.g., the reader IPX is in the room 234 of the building C). A more accurate position in the form of 3D coordinates may be provided using, for example, sophisticated location mechanisms involving many readers.

Note that, it should be possible to derive from the network location the geographical location and vice versa. Thus, an RFID reader name should be associated to its IP address.

To determine the current location of an object, the location-tracking system must provide a means for recording and maintaining the current location. A database location should be installed.

Moreover, the RFID readers must support the registration procedure that allows registering the RFID tags at the location database when it enters the RFID reader coverage zone. Thus, when a RFID reader detects that an object has entered its detection zone, it must initiate a register request, in particular, indicate the corresponding <RFID *tag, IP address of the RFID reader*>. The system must also support functions to notify a particular object has left the detection zone of the reader.

3.1.2 Tracking function
This function allows the system to determine the current location of the object. It returns, in particular, its current location.

3.1.3 Integration of the RFID system to existing communication infrastructure
To seamlessly integrate the RFID system to the communication infrastructure and associated services, a communication interface between the reader and the communication infrastructure must be defined. Once a new tagged object is detected by the reader, the interface must detect this event and initiate a registration request. If a tagged object leaves the reader coverage areas, a de-registration must be initiated. Concretely, the communication interface functions should either be integrated into the reader if available resources are provided or exist independently.

3.2 Functional architecture
Based on the requirements above, we define a functional architecture of the RFID location system (figure 1).
The architecture includes the following:
- *RFID Readers and RFID tags:* RFID readers are installed to read information from RFID tags. The readers transmit the information obtained to RFID middleware.
- RFID middleware performs the collecting and filtering functions. *The RCOM interface* ensures the integration of the RFID system to the communication infrastructure. It notifies that an object enters the reader detection area or leaves it.
- *Location service* includes two functions: location and tracking. These functions interact with the location database which, in particular, is responsible of inferring the current location of the object after a tracking request.

3.3 Performance and security
Scalability is a significant feature of an RFID based system that usually runs a very large number of tags. The system must be designed so that its performance is not altered when the number of tagged items to be processed increases.
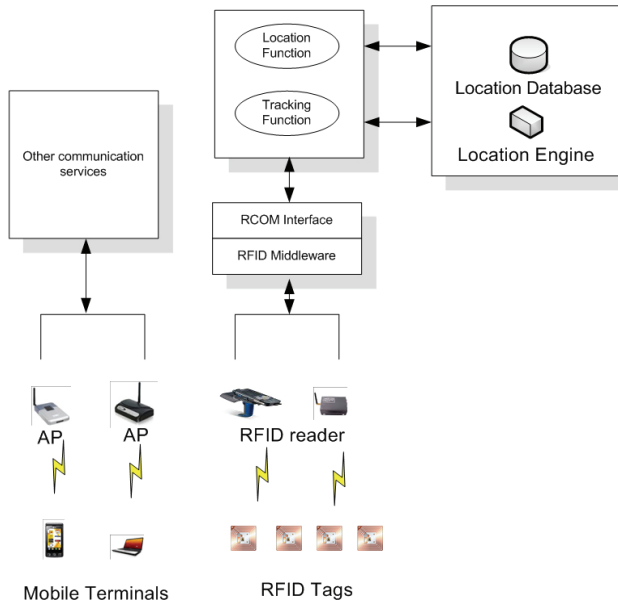
Fig. 1. Functional architecture of RFID based location system

As shown in Figure 1, the architecture of the location system is relatively centralized around the location server and the system performance is highly depended on the capacity of this server (CPU, memory, bandwidth). This capacity could be, for example, estimated by the number of queries per second that the server can process.

The location system requires various needs in terms of security. Firstly, accessing the location service should be provided only to authorized users. In addition, the location information exchange must be secured, in particular, the messages between the location server and the readers (e.g., the registration functions). The security of data transfer between the tags and readers should also be ensured. .

4. SIP-based implementation

In order to implement the location system specified above we choose to use the session initiation protocol (SIP) for several reasons:
- SIP allows easy implementation of the RFID based location service.
- SIP is widely used for VoIP (voice Over IP) services which are today an integral part of the corporate communication infrastructure. Assuming that a VoIP infrastructure is already deployed, our location service can easily be integrated into the infrastructure with a low cost deployment.

4.1 SIP model overview
The SIP architecture model is based on the concepts of SIP server (s) and SIP user agents (UA). An UA is a software entity that initiates SIP requests (UAC: UA Client) and returns SIP responses (UAS: UA Server). A SIP server can implement one or several of the following functions: *registration, proxy,* and *redirect.*

A *registration server* or *Registrar* is a server that accepts SIP requests (e.g. *SIP REGISTER*) and the role of which is to register the current location of the UA.

A *proxy server's* role is to route SIP messages. For this purpose, the *proxy server* uses the SIP destination represented by an URI (Uniform Resource Identifier) and the location service to determine the current location of the destination.

A *redirect server* is a server that responds to a *SIP INVITE* request by sending a *3xx* message type to indicate the UA the current location of the destination to reach. Unlike *proxy server*, *redirect server* does not route SIP requests, it indicates the UA the location where it can route the request.

Note that a UA must register its current location prior to initiate a SIP session.

4.2 SIP-based location system architecture

The application of the SIP model to the specification described above requires the RCOM interface to behave as a SIP UA. A SIP server that performs the *Registrar* function has to be defined to handle the registration requests initiated by the UA. The SIP server interacts with the location database to record the current location.

To support the tracking function, the SIP server should integrate *proxy and redirect* functions. The *redirect* function is used when there is a Tracking request. The *redirect server* responds by indicating the current location using a *3xx* response type. The *proxy* function occurs when the tracked object is managed by other SIP servers.

The system architecture is shown in Figure 2.
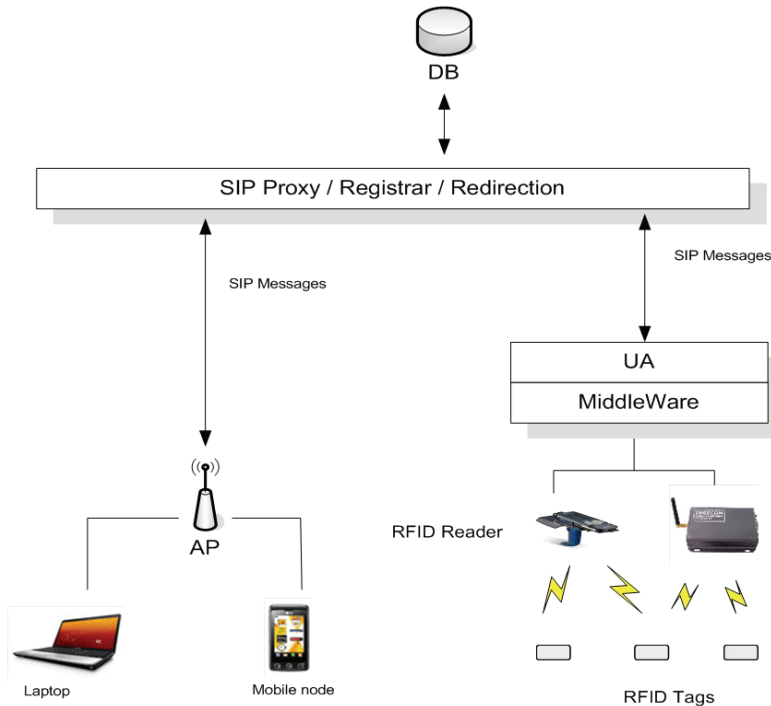
Fig. 2. SIP-based location system architecture

As shown in the previous section, the location of a tag or object is mainly determined by the IP address of the reader to which it is attached.

In this specification, each RFID tag is associated with a SIP URI (Uniform Resource Identifier) which includes the RFID tag value and the reader's IP address to which this tag is attached. This URI reflects the current location of the RFID tag.

One of challenges of the RFID implementation is how to transform the RFID raw data into an understandable format which is directly used by the backend applications (e.g. tracking application). The location database is responsible for managing and generating the understandable format of location data.

Our location system database defines 4 main tables:

RFID-Location-Event table contains information on the RFID tag and its current network location. This information includes the RFID tag of the object, the IP address of the reader to which the tag is attached, and the timestamp which indicates the instant of detection of the tag object by the reader. An example of this table is given in table 1.

Timestamp	RFID Tag	Object	IP Reader
0112200912012030	1a2e3f13ah	Enter	137.194.204.69
0112200913201734	1a2e3f43ed	Enter	137.194.204.69
0112200914012436	1a2e3f13ae	Leave	137.194.200.80
0112200918012445	1a2e4f5e6a	Enter	137.194.203.100

Table 1. RFID-Location-Event table example

RFID-Reader-Location table contains the geographical location of the RFID reader. This table maintains an association between the geographical location of the RFID reader and its IP address. An example of this table is given in table 2.

IP Reader	Location
137.194.204.69	Room C-208
137.194.200.80	Office 1B
137.194.203.100	Lab. 103

Table 2. RFID-Reader-Location table example

RFID-Name table contains the name of the object (or person) associated with the RFID tag (Table 3).

RFID Tag	RFID Name
1a2e3f13ah	Dr. John
1a2e3f43ed	Mr. Smith (Patient)
1a2e3f13ae	Ms. Mary's Laptop
1a2e4f5e6a	Mrs. Rose's cell phone

Table 3. RFID-Name table example

RFID-DB table (an example given by Table 4) is generated by the Location Server when the tracking system has to determine the current location of the object. The Location Server combines the various tables depending on whether the tracking service uses the RFID tag or the object name as identity to look for their location. If, for example, the operation of the tracking searches the geographical location of a given object, the location engine combines the three tables: *RFID-Location-Event, RFID-Reader-Location* and *RFID-Name* to generate the current location of the RFID tags in the *RFID-DB* table.

RFID Name	RFID Tag	IP Reader	Location
Dr. John	1a2e3f13ah	137.194.204.69	Room C-208

Table 4. RFID-DB table example

4.3 Location function - SIP registration

As mentioned above, the RCOM interface integrating the UA indicates the presence of tags in the detection zone of the reader by generating registration requests. *SIP REGISTER* messages are sent to the SIP server. Each *SIP REGISTER* message indicates in its *Contact field* the RFID tag and the IP address associated to the reader. The SIP server updates the location database. When an RFID tag leaves the area of the reader, a *SIP REGISTER* request with a field "Expires" = 0 is generated.

Figure 3 represents the following registration procedure. As an illustration, we assume that an RFID tag is sticked to the business card of Dr. John who is a doctor at hospital A.

Step 1.   When Dr. John arrives in the detection zone of a reader, the RFID tag information including the number of the RFID tag is collected.

Step 2.   The reader transmits the obtained information to RFID middleware that performs filtering and collecting operations.

Step 3.   The RCOM interface integrating the UA generates a *SIP REGISTER* message and sends it to the SIP server. The *SIP REGISTER* message contains the *Contact field* in an *URI* form which is the current location of the RFID tag (*tag_RFID@IP_Reader*). The server registers this information at the location database.

Step 4.   If the registration is successful, the registrar generates a *200 OK* message to the UA. We assume, in this example, a registration without authentication. A SIP server configured only for authorized users generates a 407 SIP message type to request the credentials of the user before accepting the registration.
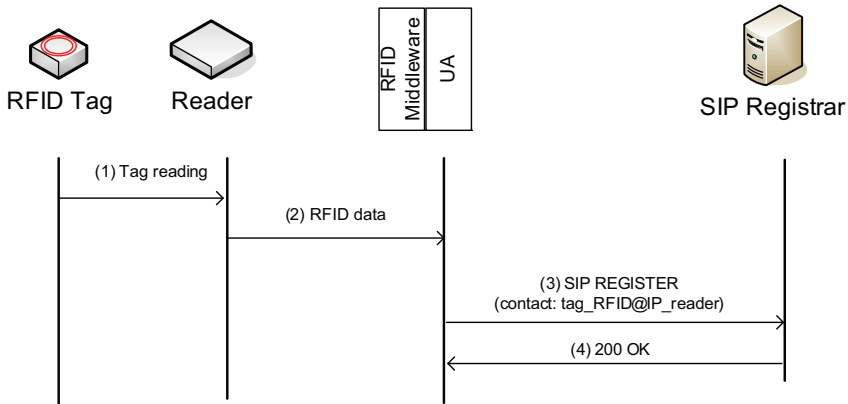
Fig. 3. Registration procedure

4.4 Tracking function - SIP redirection

To perform the tracking function, we assume that the UA is invoked by a location application which is out of scope of this specification.

The UA generates a *SIP INVITE* message sent to the SIP server. The message contains a *SIP URI* to indicate the tag or object to locate. The SIP server acts as a *redirect server* that responds to the *INVITE* request with a *"3xx"* message to indicate the current location.

Figure 4 illustrates an example of the tracking procedure. In this example, a nurse wants to know where specific medical equipment is in the hospital.

The location application generates a *SIP INVITE* message. The SIP looks for the location of the object by consulting the location database and the redirect function notifies via a "*302 Moved Temporarily*" message, the current location of the equipment, for example, *equipement_1@ office_C208*.
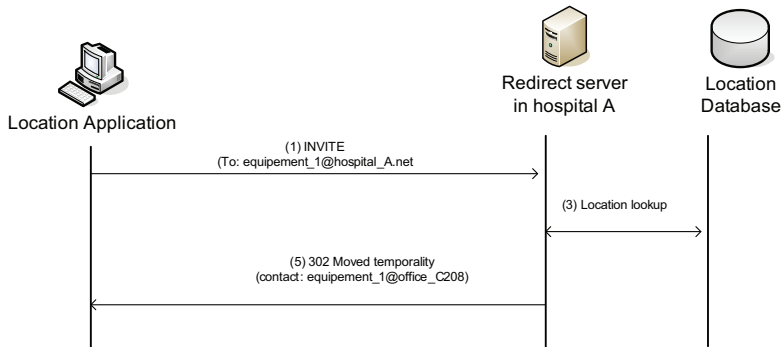
Fig. 4. Tracking procedure

4.5 System implementation

The location system is implemented under the Linux operating system and using the C programming language according to the open source GPL license. We implemented the system with some available tools of Linux environment such as *PhidgetRFID card libraries* and *SIP express router (SER).*

The PhidgetRFID card [phid] is an RFID reader which detects RFID tags that are brought in close of its proximity and returns the tag identification number. The PhidgetRFID reader uses the RFID EM4102 standard [em]. *The PhidgetRFID libraries* are APIs implemented in C under Linux that allow collecting the RFID tag and returning the unique number contained in the tag.

SIP Express Router (SER) [ser] is a high-performance, configurable, open-source GNU licensed server which can act as a SIP (RFC 3261 [sip]) registrar, proxy and redirect server. It provides many features of RFC 3261 functionality, a variety of database backends (mysql, oracle, etc.), management features (remote management via XML-RPC), NATi traversal, telephony features (LCR, speed dial), etc.

Figure 5 represents the system implementation that consists of the user agent (UA) with the location and tracking function, the SER server and the location database.

In our implementation, the backend location database uses My Structured Query Language (MySQL). We develop an UA based on the RFID source code of Phidget. We modified the SER source code so that to be able to receive/send the messages from UA.

The UA implementation have consisted in developing two events on the *PhidgetRFID card* for collecting the RFID tags and implementing a Location function to process the registration and tracking requests to the SIP server.
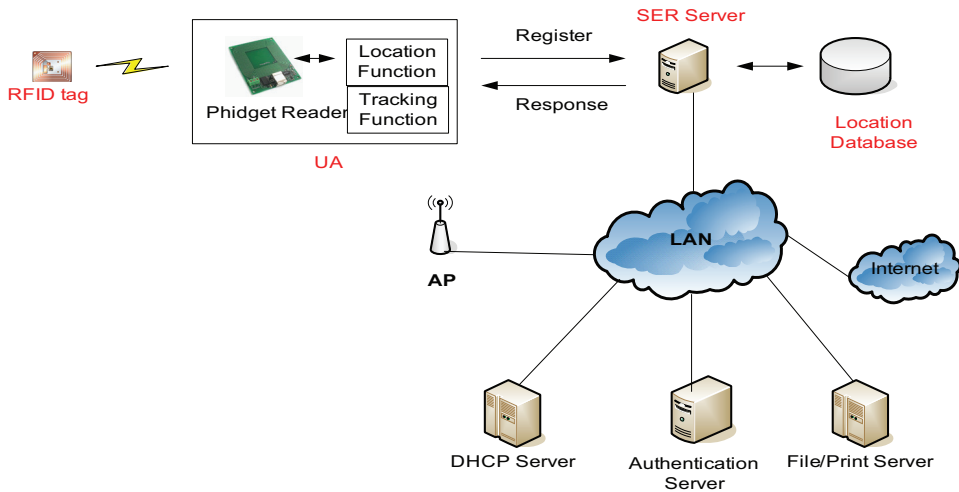
Fig. 5. The system implementation

In the following the main implemented functions are described:

*int Register-Object(CPhidgetRFIDHandle RFID, void *usrptr, unsigned char *TagVal) //* An event is issued by Phidget when a new tag is seen by the reader. The event is only fired one time for a new arrival of tag

*int Deregister-Object(CPhidgetRFIDHandle RFID, void *usrptr, unsigned char *TagVal) //* An event is issued by Phidget when a tag is out of the coverage zone of the reader.

char Create_Request_Line(char *domain) //* The request line specifies the type of request being issued by UA (e.g. SIP REGISTER or SIP INVITE), while the response line of SER server indicates the success or failure of a request (e.g. 200 OK, 302 Move temporality, …).

char Create_Contact(char *user_ip, char * user_port, char *user_name) //* The contact field contains the current location of object. It indicates the corresponding <RFID tag, IP address of the RFID reader>

char Create_Challenge_Register_Body (int seq, char *user_name, char *user_ip, char *user_port, char *domain, char *call_id, char *tag) //* This function generates the authentication message. The authentication uses the HTTP Digest method. The HTTP Digest authentication scheme is documented in [RFC3310] and extended in [RFC2617].

char Create_Auth_Register(char *nonce, int seq, char *user_name, char *user_ip, char *user_port, char *domain, char *call_id, char *tag, char *user_password); //* This function generates the authentication response message.

5. Conclusion

In this chapter, we proposed an IP-based RFID architecture that allows low cost and large scale deployment, as well as easy integration with IP-based services.
Particularly, a location management support is provided. The RCOM interface is introduced to handle location registration messages and entering/leaving tags detection.

A SIP-based architecture and the system implementation have been proposed for validation purpose.

This work is a part of an overall project which aims at developing a global communication network including RFIDs and IP entities inthe effort to contribute the realization of the future Internet of things.

6. References

[aero] Aeroscout solutions – [online] http://www.aeroscout.com

[cho]   Cho, K. Pack, S. Kwon, T. Choi, Y. (2007), SRMS: SIP-based RFID Management System, *Proceedings of IEEE International Conference on Pervasive Services*, pp. 11-18, ISBN: 1-4244-1325-7, Istanbul (Turkey), 15-20 Jul. 2007.

[edoc]   Ekahau Whitepaper (2005) - Comparison of Wireless Indoor Positioning Technologies   -   [online]http://www.productivet.com/docs-2/Wireless_Comparison.pdf

[ekah] Ekahau Solutions - [online]http://www.ekahau.com

[em] EM4102 protocol - [online]http://www.ibtechnology.co.uk/PDF/EM4102_DS.pdf

[epc] EPCglobal Website, [online]http://www.epcglobalinc.org.

[high] J. Hightower, C. Vakili, C. Borriello and R. Want (2001), Design and calibration of the SpotON ad-hoc location sensing system, UW CSE 00-02-02, *University of Washington, Department of Computer Science and Engineering*, Seattle, WA, August 2001.

[itu]   ITU   Internet   Report   (2005)   -   The   Internet   of   Things,   -   [online] http://www.itu.int/dms_pub/itu-s/opb/pol/S-POL-IR.IT-2005-SUM-PDF-E.pdf

[ivan] Getting, Ivan A (1993), The Global Positioning System, *In: IEEE Spectrum*, pp. 36 – 37, December 1993.

[joy]   Joy, V. Vimal Laxman, P. (2007), Smart Spaces: Indoor Wireless Location Management System, *Proceedings of Next Generation Mobile Applications, Services and Technologies (NGMAST),* pp. 261-266, ISBN: 978-0-7695-2878-6, Cardiff, 12-14 Sept. 2007.

[jud]   Judith M. Myerson (2006), RFID in the Supply Chain: A Guide to Selection and Implementation, ISBN / ASIN: 0849330181, AUERBACH, 20 Nov. 2006

[klau]   Klaus F. (2003), RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification, 2nd Edition, ISBN / ASIN: 0470844027, Wiley, 23 May 2003

[liu] X. Liu, M.D. Corner, and P. Shenoy (2006), Ferret: RFID Localization for Pervasive Multimedia, *In P. Dourish, and A. Friday (Eds.), International Conference of Ubiquitous Computing (Ubicomp 2006).* LNCS 4206, pp. 422-440, 2006.

[nad] Boukhatem, N. Tran, P.N. (2008), IP-based RFID architecture and location management, *Proceedings of the 16th International Conference on Software, Telecommunications and Computer Networks (SoftCOM)*, pp. 95-99, ISBN: 978-953-6114-97 9, Split (Croatia), 25-27 Sept. 2008.

[ni] L. Ni , Y. Liu , Y. Cho Lau, A. Patil (2004), LANDMARC: Indoor Location Sensing Using Active RFID. *In Wireless Networks 10*, pp.701–710, Kluwer Academic Publishers. Netherlands, 2004.

[ohta] Y. Ohta, M. Sugano, and M. Murata (2005), Autonomous Localization Method in

Wireless Sensor Networks, *Proceedings of 3rd IEEE International Conference on Pervasive Computing and Communications Workshops 2005 (PerCom 2005),* Kauai Island, USA, 2005.

[phid] PhidgetRFID card - [online]
http://www.phidgets.com/products.php?category=14&product_id=1023

[RFC3310]   Hypertext Transfer Protocol (HTTP) Digest Authentication Using Authentication and Key Agreement (AKA) - [online] ftp://ftp.isi.edu/in-notes/rfc3310.txt

[RFC2617] HTTP Authentication: Basic and Digest Access Authentication - [online] ftp://ftp.isi.edu/in-notes/rfc2617.txt

[ser] SIP Express Router - [online] http://www.iptel.org/ser

[sip] SIP: Session Initiation Protocol – RFC3261- [online]
http://www.ietf.org/rfc/rfc3261.txt

[sue] K.L. Sue, C.H. Tsai, and M.H. Lin (2006), FLEXOR: A Flexible Localization Scheme Based on RFID, *In I. Chong, and K. Kawahara (Eds.), International Conference on Information Networking (ICOIN)*, LNCS 3961, pp. 306-316, 2006.

[teso] R. Tesoriero, R. Tebar, J.A. Gallud , M.D. Lozano, V.M.R. Penichet (2009), Improving location awareness in indoor spaces using RFID technology, *In Expert Systems with Applications Journal*, Vol. 37 (2010), pp. 894–898

[wein] Weinstein, R. (2005), RFID: a technical overview and its application to the enterprise, *In: IT Professional*, Volume: 7, Issue: 3, pp. 27- 33, ISSN: 1520-9202, May-June 2005.

[yang] Q. Yang, Y. Chen, J. Yn, and X. Chai (2004), LEAPS: A Location Estimation and Action Prediction System in a Wireless LAN Environment, In H. Jin et al. (Eds.), *IFIP International Conference on Network and Parallel Computing (NPC 2004)*, LNCS 3222, pp. 584-591, 2004.

[zang] Zang, L. Chao-Hsien, C. Wen, Y. (2008), SIP-RLTS: An RFID Location Tracking System Based on SIP, *Proceedings of IEEE International Conference on RFID*, pp. 173-182, Las Vegas (USA), 978-1-4244-1711-7, 16-17 Apr. l 2008.

[zhang] Zhang T., Xiong Z., Ouyang Y. (2006), A Framework of Networked RFID System Supporting Location Tracking, *Proceedings of the 2nd IEEE/IFIP International Conference in Central Asia on Internet*, ISBN: 1-4244-0543-2, pp. 1-4, Tashkent, Uzbekistan, 19 -21 September 2006.

[weiser] M. Weiser (1991), The computer of the 21st century, *Scientific American*, pages 94–100, September 1991.

Tracking Methodologies in RFID Network

M Ayoub Khan
Centre for Development of Advanced Computing, NOIDA
(Ministry of Communications and IT, Govt. of India)
India

1. Introduction

RFID is a wireless communication technology that uses radio waves. The RFID system consists of a reader, tags and antenna. The RFID reader is sometimes called Interrogator as well and RFID tag is called transponder (K. Finkenzeller, 2003). This transponder is attached to or embedded in a physical object to be automatically identified. The transponder, which doesn't usually possess its own power supply, is not within the interrogator zone of a reader it is totally passive. This transponder is activated when it is within the interrogator zone of the reader. In contrast to it, a transponder is called active, if it has own source of power.

In this chapter, passive transponder is assumed along with the fixed RFID interrogators. This tracking system consists of RFID Interrogators, RF transponders, ZigBee (Stanislav Safaric et al. 2006; J. A. Gutierrez et al. 2001) modules, Tracking application, and back-end database that stores tracking vectors collected by ZigBee enabled RFID Interrogators.

Virtual Route Tracking (VRT) algorithm is designed to keep track of object in ZigBee enabled RFID Mesh Network. The object can be any person or article in the network. A RFID transponder is attached to the object. The RFID interrogators are connected by the ZigBee wireless network (Stanislav Safaric et al. 2006; J. A. Gutierrez et al. 2001), herein consist of densely deployed RFID interrogators. The proposed algorithm have feature of tracking as well as tracing the object. Tracking knows where an object is and tracing knows where an object has been. The RFID back-end database helps in storing history (past information) and the present status of the transponder movement. There are many technologies for tracking and tracing. Using RFID is one of the most cost effective methods.

In today's world tracking objects with RFID is important everywhere (Lionel M Ni et al, 2003; RFID Journal, 2008) i.e. supply chain, asset and people. Optimizing data exchange between partners in the supply chain is traditionally done through organizations like EAN, today known, as GS1. The influence of GS1 and Electronic Product Code (EPC) is highly important in the development and acceptance of RFID technology throughout the world. Allowing a person to discover the location of things and their co-works has long been identified as an interesting topic in ubiquitous computing (J. Hightower, 2001; A. Ward, et al, 1997; R. Want et al, 1992). Therefore, we are proposing the use of EPC (RFID Journal, 2008) for identifying the transponder in the RFID mesh network.

An Electronic Product Code (EPC) is a unique object identifier. An EPC consists of version number, manufacturer, product and serial number (K. Finkenzeller, 2003). The version

number specifies the EPC format i.e. 64-bit EPC, 96-bit EPC and 256-bit EPC. The manufacturer field is a unique number assigned to a particular manufacturer. The product number is a unique number allocated to a specific product class produced by a manufacturer. The serial number is a unique number assigned by the manufacturer to every individual product. The manufacturer within a product class should not duplicate the serial. Therefore, triplet of manufacturer number, product number, and serial number uniquely identifies an object. This EPC will be used for the purpose of tracking object in the mesh network.

The chapter is organized as follows: fundaments of object tracking are discussed in section 2. Section 3 presents the technique to formulate a RFID network using ZigBee protocol as backbone. Section 4 explores the scope of suitable database based on the characteristics of RFID data. Section 5 has a focus on the architecture of tracking applications. The algorithm for tracking an object in RFID network is presented in section 6. Finally, a conclusion is presented in the last section.

2. Fundamental of object tracking

The locating and identification of a tag can be classified as: Discrete and Continuous (Christian Hillbrand et al., 2007). Discrete mode identifies tag on predefined locations and intervals, while Continuous mode works seamlessly to locate the object continuously. These two modes are very effective in designing the system for location estimation. Here, we define location estimation technique as the process of estimation of physical coordinates of an object in RFID field. The coordinates may correspond to some location in the plane. The location information is useful for warehouses to locate product, in hospitals for locating equipments, in library for locating books etc to name a few. Whatever is the use of location information, underlying techniques to locate may differ from each other. Different applications and areas require different types of information pertaining to location. The types of information can be physical location, symbolic location, absolute location and relative location (Hightower and G. Borriello, 2001).

Physical location: This is expressed in the terms of co-ordinates, used to identify a location with 2-D/3-D map.

Symbolic location: This is expressed in neutral-language like near reception; lobby, in the drawing room.

Absolute location: It is expressed by using shared reference   grid for all located objects.

Relative location: This is expressed by known nearness of the reference points.

The localization can be of broadly classified as Indoor and Outdoor. The Indoor location can be sensed by various wireless technologies, which can be classified on the basis of: (1) positioning algorithm (2) employed infrastructure. In general RFID positioning systems consists of tag, receiver and central computer (Shomit S et al, 2004). There are four different system topologies for positioning systems (C. Drane et al, 1998). First, remote positioning system, where measuring unit receives the transmitter signal and transmitter (signal) is mobile. The second, self-Positioning system where the mobile measuring unit receives the signal from other transmitters kept at known locations, and contributes in its location finding based on measured signals. Third, indirect remote positioning system where the measurement results from self positioning system is send to remote site using wireless link

for location computation. Fourth is indirect self-positioning, where mobile unit receives the measurement result from remote positioning side.

In the outdoor environments, the Global Positioning System (GPS) is the most widely used technology to acquire the position of an object. For wearable system it becomes difficult for the GPS to achieve stepped level of precision due to constraint on size and weight of the hardware. The other disadvantage of GPS includes its exclusive use in outdoor applications, as it requires satellites to be "visible". In proximity of narrow valleys, raised buildings, forests, the signals of the GPS system has shadowing effects. Positioning technologies provided by GSM are: Network-based, Device-based and Hybrid systems (Christian Hillbrand et al., 2007). The Network-based method uses service provider network (cellular phone) to determine the position of a mobile device. For capturing positions of the mobile terminal device, service provider identifies its relative position in relation to a serving GSM Base Transceiver Station (BTS) (Christian Hillbrand et al., 2007). Device-based system for positioning purposes captures the data on the mobile terminal device (Christian Hillbrand et al., 2007). Either or both interacting GSM and non-GSM components are used by Hybrid GSM systems for positioning of mobile device. Assisted GPS (A-GPS) is an example of hybrid GSM systems. A mobile terminal device now comes with GPS equipped receivers. The positioning accuracy reported ranges between 3m and 30m (Christian Hillbrand et al., 2007). Here, in this chapter we are introducing a concept of discrete time locating technique known as virtual route tracking. Let's understand with the help of figure 1. This consists of RFID readers ($R_1...R_{20}$). Each row in the plane has five readers. When a tagged object starts moving from R_1 to R_{16} then R_7, R_8, R_4, R_{10}, R_{15}, R_{19}, R_{18}, R_{12}, R_{16} intermediate readers interrogates the tag.
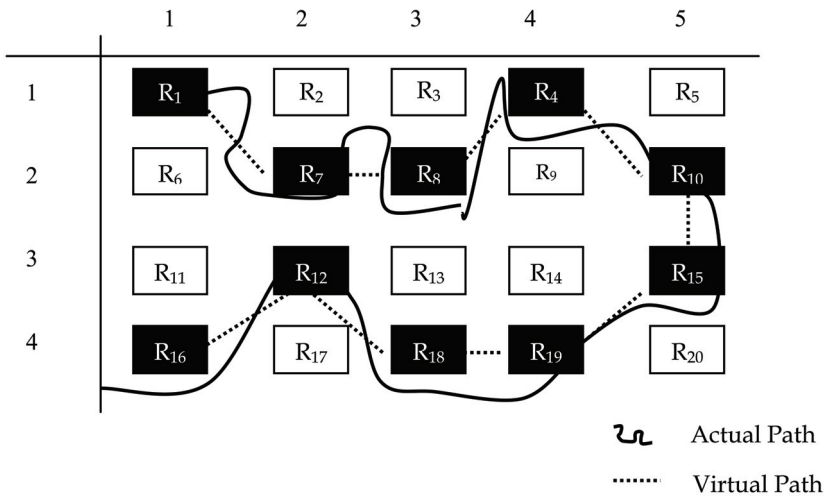
Fig. 1. RFID reader network

When the tag moves from reader R1 to R7, the straight line between them is regarded as the track (virtual) of the transponder. The thick curve in the RFID Network denotes the real path of a person or object. So, the track of the figure 1 is as follows:

$Track=Virtual\ Track=(1,1) \rightarrow (2,2) \rightarrow (2,3) \rightarrow (1,4) \rightarrow (2,5) \rightarrow (3,5) \rightarrow (4,4) \rightarrow (4,3) \rightarrow (3,2) \rightarrow (4,1)$

This grid base placement of the reader is an ideal situation but in real environment they may be placed in mesh fashion. In the following section, we would discuss the background of formulating such mesh-based placement.

3. Formulation of RFID network

We have chosen ZigBee communication technology to formulate mesh network of RFID readers because ZigBee operates in the industrial scientific and medical (ISM) band. The ZigBee offers three frequency bands, with 27 channels specified as following (McInnis, M. 2003; J. A. Gutierrez, 2001):

Frequency Band	Channels	Data Rate
868 and 868.6 MHz	Channel 0, 10	20 Kbps
902.0 and 928.0 MHz	Channel 1-10	40 Kbps
2.4 and 2.4835 GHz	Channel 11-26	250 Kbps

Table 1. ZigBee features

The ZigBee has capability to self-organize and self-healing dynamic mesh network based on the standards. The ZigBee standards define two types of devices, a full-function device (FFD), and reduced function device (RFD) (McInnis, M. 2003; J. A. Gutierrez, 2001). These two types of devices have different mode of operation. The FFD can operate in three different modes depending on the requirement *viz*. personal area network (PAN) coordinator, a coordinator ore a device (McInnis, M. 2003). However, RFD is intended for application that minimal resource and very low data transfer rate. A system conforming to IEEE 802.15.4 consists of several core components.
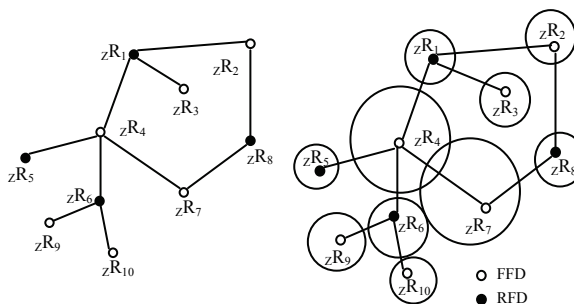
Fig. 2. Mesh network of RFID readers

This network (Fig. 2 a) consists of five full function device and five reduced function device. This FFD and RFD are attached with a standalone interrogator, which transmits the information to the host computer (central) when it reads the tag. In, figure 2 b, we have shown the intersecting zone by the circles. We are proposing a vector that will contain information about the transponder, which he has interrogated. The vector contains following attributes:

$$<E_i, t_j, {}_zI_k> = < \text{EPC code } i, \text{ TimeStamp } j, \text{ InterrogatorID } k>$$

Here, EPC identifies the transponder uniquely across the globe. This EPC is stored in the memory of the transponder (RFID Journal, 2008). The TimeStamp is the time when interrogator has red the tag. The zInterrogatorID will uniquely identify the ZigBee enabled RFID Interrogator on the network. To deduce the relationship between the interrogators, an interrogator neighbour matrix (INM) is formed.

$$\begin{bmatrix} 0 & 0 & 0 & 0 & -1 & -1 & -1 & -1 & -1 & -1 \\ 0 & 0 & 0 & -1 & -1 & -1 & -1 & 0 & -1 & -1 \\ 0 & 0 & 0 & 0 & -1 & -1 & 0 & 0 & -1 & -1 \\ 0 & -1 & 0 & 0 & 0 & 0 & 1 & 0 & -1 & -1 \\ -1 & -1 & -1 & 0 & 0 & 0 & -1 & -1 & 0 & -1 \\ -1 & -1 & -1 & 0 & 0 & 0 & 0 & -1 & 0 & 0 \\ -1 & -1 & 0 & 1 & -1 & 0 & 0 & 0 & -1 & 0 \\ -1 & 0 & 0 & 0 & -1 & -1 & 0 & 0 & -1 & 0 \\ -1 & -1 & -1 & -1 & 0 & 0 & -1 & -1 & 0 & 0 \\ -1 & -1 & -1 & -1 & -1 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

Fig. 3. Interrogator neighbour matrix

The network is formed in a mesh fashion; therefore determination of the adjacent or neighbour becomes subjective matter. The interrogators are not placed in a matrix form, so there can be number of neighbour/adjacent in omni direction. Hence, we proposed an interrogator adjacency matrix, which will contain the information about the relationship viz. neighbour: 0, intersecting: 1, non-neighbour: -1. Two interrogators i and j are called neighbours, if transponder moves toward interrogator j and j is the only interrogator to interrogate it. Two interrogators i and j are called intersecting interrogator, if the tag will be interrogated by two or more interrogators. This situation occurs in a mesh network where there is intersecting interrogation zone. Two interrogators i and j are intersection to each other, if transponder enters into a zone where two interrogators i and j interrogate it. The interrogator neighbor matrix is defined as below:

INM (i, j) = 0 if i, j are neighbor interrogators
= 1 if i, j are intersecting interrogators
= -1 if i, j are non- neighbor interrogators

Two Interrogators i and j or intersection to each other, if transponder enter into a zone where two interrogators i and j interrogate it. This can be done manually, by measuring RF filed strength and pattern of i and j.

In this work, we have considered the reader collision protocol, so network can't generate two or more tracking vectors with same timestamp for any transponder Ei. Presently, we haven't exploits the ZigBee neighbor table for the purpose of identify and updating INM. Here, we are using ZigBee as a wireless media to transfer the data to host computer.

4. Database for tracking objects

The database is an important aspect of tracking system to ensure the persistence of data. We have stored reader, Interrogator neighbour matrix and tracking information into different

table. These tables are created in Oracle 8i relational database management system. These tables are as follows:

Reader _ID	Location_ID
111.123.123.134	0001: Security check

Table 2. Reader

Reader table contains information reader identification and location identification. The reader identification coding is akin to the IP address while the location ID is four digit integer numbers to identify a particular location within the premises. The Interrogator neighbour matrix table identifies the relationship among the readers. In the following, the relationships of reader ID 111.123.123.134 with other readers are shown. Here, '"0" represents neighbour, "1" represents intersecting relationship and "-1" represents no relationship among readers.

Reader_m	Reader_n	Relationship
111.123.123.134	111.123.123.130	0
111.123.123.134	111.123.123.130	1
111.123.123.134	111.123.123.136	1
111.123.123.134	111.123.123.140	1
111.123.123.134	111.123.123.149	-1
111.123.123.134	111.123.123.132	-1
111.123.123.134	111.123.123.104	-1

Table 3. INM

The tagged object is interrogator by the readers as soon enters into the vicinity of some other reader. This movement changes the state of the object as it modifies information like location of the object, interrogation time, and duration of stay in particular vicinity. The tracking table has been designed to store the sufficient information about the moving tagged object. The EPC field in the table contains the identification of the tag in EPC format. The duration contains the difference between the last read timestamp and the first read timestamp.

EPC	TimeStamp	Reader_ID	Duration
E_1(96 bit format)	t_1	$_zR_4$	t_4-t_1

Table 4. Tracking

5. Application architecture

The proposed architecture of the tracking system consists of four layers as shown in Fig. 4. The layer 0 is a hardware layer, which consists of RFID interrogators, antenna, and ZigBee modules. This layer reads the raw data from the RFID transponder. This event data is transferred from the antennas/readers to the middleware layer (layer 1) via ZigBee transceiver module. The layer 1 performs the data filtering and aggregation. The data that is relevant for the higher layers (back-end layer) is transferred to the middleware. Middleware

is typically installed in the data center (Christian Floerkemeier et al, 2007). The layer 2 is the repository for the filtered data. This repository will be used for deducing the virtual track as well as trace. This layer transfers the data to the layer 3 (application layer) upon triggering a query from the tracking application. The application layer consists of GUI based application where users can track/trace the route of the particular transponder by specifying the EPC. The application layer will trigger a query to the back-end layer. The back-end layer, in turn will select the data from the tracking database and transfer back to the application layer. Based on the data received from back-end layer, tracking application will graphically draw the route of the transponder.

Layer 3	Tracking Application
Layer 2	Oracle Database
Layer 1	RFID Middleware Server
Layer 0	ZigBee enabled RFID Infrastructure
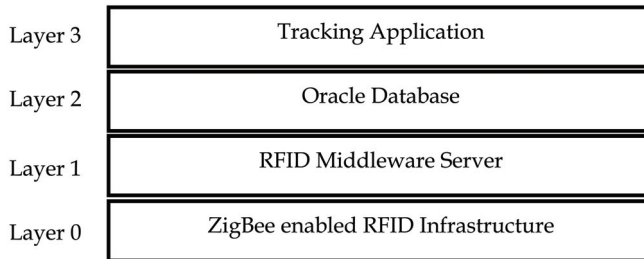
Fig. 4. Application architecture

6. Tracking algorithms

Suppose transponder E_1 enters into the zone of interrogator $_ZR_5$ at time t_1 then moves into the zone of $_ZR_4$ at time t_2. In this case, the interrogator $_ZR_5$ and $_ZR_4$ will send following tracking dataset.

$$_ZR_5 \rightarrow \{E_1, t_1, {}_ZR_5\}$$
$$_ZR_4 \rightarrow \{E_2, t_2, {}_ZR_4\} \qquad t_1 < t_2$$

Now, virtual route tracking algorithm will analyze the relationship between $_ZR_5$ and $_ZR_4$ with the help of interrogator neighbor matrix.

If INM (5,4)==0 then
        relationship=0 // neighbor
else if INM(5,4)==1 then
        relationship=1 //intersecting
else
        relationship=-1 // non-neighbor
Second, the algorithm will analyze about the values of E_1 and E_2.
If the values of E_1 and E_2 are equal, two tracking dataset are derived from the same source then the track would be deduces as follows:

$$\text{virtual track} = {}_ZR_5 \rightarrow {}_ZR_4, \text{where } t_1 < t_2$$
$$\text{virtual track} = {}_ZR_4 \rightarrow {}_ZR_5, \text{where } t_1 > t_2$$

To deduce the path correctly, VRT algorithm will always keep on grouping the tracking dataset according to the values of E_i i.e. $E_1=E_2$; tracking dataset belong to same transponder, so put it into one group.
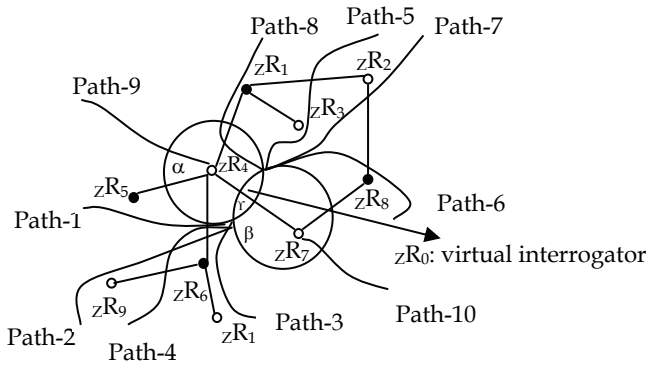
Fig. 5. RFID mesh network with possible path

Suppose, transponder enters into the intersecting zone, as in path (1, 2 or 3) in Fig. 5. In this case, all the two interrogators will interrogate it at different time slot. Therefore, two tracking dataset will be independently generated containing different timestamps. However, only one interrogator and its corresponding tracking dataset shall remain in the database. The deduction of this knowledge will be based on the position of the previous and the next interrogator of these two interrogators along the track. So, the algorithm will first find out the last interrogator who has interrogated transponder E_i as follows.

1. Find the $_zR_p$, previous interrogator for the transponder E_i.
2. The relations of the previous interrogator can be as follows:
   a. $_zR_p$ is neighbor of $_zR_4$ but $_zR_p$ is not neighbor of the $_zR_7$ (Path-1)
   b. $_zR_p$ is not neighbor of $_zR_4$, but $_zR_p$ is neighbor of $_zR_7$ (Path-3)
   c. $_zR_p$ is neighbor of $_zR_4$, but also neighbor of $_zR_7$. (Path-2)
   d. $_zR_p$ is not neighbor of both $_zR_4$ and $_zR_7$. (Path-4)

Case 1:
$_zR_p$ is neighbor of $_zR_4$ but $_zR_p$ is not neighbor of the $_zR_7$ (along path-1 in Fig 3), the algorithm will choose $_zR_4$, whereas deleting the tracking dataset $R_7 \rightarrow \{E_1, t_2, {}_zR_7\}$.

Case 2:
In a similar way, tracking dataset $R_4 \rightarrow \{E_1, t_1, {}_zR_4\}$ will be deleted when transponder follow path-3 and interrogated by $_zR_4$. However, we need to apply more intelligence when the previous interrogator is neighbor of both $_zR_4$ and $_zR_7$.

Case 3:
In the third case, being neighbor of both the interrogators one has to observe the next interrogator who will read it. So, algorithm will now find out the next interrogator who has interrogated transponder E_i as follows.

1. Find the $_zR_n$, next interrogator for the transponder E_i.
2. The relations of the next interrogator can be as follows:
   a. $_zR_n$ is neighbor of $_zR_4$ but $_zR_p$ is not neighbor of the $_zR_7$ (Path-4)
   b. $_zR_n$ is not neighbor of $_zR_4$, but $_zR_p$ is neighbor of $_zR_7$ (Path-6)
   c. $_zR_n$ is neighbor of $_zR_4$, but also neighbor of $_zR_7$. (Path-5)
   d. $_zR_p$ is not neighbor of both $_zR_4$ and $_zR_7$. (Path-7)

Now, consider transponder E_1 that moves along with path 4 in Fig. 5, so the collected tracking dataset are as follows.

$\{E_1, t_1, {}_ZR_6\}$
$\{E_1, t_2, {}_ZR_4\}$
$\{E_1, t_3, {}_ZR_7\}$
$\{E_1, t_4, {}_ZR_1\}$

As Fig. 5 illustrated, tracking dataset generated by interrogator ${}_ZR_7$ will be deleted and the resulting dataset will be as:

$\{E_1, t_1, {}_ZR_6\}$
$\{E_1, t_2, {}_ZR_4\}$
$\{E_1, t_4, {}_ZR_1\}$

Virtual Route for transponder E_1 is: ${}_ZR_6 \rightarrow {}_ZR_4 \rightarrow {}_ZR_1$ Now, consider transponder E_1 moves along with path 6 in Fig. 5, so the collected tracking dataset are as follows.

$\{E_1, t_1, {}_ZR_6\}$
$\{E_1, t_2, {}_ZR_4\}$
$\{E_1, t_3, {}_ZR_7\}$
$\{E_1, t_4, {}_ZR_8\}$

As Fig. 5 illustrated, tracking dataset generated by interrogator ${}_ZR_4$ will be deleted and the resulting dataset will be as:

$\{E_1, t_1, {}_ZR_6\}$
$\{E_1, t_2, {}_ZR_7\}$
$\{E_1, t_4, {}_ZR_8\}$

Virtual Route for transponder E_1 is: ${}_ZR_6 \rightarrow {}_ZR_7 \rightarrow {}_ZR_8$ Now, consider transponder E_1 moves along with path 5 in Fig. 5, so the collected tracking dataset are as follows.

$\{E_1, t_1, {}_ZR_6\}$
$\{E_1, t_2, {}_ZR_4\}$
$\{E_1, t_3, {}_ZR_7\}$
$\{E_1, t_4, {}_ZR_3\}$

As Fig. 5 illustrated, tracking dataset generated by interrogator ${}_ZR_7$ will be deleted and the resulting dataset will be as:

$\{E_1, t_1, {}_ZR_6\}$
$\{E_1, t_2, {}_ZR_0\}$
$\{E_1, t_4, {}_ZR_3\}$

In, this case a virtual interrogator has been created at the mid point area Υ to correct the track. Virtual Route for transponder E_1 is: ${}_ZR_6 \rightarrow {}_ZR_0 \rightarrow {}_ZR_3$

Case 4:

Now, we will investigate another case, in which transponder is moving around the vicinity of the particular interrogator. Suppose transponder E_1 is roaming around ${}_ZR_4$, so at different interval of time it will generate the following tracking dataset.

$$
\begin{cases} \{E_1, t_1, {}_ZR_4\} \\ \{E_1, t_2, {}_ZR_4\} \\ \{E_1, t_3, {}_ZR_4\} \\ \{E_1, t_4, {}_ZR_4\} \end{cases} \longrightarrow \begin{cases} \{E_1, t_1, {}_ZR_4\} \\ \{E_1, t_2, {}_ZR_4\} \\ \{E_1, t_4, {}_ZR_4\} \end{cases} \quad t_1 < t_2 < t_3 < t_4
$$

Assuming, the difference between two successive interrogation timestamp is negligible, therefore, tracking database will store first tracking dataset along with the duration $(t_4 - t_1)$ of stay in the vicinity of the interrogator as shown in Table 4.

6.1 Proposed tracking algorithm

In the analysis of various scenarios in section 3, now we will present the algorithm for tracking virtual route. The part of the algorithm will be executed in the middleware layer and the rest will be in the application layer.

Step 1. Check Mesh topology

> If changes took place then
>> update(INM)
> else
>> go to step 2

Step 2. Filter and Aggregate

Upon receiving tracking dataset, classify the dataset weather it belongs to one transponder or not. This will make a group of the transponders, whose contents of E_i are same. Using a Structured Query Language (SQL) and the special constructs provided in the Middleware can do filter and aggregate.

$$\begin{Bmatrix} \{E_1, t_1, zR_4\} \\ \{E_1, t_2, zR_1\} \\ \{E_2, t_1, zR_2\} \\ \{E_1, t_4, zR_5\} \\ \{E_2, t_4, zR_6\} \\ \{E_3, t_7, zR_7\} \\ \{E_3, t_3, zR_7\} \end{Bmatrix} = \begin{Bmatrix} G1: \\ \{E_1, t_1, zR_4\} \\ \{E_1, t_2, zR_1\} \\ \{E_1, t_4, zR_5\} \end{Bmatrix} \begin{Bmatrix} G2: \\ \{E_3, t_7, zR_7\} \\ \{E_3, t_3, zR_7\} \end{Bmatrix}$$

$$\begin{Bmatrix} G3: \\ \{E_2, t_1, zR_2\} \\ \{E_2, t_4, zR_6\} \end{Bmatrix}$$

Step 3. Eliminate redundant interrogation If a transponder is roaming around a particular interrogator then the successive timestamp t_i and t_j will be negligible. Therefore, find out the difference between the first interrogated timestamp and last interrogated timestamp from the interrogation tracking dataset series.

Step 4. Check relationship

By using interrogator neighbor matrix, deduce the track using the previous and next interrogator reader relationship as discussed in the section 3.

Step 5. display the virtual track on the screen from list of track

6.2 Simulation of the algorithm
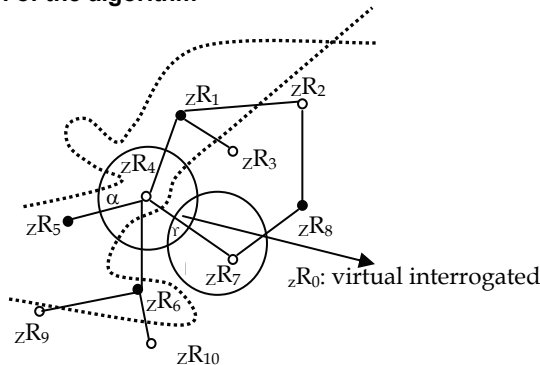
Fig. 6. Transponder movement in RFID network

We have simulated the proposed algorithm of tracking virtual route by developing tracking application in the Microsoft .Net framework. The tracking dataset and other database have been created using the Oracle 8i. The virtual tracking algorithm is implemented in the application layer, but in future work we will implement filter and aggregate functions in middleware layer. In the present version, we have manually entered all the values in the interrogator neighbor matrix. Initially, we provided data for the two transponders, which begin to move at the same time.

The data generated from these two transponders are as follows:

$$\left\{\begin{array}{l}\{E_1, t_1, {}_zR_9\}, \{E_2, t_1, {}_zR_5\} \\ \{E_1, t_2, {}_zR_1\}, \{E_2, t_2, {}_zR_4\} \\ \{E_1, t_3, {}_zR_6\}, \{E_2, t_3, {}_zR_4\} \\ \{E_1, t_4, {}_zR_4\}, \{E_1, t_5, {}_zR_7\} \\ \{E_2, t_5, {}_zR_1\}, \{E_1, t_6, {}_zR_3\} \\ \{E_1, t_7, {}_zR_2\}, \{E_2, t_6, {}_zR_2\}\end{array}\right\}$$

Step 1: No change in the topology
Step 2: Filter and Aggregate
Step 3: Eliminate redundant interrogation

$$\left\{\begin{array}{l}\{E_1, t_1, {}_zR_9\} \\ \{E_1, t_2, {}_zR_1\} \\ \{E_1, t_3, {}_zR_6\} \\ \{E_1, t_4, {}_zR_4\} \\ \{E_1, t_5, {}_zR_7\} \\ \{E_1, t_6, {}_zR_3\} \\ \{E_1, t_7, {}_zR_2\}\end{array}\right\} + \left\{\begin{array}{l}\{E_2, t_1, {}_zR_5\} \\ \{E_2, t_2, {}_zR_4\} \\ \{E_2, t_5, {}_zR_1\} \\ \{E_2, t_6, {}_zR_2\}\end{array}\right\}$$

$$\left\{\begin{array}{l}\{E_1, t_1, {}_zR_9\} \\ \{E_1, t_2, {}_zR_1\} \\ \{E_1, t_3, {}_zR_6\} \\ \{E_1, t_4, {}_zR_4\} \\ \{E_1, t_5, {}_zR_7\} \\ \{E_1, t_6, {}_zR_3\} \\ \{E_1, t_7, {}_zR_2\}\end{array}\right\} + \left\{\begin{array}{l}\{E_2, t_1, {}_zR_5\} \\ \{E_2, t_2, {}_zR_4\} \\ \{E_2, t_3, {}_zR_4\} \\ \{E_2, t_5, {}_zR_1\} \\ \{E_2, t_6, {}_zR_2\}\end{array}\right\}$$

Step 4: check relationship

$$\left\{\begin{array}{l}\{E_1, t_1, {}_zR_9\} \\ \{E_1, t_2, {}_zR_1\} \\ \{E_1, t_3, {}_zR_6\} \\ \{E_1, t_4, {}_zR_0\} \\ \{E_1, t_6, {}_zR_3\} \\ \{E_1, t_7, {}_zR_2\}\end{array}\right\} + \left\{\begin{array}{l}\{E_2, t_1, {}_zR_5\} \\ \{E_2, t_2, {}_zR_4\} \\ \{E_2, t_5, {}_zR_1\} \\ \{E_2, t_6, {}_zR_2\}\end{array}\right\}$$

The final tracking result of this algorithm for transponders is as follows:

$$E_1 \text{ is } {}_zR_9 \rightarrow {}_zR_1 \rightarrow {}_zR_6 \rightarrow {}_zR_0 \rightarrow {}_zR_3 \rightarrow {}_zR_2 \text{ and } E_2 \text{ is } {}_zR_5 \rightarrow {}_zR_4 \rightarrow {}_zR_1 \rightarrow {}_zR_2$$

Step 5: Display the virtual track

7. Conclusion

In this research work, we have made an attempt to track the virtual route of an object, which is moving in a ZigBee enabled RFID interrogator mesh network. We presented different type of relationship among the interrogators. An algorithm is proposed and implemented to track the path of an object. As shown in the simulation results, the proposed VRT algorithm quite accurately tracks the objects specified in the simulation. This VRT can be used to track any object or person. But, when talking about the person, privacy is always a serious issue that needs to address carefully (Alastair R. Beresford et al, 2003). Privacy had been the scapegoat of the failure in the indoor-location based sensing, but privacy might become irrelevant in the newer business models (Jonathan spinney, 2004).

8. References

Auto-ID Technical report(2002) 860MHz–930MHz EPC Class I, Generation 2 RFID Tag & Logical Communication Interface Specification, Auto-ID Centre, *MIT*, USA

A. Ward, A. Jones and A. Hopper(1997), A New location technique for the active office, *IEEE Personal Communications*

Alastair R. Beresford and Frank Stajano(2003), Location privacy in pervasive computing, *IEEE Pervasive Computing*, 3(1):46.55

Christian Hillbrand, Robert, Schoech,(2007), Shipment Localization Kit: An Automated Approach for Tracking and Tracing General Cargo, *IEEE: ICMB*

C. Drane,M. Macnaughtan, and C. Scott(1998), Positioning GSM telephones, *IEEE Communication. Mag.*, vol. 36, no. 4, pp. 46–54

Christian Floerkemeier et al(2007), RFID Application Development with the Accada Middleware Platform, *IEEE SJ* ,Vol. X No. X

EPC Global, http://www.epcglobalinc.org

Hightower and G. Borriello(2001), Location systems for ubiquitous computing, *IEEE Computer*, vol. 34, no. 8

J. Hightower and G. Borriello(2001) , Location System for Ubiquitous Computing", *IEEE Computer Magazine*, pp.57-66.

J. A. Gutierrez, M. Naeve, E. Callaway (2001) , IEEE 802.115.4; A Developing Standard for Low Power, Low Cost Wireless PAN, I*EEE Network*, vol. 15, no. 5, pp 12-19.

Jonathan spinney(2004), Location-Based Services and the proverbial Privacy Issue, *In ESRI*

K. Finkenzeller(2003), RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification, *John Wiley & Sons; 2 edition*

Lionel M Ni et. al(2003) , Landmarc: Indoor location sensing using active RFID, *PERCOM*

McInnis, M. (2003), 802.15.4–IEEE Standard for Information Technology", *IEEE*, New York

R. Want, A Hopper, V Falcao and J. Gibbons(1992), The Active Badge Location System, *ACM Transaction on Information System*, pp. 91-102

RFID Journa(2008)l, http://www.rfidjournal.com

RFID Handbook(2008), http://www.rfid-handbook.com

Stanislav Safaric, Kresimir Malaric(2006), ZigBee wireless standard, *48th International Symposium ELMAR-2006*, Zadar, Croatia

Shomit S. Manapure Houshang Darabi Vishal Patel Prashant Banerjee(2004), A Comparative Study of RF-Based Indoor Location Sensing Systems , *IEEE: ICNSC*, Taipei

The Modeling and Analysis of the Strong Authentication Protocol for Secure RFID System

Hyun-Seok Kim and Jin-Young Choi
Korea University
Republic of Korea

1. Introduction

In the RFID security domain, various issues are related to data protection of tags, message interception over the air channel, and eavesdropping within the interrogation zone of the RFID reader (Sarma. et al., 2003; EPCglobal). This topic has been so far been dominated by the topics of data protection associated with data privacy and authentication between tag and reader. In this paper, when using RFID, two aspects on the risks imposed on the passive party are discussed.

Firstly, the data privacy problem is such that storing person-specific data in a RFID system can threaten the privacy of the passive party. This party may be, for example, a customer or an employee of the operator. The passive party uses tags or items that have been identified as tags, but the party has no control over the data stored on the tags.

Secondly, authentication is carried out when the identity of a person or program is verified. Then, on this basis, authorization takes place, i.e. rights, such as the right of access to data. In the case of RFID systems, it is particularly important for tags to be authenticated by the reader and vice-versa. In addition, readers must also authenticate themselves to the backend, but in this case, there are no RFID-specific security problems.

To satisfy the above requirements, security protocols play an essential role. As with any protocol, the security protocol comprises a prescribed sequence of interactions between entities, and is designed to achieve a certain end. A diplomatic protocol typically involves a memorandum of understanding exchange, intended to establish agreement between parties with potentially conflicting interests. Security protocols are, in fact, excellent candidates for rigorous analysis techniques: they are critical components of distributed security architecture, very easy to express, however, extremely difficult to evaluate by hand. They are deceptively simple: literature is full of protocols that appear to be secure but have subsequently been found to fall prey to a subtle attack, sometimes years later. Cryptographic primitives are used as building blocks to achieve security goals such as confidentiality and integrity authentication.

Formal methods play a very critical role in examining whether a security protocol is ambiguous, incorrect, inconsistent or incomplete. Hence, the importance of applying formal methods, particularly for safety critical systems, cannot be overemphasized. There are two main approaches in formal methods, logic based methodology (Burrows et al., 1989; Hoare, 1985), and tool based methodology (Lowe, 1997; FDR, 1999). In this paper, the hash (Sarma.

et al., 2003) based RFID authentication protocols which employs hash functions to secure RFID communication are specified and verified whether this protocol satisfies security properties such as secrecy and authentication using GNY(Gong L., Needham R., and Yahalom R.; Gong et al., 1990) logic as the Modal logic (Burrows et al., 1989) methodology. After verifying the protocols as GNY logic, the existence of known security flaws in the protocols is confirmed, and the problems of the hash based technique are described. The contribution of this paper is designing and verifying the secure authentication protocol, which is widely researched in RFID systems using formal methods. This paper is organized as follows. In brief, Section 2 describes related work on RFID security and authentication schemes associated with hash functions. In Section 3, the use of modal logic (GNY) is outlined for analyzing security protocols. Section 4 describes the analyzed result of the protocol. Section 5 presents the proposed security scheme. Section 6 addresses conclusions and future work.

2. Related work

There has been much literature attempting to address the security concerns raised by the use of RFID tags.

2.1 The hash lock scheme

A reader defines a "Lock" value by computing lock = hash (key)(Weis et al., 2003), where the key is a random value. This lock value is sent to a tag and the tag stores this value in its reserved memory (i.e. a metaID value), the tag then enters into a locked state automatically. To unlock the tag, the reader transmits the original key value to the tag, and the tag performs a hash function on that key to obtain the metaID value. The tag then has to compare the metaID with its current metaID value. If both values match, the tag is unlocked. Once the tag is in an unlocked state, it can transmit its identification number, such as the Electronic Product Code (EPC) to readers' queries in the forthcoming cycles. This approach is simple and straightforward in achieving data protection, i.e. the EPC code stored in the tag is being protected. An authorized reader is able to unlock and read the tag, then lock the tag again after reading the code. This scheme is analyzed in Section 4 in detail.

2.2 The randomized hash lock scheme

This is an extension of hash lock (Weis et al., 2003) based on pseudo random functions (PRFs). An additional pseudo-random number generator is required to be embedded into tags for this approach. Presently, tags respond to reader queries using a pair of values (r, hash(IDk || r)), where r is the random number generated by a tag, IDk is the ID of the k-th tag among a number of tags in ID1, ID2, . . ., IDk, . . ., IDn. For reader queries, the tag returns two values. The first is the random number. The second is a computed hash value based on concatenation(||) of its IDk and r. When the reader obtains these two values, it retrieves the current N number of ID (i.e. ID1, ID2, . . ., IDn) from the backend database. The reader will perform the above hash function on each ID from 1 to n, with r, until it finds a match. When the reader finds a match, the reader is able to identify the tag k is on its tag's ID list (i.e. tag authentication). The reader will then transmit the IDk value to the tag for unlocking. Once the tag is in an unlocked state, the reader can obtain its EPC code in the subsequent reading cycle.

In addition to achieving RFID tag security, this scheme also provides location privacy. In the hash lock scheme, tags still disclose metaID values. However, this approach only discloses *r* and the hashed value.

2.3 The chained hash scheme

Ohkubo et al.(Okubo et al.; Okubo et al., 2004) suggested the chained hash procedure as a cryptographically robust alternative. In every activation, the tag calculates a new meta ID, using two different hash functions. First, the current meta ID is hashed in order to generate a new meta ID, which is then hashed again with the aid of the second function. It is this second meta ID that is transmitted to the reader. For the purpose of decoding, the reader must hash until a match with the meta ID transmitted from the tag has been found. The advantage of this procedure is that it is not sensitive to repeated attempts to eavesdrop the meta ID during transmission via air waves.

2.4 Other approaches

Another hash-based approach is *Hash based Varying Identifier* proposed by Henrici and Müller (Henri & Müller, 2004). Their scheme also adopts a hash function and a random number generator (RNG), but a pseudo random number is generated by a back-end server and transmitted to the tag every interrogation, to make the tag's queried identifier random and preserve location privacy.

Hwang et al. (Hwang et al., 2004) proposed an improved authentication protocol of *Hash based Varying Identifier.* In their scheme, the main difference is that a reader has a random number generator to protect against a man-in-the-middle attack.

3. Formal methods for security protocols

3.1 Modal logic: GNY(Gong L., Needham R., and Yahalom R.)

GNY(Gong et al., 1990) logic is used to reason about security protocols. GNY logic is a direct successor to BAN (Burrows et al., 1989) logic and is quite powerful in its ability to uncover even subtle protocol flaws. Discussion of the virtues and limitations of the logic can be found in (Mathuria et al., 1994).

In GNY logic, message extensions are added to the protocol description during protocol formalization, so that principals can communicate their beliefs and thus reason about each other's beliefs. The use of message extensions enables the logic to deal with different levels of trust among protocol principals. As such, it is considered an improvement over BAN logic, which assumes that all principals are honest and competent. This development is noteworthy as many protocol attacks are performed by dishonest principals. As an example of a message extension, consider the following: P → Q: {K; P}Ks- is formally stated as Q ◁ *{*K, P}Ks- ~> S |≡ P $\underset{\longleftrightarrow}{K}$ Q. This means that principal Q is informed of a session key, K, and an identity, P, encrypted under the private key of principal S. The session key, K, is marked with a not-originated-here asterisk. Q is informed that S believes K is a suitable shared secret for P and Q.

The postulates of GNY logic are used to deduce whether protocol goals can be derived from the initial assumptions and protocol steps. If such a derivation exists, the protocol is successfully verified.

Logic-based formal verification involves the following steps:

1. *Formalization of the protocol messages*;
2. *Specification of the initial assumptions*;
3. *Specification of the protocol goals*;
4. *Application of the logical postulates*.
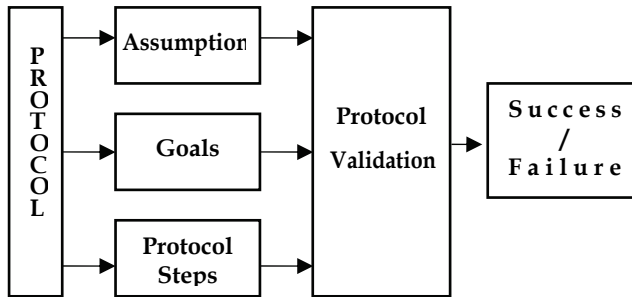
Fig. 1. The process of verification with modal logic

The first step in logic-based verification involves specifying the protocol in the language of the logic by expressing each protocol message as a logical formula. This step is known as protocol formalization (some authors also refer to it as idealization). A formal description of the protocol, obtained by formalization, does not simply list the components of each message but attempts to show the purpose of these components so as to avoid ambiguity.

The second step in the verification process involves formally specifying the initial protocol assumptions. These assumptions reflect the beliefs and possessions of the involved principals at the beginning of each protocol run.

In the third step, the desired protocol goals are expressed in the language of the logic. These goals are specified in terms of the beliefs and possessions of the protocol participants at the end of a successful protocol run.

The final verification step concerns the application of logical postulates to establish the beliefs and possessions of protocol principals. The objective of the logical analysis is to verify whether the desired goals of the protocol can be derived from the initial assumptions and protocol steps. If such a derivation exists, the protocol is successfully verified; otherwise, verification fails. A successfully verified protocol can be considered secure within the scope of the logic. On the other hand, even the results of failed verification are helpful, as these may point to missing assumptions or weaknesses in the protocol. If a weakness is discovered, the protocol should be redesigned and re-verified. However, verification logic techniques have their limitations, not least of which is the likelihood of errors in protocol formalization. The number of opportunities to make such mistakes increases as the verification process becomes more complicated, requiring a thorough understanding of the logic used. During the verification process, the semantics of the protocol must be interpreted, in order to specify the meaning that a protocol message is intended to convey. This 'interpretation process' is somewhat controversial––different authors may interpret the same messages differently. If the formalized protocol does not properly represent the original design, then the proof demonstrates only that the protocol corresponding to this formal description is secure. However, no claims can be made on the security of the original design. Lack of clarity about protocol goals and initial assumptions is a further cause for concern.

In some cases the same protocol may be used for slightly different purposes. For example if a protocol is used to generate a new session key, each principal involved in the protocol run may require that the other principal believes the session key to be a shared secret. This property is known as second level belief. If a protocol is verified as secure for first level belief only and used in an application where second level belief is required, serious security breaches are likely. Hence, it is vital to note the assumptions and goals under which a security protocol is considered secure during its formal verification.

Despite these criticisms, different logic techniques have identified numerous protocol weaknesses and are considered as successful. Gligor et al. (Gligor et al., 1991) summarize the virtues of authentication logic as follows:

- They help formalize reasoning about useful abstract properties of cryptographic protocols.
- They force designers to make explicit security assumptions.
- They achieve a reasonably well-defined set of authentication goals.

4. The RFID authentication protocol and its verification

Firstly, the behavior of the hash unlocking protocols is modeled as hash unlocking of the hash lock scheme. The simple description of the hash locking is already described in Section 2.1 and the role of the reader simply writes the metaID as a keyed hash value in the tag. The general overview of the authentication protocol (Fig.2) is as follows;

T	RF tag's identity
R	RF reader's identity
DB	Back-end server's identity that has a database
Xkey	Session key generated randomly from X
metaID	Key generated from reader using hash function
ID	Information value of tag
Xn	A random nonce generated by X
H	Hash function
$E_{key}(M)$	Encrypted message with key

Table 1. Hash lock scheme notation

```
Message 1. : R  -> T  : Query
Message 2. : T  -> R  : metaID
Message 3. : R  -> DB : metaID
Message 4. : DB -> R  : Rkey, ID
Message 5. : R  -> T  : Rkey
Message 6. : T  -> R  : ID
```

Fig. 2. The overview of the hash unlocking protocol

- Message 1: Request by the reader.
- Message 2: The tag transmits the metaID(locked value as hashed key) to the reader.
- Message 3: The reader forwards the metaID to the Database.

- Message 4: The database transmits the original key value and tag ID to the reader after checking the match between metaID from the reader and metaID in the database.
- Message 5: The reader transmits original key to the tag to ensure tag authentication.
- Message 6: The tag transmits its information value to the reader.

(X,Y)	Concatenation of two formulae
{X}K,	Symmetric encryption and decryption
{X}K-	The formula X is fresh. X has not been sent in a message at any time before
#(X)	the current run of the protocol
ϕ(X)	Formula X is recognizable
P◁ X	P has a received a message containing X and P can read and repeat X, possibly after performing some decryption
P◁*(X)	P is told formula X which he did not convey previously during the current
P ∋ X	protocol run
P |~ X	P possesses or is capable of possessing formula X
P |≡ X	P conveyed X
	P believes X. That is, the principal P acts as if X is true
X ~> C	Formula X has the extension C. The precondition for X being conveyed is represented by statement C
P |⇒ X	P has jurisdiction over X. The principal P is an authority on X and should be trusted on this matter. This construct is used when a principal has delegated authority over some statement
P $\xleftrightarrow{K}$ Q	K is a suitable secret for P and Q. They may use it as a key to communicate or as a proof of identity

Table 2. Notation of GNY logic

4.1 Formalization of the protocol step

M 1. $R \triangleleft *metaID \sim> R \mid\equiv \xrightarrow{H(RKey)} T,$
$\qquad\qquad T \mid\equiv R \mid\sim H(RKey)$

M 2. $DB \triangleleft *metaID$

M 3. $R \triangleleft RKey, *ID \sim> R \mid\equiv \xrightarrow{RKey} DB,$
$\qquad\qquad R \mid\equiv \xrightarrow{ID} DB$

M 4. $T \triangleleft RKey$

M 5. $R \triangleleft ID$

Fig. 3. Formalization of the protocol step

A formalized version of the protocol is shown in Fig.3 (from table 2). The asterisks denote the ability of each principal to recognize that it did not transmit the received message at an earlier stage in the protocol.

In M1, the reader is told the metaID (locked value as hashed key) from the tag and the message extension in the first message indicates that if a reader transmits a H(RKey) to lock a tag, then the tag believes that RKey contained in that metaID belongs to the reader. In M2,

the DB is told the metaID from the reader and it means the metaID is forwarded from the reader to DB. In M3, the reader is told the original key value and tag ID from the database to the reader after checking the match between metaID from the reader and metaID in the database and the message extension in the third message indicates that if the reader receives RKey and ID from some principal, then the reader believes that RKey contained in that metaID belongs to the DB. In M4, the tag is told the original key from the reader and in M5, the reader is told the tag ID from the tag.

4.2 Specification of the initial assumptions
The initial assumptions for the hash unlocking protocol are as follows:

$$T \ni metaID \; ; \; T \ni RKey \; ; \; T \ni ID;$$
$$DB \ni RKey \; ; \; DB \ni ID \; ;$$
$$R \mid\equiv \phi(RKey); \; R \mid\equiv \phi(ID);$$
$$T \mid\equiv \xrightarrow{RKey} DB; \; T \mid\equiv \xrightarrow{ID} DB;$$
$$T \mid\equiv DB \mid\Rightarrow DB \mid\equiv *; \; R \mid\equiv DB \mid\Rightarrow DB \mid\equiv *;$$

The first two rows state the possessions of both principals. Each principal possesses its information, its symmetric key and its identification data. The next row states the recognizability assumptions. Reader recognizes his symmetric key and other's identification data. The final two rows concern beliefs regarding the database server. Tag believes that RKey is the symmetric key between DB and Reader, ID is a secret value for DB and Tag, that DB is honest and competent, and that DB has jurisdiction over the other principal's symmetric key.

4.3 Specification of the protocol goal
The goals of the hash unlocking protocol are as follows:

$$R \mid\equiv \#H(RKey); \; T \mid\equiv \#H(RKey);$$
$$T \mid\equiv R \mid\sim RKey; \; R \mid\equiv T \mid\sim ID;$$
$$R \ni ID$$

The goals in the first row state that both principals believe it to be fresh. The next row concerns authentication: each principal should believe that its counterpart conveyed the respective identification data. The goal on the remaining row describes the confidentiality of the information.

4.4 Application of the logical postulates (from Appendix)
M 1. $R \triangleleft *metaID \rightsquigarrow R \mid\equiv \xrightarrow{H(RKey)} T, \; T \mid\equiv R \mid\sim H(RKey)$

- Applying T1 to M 1 yields $R \triangleleft metaID$. R is told T's metaID without not-originated-here asterisk.
- Applying P1 yields $R \ni metaID$. The reader possesses the metaID value of the tag.
- Since R recognizes RKey, by R1 $R \mid\equiv \phi(H(RKey))$. R recognizes the H(RKey).
- However, R cannot believe that metaID is the valid current value of the tag. The preconditions of J2 are not achieved and the freshness of H(RKey) is not satisfied. An intruder could use an old compromised hash value belonging to the tag in order to masquerade as the reader.

M 2. DB ◁ *metaID

- Applying T1 to M 2 yields *DB ◁ metaID*. DB is told T's metaID without not-originated-here asterisk.
- Applying P1 yields *DB ∍ metaID*. The database possesses the metaID value of the tag.
- However, R still cannot believe that metaID is the valid current value of the tag. The preconditions of J2 are not achieved as in *M 1*. An intruder still could use an old compromised hash value belonging to the tag in order to masquerade as the reader.

M 3. R ◁ RKey, *ID ~> R |≡ $\xrightarrow{RKey}$ DB,R |≡ $\xrightarrow{ID}$ DB

- Applying T1 and P1 yields *R ∍ (RKey, ID)*. The reader possesses the (RKey, ID). By T2, *R ∍ RKey, R ∍ ID.*
- However, R cannot believe that RKey is the valid current value from the tag's metaID. Since the freshness of RKey is not satisfied, the reader cannot transmit RKey to the tag.

M 4. T ◁ RKey

M 5. R ◁ ID

- Applying T1 and P1 to M4 and M5 yields *T ∍ RKey, R ∍ ID.*
- However, by I4, J2, the tag cannot believe that the reader transmits RKey to the tag. The reader cannot believe that the tag transmits the ID to the reader.

4.5 Weakness in the Hash unlocking protocol
The above verification of the hash unlocking protocol identifies the following failed goals:
1. R cannot derive that the H(RKey) is fresh;
2. T cannot derive that the H(RKey) is fresh;
3. T cannot derive that R conveyed RKey ;
4. R cannot derive that T conveyed ID;
5. R cannot derive that ID is valid;

5. The proposed the strong authentication protocol for RFID systems

5.1 Analysis of the strong authentication protocol using GNY logic
In the previous schemes (Weis et al., 2003; Ohkubo et al. 2004; Henrici & Muller, 2004; Hwang et al., 2004), it is assumed that database is a TTP (Trusted Third Party) and the communication channel between reader and database is secure. However, this paper assumes that database is not a TTP and the communication channel is as insecure as current wireless networks. It is also assumed that k is the secret session key shared between reader and database, and reader and database have enough capability to manage the symmetric-key crypto-system and sufficient computational power for encryption and decryption.
To satisfy security requirements, the most effective protective measure against an attack involving eavesdropping at the air interface is not to store any contents on the tag itself and instead to read only the ID of the tag that database has transmitted to be scanned from reader. This measure, which is most often recommended in the technical literature and which is assumed by EPC global, offers the additional advantages that less expensive tags can be used, the memory for the associated data in the database is practically unlimited. The main idea of this framework is based on the security algorithm employed in the Yahalom protocol(Paulson, 2001).

The proposed protocol must guarantee the secrecy of the session key: in message 4, 5, the value of the session key must be known only by participants playing the roles of T and R. R and T also must be properly authenticated to the DB.

$$\text{Message 1. R} \quad \text{-> T} \quad : \text{Query}$$
$$\text{Message 2. T} \quad \text{-> R} \quad : \text{Tn}$$
$$\text{Message 3. R} \quad \text{-> DB:} \; E_{ServerKey(R)} \, (\, T, Tn, Rn \,)$$
$$\text{Message 4. DB -> T} \quad : E_{ServerKey(T)} \, (\, R, DBkey, Tn, Rn, ID)$$
$$\text{Message 5. DB -> R} \quad : E_{ServerKey(R)} \, (\, T, DBkey \,)$$
$$\text{Message 6. T} \quad \text{-> R} \quad : E_{DBkey} \, (\, ID \,)$$

Fig. 4. Overview of the proposed strong authentication protocol

The main idea of the proposed protocol is that the ServerKey and Tag's Nonce(Tn) is used to minimize the burden of the Tag and to ensure authentication between Tag and Reader. The definition of a function called ServerKey that takes in the name of a Server and returns a ServerKey could be regarded as shared: Agent -> ServerKey. If reader would like to transmit any messages to database, then he would use the ServerKey with his identity as parameter. This description resembles a functional programming language.

The general description of the proposed protocol is described as follows;
- Message 1: Query request by the reader
- Message 2: T is defined to take a random nonce Tn and transmit R. This makes simple challenge-response easy.
- Message 3: Through T, Tn, and Reader's Nonce (Rn) with Server Key, R can ensure database authentication.
- Message 4: DB encrypts all of the R, DBkey, Tn, Rn, and ID received from R and transmits these to T to allow R to authenticate securely using the server key.
- Message 5: DB also transmits T, DBkey to R to decrypt Tag's ID.
- Message 6: T can transmit ID securely using the DBkey received in Message 4.

In addition, message 4,5 mean the protocol step that can be transmitted from database to other participants simultaneously to decrypt the tag's ID in message 6.

5.1.1 Formalization of the protocol steps

$$M \, 1. \; R \quad \vartriangleleft *Tn$$
$$M \, 2. \; DB \vartriangleleft *\{T, Tn, Rn\}K(R)$$
$$M \, 3. \; T \quad \vartriangleleft \{*R, *DBKey, Tn, *Rn, *Id\}K(T)$$
$$M \, 4. \; R \quad \vartriangleleft \{T, *DBKey\}K(R)$$
$$M \, 5. \; R \quad \vartriangleleft \{*Id\}DBKey$$

Fig. 5. The formalization of the protocol step

A formalized version of the protocol is shown in Fig. 5. The asterisks denote the ability of each principal to recognize that it did not transmit the received message at an earlier stage in the protocol. The protocol step in message 1 (Fig.4.) was omitted in Fig 5.

5.1.2 Specification of the initial assumption

The initial assumptions for the proposed protocol are as follows;

$$T \ni Tn; T \ni K(T); R \ni Rn; R \ni K(R);$$
$$DB \ni Id; DB \ni DBKey; DB \ni K(T); DB \ni K(R);$$
$$T \models \phi(Id); T \equiv \phi(T, DBKey);$$
$$R \equiv \phi(Id); R \equiv \phi(DBKey);$$
$$T \equiv \#Tn; R \equiv \#Rn; DB \equiv \#DBKey;$$
$$T \equiv \xrightarrow{DBKey} DB; T \equiv \xrightarrow{K(T)} DB; T \equiv(DB \Rightarrow \xrightarrow{DBKey} R);$$
$$R \equiv \xrightarrow{DBKey} DB; R \equiv \xrightarrow{K(R)} DB; R \equiv(DB \Rightarrow \xrightarrow{DBKey} T);$$

The first two rows mean that each principal possesses its random nonce, symmetric key and information data. The next two rows state that the tag and reader recognize the other's symmetric key and information data. The next row means that each principal believes its nonce or key freshness. The final two rows concern beliefs regarding the database server that DB has jurisdiction over its own key and the other principal's symmetric key.

5.1.3 Specification of the protocol goal

The goals of the proposed protocol are as follows;

$$DB \equiv \#\{T, Tn, Rn\}K(R);$$
$$T \equiv \#\{R, DBKey, Tn, Rn, Id\}K(T);$$
$$R \equiv DB \mid \sim \{DBKey\}K(R); R \equiv T \mid \sim \{ID\}DBKey;$$
$$T \equiv T \xleftrightarrow{DBKEY} R; R \equiv T \xleftrightarrow{DBKEY} R;$$
$$R \ni Id$$

The first three rows concern authentication: each principal should believe that its counterpart is conveyed in the respective identification data. The goals in the fourth row describe key agreement: both principals should possess the shared key through a challenge-response process. The goal on the remaining row describes the confidentiality of the information.

5.1.4 Application of the logical postulates(from Appendix)

M 1. $R \triangleleft {}^*Tn$

- Applying T1 and P1 yields $R \ni Tn$. The reader possesses the T's random nonce.

M 2. $DB \triangleleft {}^*\{T, Tn, Rn\}K(R)$

- Applying T1 and T3 yields $DB \triangleleft T, Tn$, and Rn, by T2 and P1 $DB \ni T, DB \ni Tn, DB \ni Rn$.
- Applying F1 yields $DB \equiv \#\{T, Tn, Rn\}K(R)$ and satisfies the goal at the first row in Section 5.1.3.

M 3. $T \triangleleft \{{}^*R, {}^*DBKey, Tn, {}^*Rn, {}^*ID\}K(T)$

- Applying T3 yields $T \triangleleft ({}^*R, {}^*DBKey, Tn, {}^*Rn, {}^*ID)$.
- Applying T2 and T1, P1 yields $T \ni DBKey, T \ni Tn, T \ni Rn,$ and $T \ni ID$.
- Applying F1 yields $T \equiv \#\{R, DBKey, Tn, Rn, ID\}K(T)$ and satisfies the goal at the second row.

M 4. $R \triangleleft \{T, *DBKey\}K(R)$

- Applying T3 yields $R \triangleleft \{T, *DBKey\}$.
- Applying T2, T1 and P1 yields $R \ni DBKey$.
- Applying I4 yields $R \mid\equiv DB \mid\sim \{DBKey\}K(R)$ and satisfies the first goal at the third row.
- Applying $R \ni DBKey$ and I4, yields $R \mid\equiv T \mid\sim \{ID\}DBKey$ and satisfies the second goal at the third row.

M 5. $R \triangleleft \{*ID\}DBKey$

- Applying T3 and P1 yields $R \ni ID$ and satisfies the goal at the last row.

Through $T \ni DBKey$ in M3. and $R \ni DBKey$ in M4., the goals($T \mid\equiv T \xleftrightarrow{DBKEY} R$; $R \mid\equiv T \xleftrightarrow{DBKEY} R$;) at the fourth row.

Lists	Hash Lock	Randomized Hash	Chained Hash	Proposed
Data confidentiality	-	-	-	O
Tag anonymity	-	-	-	O
Data integrity	-	O	O	O
Reader authentication	-	O	O	O
DB authentication	O	O	-	O
MitM attack	-	-	-	O
Replay attack	-	O	-	O

Table 3. Comparison among protocols (o: secure, -: insecure)

From table 3, it can be seen that the proposed protocol meets all security requirements listed above. These protocols were primarily designed to provide link security to protect against passive and active attacks over the air interface. Due to the limitation of the space, all result that been analyzed the vulnerabilities about other protocols, randomized protocol and chained hash protocol were described in brief in table 3.

5.2 The result of verification

After verifying the protocols using GNY logic, it is confirmed that the proposed protocol solves the security weakness in previous hash-based protocols.

- Secrecy: Spoofing, Replay Attack, Tracking, Eavesdropping on communication between tag and reader are attacks that threaten all participants. To protect from these attacks, the countermeasures are therefore essentially identical in this protocol as follows. Firstly, shifting all data except ID to the backend. This is also to be recommended for reasons of data management (i.e. the ID for the tag existing at the backend database will be shifted to protect spoofing and eavesdropping attacks to the tag through the database when the reader sends a request).
  Secondly, encoding data transmission: encryption of the data transmission is supported to ensure authorized access to the data of concern and to protect replay attacks and tracking.
- Authentication: When a tag receives a "get challenge(query)" command from a reader, it generates a random number Tn and sends this number to the reader. The reader in

turn generates a random number Rn with it and the random number Tn generates an encrypted data block (token T) on the basis of an encryption algorithm and server key (R). The data block is then returned to the database to authenticate the reader. The reader and tag both use the same encryption algorithm and since the server key is stored on the tag, the tag is capable of decrypting the server key(T). If the original random number Tn and the random number Tn, which has now been decrypted, are identical, then the authenticity of the tag vis-a-vis the reader is demonstrated.

5.3 The comparison of availability

In this paper, we propose the strong symmetric key algorithm based RFID authentication protocol. Regarding performance of protocol in application level, our assumption is that CPUs are now faster and memory and network speeds have also increased, but not nearly as much as CPU speeds. Pure computation, such as is used in a block cipher, is cheaper in both absolute terms and relative to other tasks, such as writing the data to disc. Unlike DES, nearly all of the AES candidates are designed for high performance in software.

It could be argued that for most applications, nearly all the AES algorithms are fast enough. Some literature(Roe, 2000) reached the point where cryptography is not a significant portion of the total CPU burden, and the relative speed of the algorithms no longer matters very much. Therefore, our proposed protocol can be available for light-weight tags in the RFID system.

6. Discussion and conclusions

Home network is defined as environments where users can receive home network services for anytime and anywhere access through any device, connected with a wired and wireless network to home information appliances including the PC. In this environment, there are many security threats that violate user privacy and interfere with home services. Especially, the home network consists of several networks with RFID system therefore authentication between the reader and the appliance devices affixed tag is required.

In this paper, the RFID security requirements in home network environments are defined, and authentication mechanism among reader, tag and database is proposed. The focus is to analyze the vulnerabilities of the protocol using formal methods and to design and verify the secure authentication protocols, which is widely researched in RFID systems. In verifying these protocols using GNY logic, it is possible to confirm some of the known security vulnerabilities likely to occur in RFID systems.

Finally, a strong authentication protocol based encryption algorithm, is proposed for guarding against man-in-the-middle, and replay attacks, and also for verifying safety using GNY logic.

7. Appendix. GNY logical postulates

In this appendix we list the logical postulates of GNY logic used throughout this paper.

T 1 : $\dfrac{P \triangleleft {}^*X}{P \triangleleft X}$

If a principal is told a formula is marked with a not-originated-here asterisk, then the principal is told that formula.

T2 : $\underline{P \lhd (X, Y)}$

       $P \lhd X$

Being told a formula implies being told each of its concatenated components.

T3 : $\underline{P \lhd \{X\}K, P \ni K}$

        $P \lhd X$

If a principal is told that he possesses a formula encrypted with a key, then he is considered to have been told the decrypted contents of that formula.

P1: $\underline{P \lhd X}$

     $P \ni X$

A principal is capable of possessing anything he is told.

F1 : $\underline{\qquad P \mid\equiv \#(X) \qquad}$

     $P \mid\equiv \#(X, Y), P \mid\equiv \#(F(X)).$

If a principal believes that a formula X is fresh, then it is believed that any formula of which X is a component is fresh and that a computationally feasible one-to-one function, F, of X is fresh.

R1 : $\underline{\qquad P \mid\equiv \phi\,(X) \qquad}$

     $P \mid\equiv \phi\,(X, Y), P \mid\equiv \phi\,(F(X)).$

If a principal believes that a formula X is recognizable, then it is believed that any formula of which X is a component is recognizable and that a computationally feasible one-to-one function, F , of X is recognizable.

I4 : $\underline{P \lhd \{X\}K\text{-}, P \ni K\text{+}, P \mid\equiv \overset{K+}{\mapsto} Q, P \mid\equiv \phi\,(X), P \mid\equiv \#(X, K\text{+})}$

          $P \mid\equiv Q \mid\sim X, P \mid\equiv Q \mid\sim \{X\}K\text{-}.$

If, for principal P, the following conditions hold: P receives a formula X encrypted under private key (K-), P possesses the corresponding public key (K+), believes the public key belongs to Q, and P believes that the formula X is recognizable that either X or K+ is fresh. Then, P believes that Q once conveyed the message X, and that Q once conveyed the message X encrypted under Q's private key   (K-).

J2 : $\underline{P \mid\equiv Q \mid\Rightarrow Q \mid\equiv *, P \mid\equiv Q \mid\sim(X\sim>C), P \mid\equiv \#(X)}$

            $P \mid\equiv Q \mid\equiv C$

If principal P believes that Q is honest and competent and P receives a fresh message X with the extension C, which he believes Q conveyed, then P believes that Q believes C.

8. References

Sarma, S.; Weis, S. & Engels, D. (2003). RFID systems and security and privacy implications, *Workshop on Cryptographic Hardware and Embedded Systems (CHES) 2002*, LNCS No. 2523, pp. 454-469.

EPCGLOBAL INC.: http://www.epcglobalinc.org.

Burrows, M.; Abadi, M. & Needham, R. (1989). A Logic of Authentication, *ACM Operating System Review*, Vol.23, No.5, pp.1-13.

Hoare, C.A.R. (1985). *Communicating Sequential Processes*, Prentice-Hall, Englewood Cliffs, NJ.

Lowe, G. (1997). Casper: A compiler for the analysis of security protocols, *The 1997 IEEE Computer Security Foundations Workshop X, IEEE Computer Society*, Silver Spring, MD, pp. 18-30.

Formal Systems Ltd. FDR2 User Manual, Aug. 1999.

Weis, S., Sarma, S., Rivest, R. & Engels, D. (2003). Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems, *Proceedings of Security in Pervasive Computing (SPC)*.

Ohkubo, M., Suzuki, K. & Kinoshita, S. Cryptographic Approach to Privacy-Friendly Tags, *RFID Privacy Workshop*, Massachusetts Institute of Technology, Cambridge, MA, USA.

Ohkubo, M., Suzuki, K. & Kinoshita, S. (2004). Hash-Chain Based Forward-Secure Privacy Protection Scheme for Low-Cost RFID, *Symposium on Cryptography and Information Security*, pp.719-724.

Henrici, D. & Müller, P. (2004). Hash based Enhancement of Location Privacy for Radio-Frequency Identification Devices using Varying Identifiers, *Proceedings of PerSec'04 at IEEE PerCom*, pp.149-153.

Hwang, Y., Lee, S., Lee, D. & Lim, J. (2004). An Authentication Protocol for Low-Cost RFID in Ubiquitous, *Proceedings of CISC S'04*, pp.109-114.

Mathuria, A., Safavi-Naini, R. & Nikolas, P. (1994). Some Remarks on the Logic of Gong, Needham, and Yahalom, *The International Computer Symposium*, Vol.1, pp.303-308.

Gligor, V.D., Kailar, R., Stubblebine, S. & Gong, L. (1991). Logics for Cryptographic Protocols – Virtues and Limitations, *Proceedings of Computer Security Foundation Workshop*, pp. 219-226.

Lawrence Paulson, C. (2001). Relations between Secrets: Two Formal Analyses of the Yahalom Protocol, *Proceedings of IEEE Computer Security*.

Gong, L., Needham, R. & Yahalom., R. (1990). Reasoning about Belief in Cryptographic Protocols, *Proceedings of The 1990 IEEE Symposium on Security and Privacy*, pp. 18-36.

Roe, M. (2000). Performance of Protocols: Security Protocols, *Lecture Notes in Computer Science 1796*, pp.140-146.

Kim, H. S., Oh, J. H. & Choi, J.Y. (2006). Security Analysis of RFID Authentication for Pervasive Systems using Model Checking, *Proceedings of The thirtieth Annual International COMPSAC*, pp. 195-202.

Evaluation of Group Management of RFID Passwords for Privacy Protection

Yuichi Kobayashi[1], Toshiyuki Kuwana[1],
Yoji Taniguchi[1] and Norihisa Komoda[2]
[1]Hitachi, Ltd.,
[2]Osaka University
Japan

1. Introduction

The RFID tag is equipped with a small IC tip and antenna, and data can be read from or written to it via radio signal. This device has attracted much attention because it is extremely effective for promoting work efficiency in supply chains and for building IT-based systems connecting companies and/or industries. The scope of RFID use is spreading throughout the entire product life cycle, and RFID is now used not only for primary distribution from production to sale, but also for secondary forms of distribution, such as recycling or maintenance.

The difference between the scope of primary distribution only and the scope of a product's entire life cycle is that in the latter a greater number of general companies and people are involved in the distribution process. Therefore, a provision for protecting data written to RFID tag memory must be included when RFID systems are built so that data cannot be illegally read or overwritten.

In addition, a solution to RFID privacy problems is required so that items with RFID tags can be safely provided to many consumers (CASPIAN et al., 2003; Albrecht & Mcintyre, 2005). We define the privacy problem as unauthorized persons abusing the radio-communications function of RFID tags, and we consider two kinds of privacy problem:

a. Possession Privacy Problem: This is the problem of unauthorized persons or agents being able to surreptitiously detect items that other persons are carrying because of the item codes recorded in the memory of IC tags.

b. Location Privacy Problem: This is the problem of an unauthorized persons or agents knowing where a person is without that person's knowledge because a unique ID is recorded in an IC tag memory.

A guideline for solving privacy problems (GS1 EPCglobal, 2005) states that RFID tags should be removed from products before the products are provided to consumers. However, the requirements for consumers, who want to protect their privacy, conflict with those of industries that want to use RFID tags throughout the entire life cycle of products – satisfying both requirements is very difficult.

To protect consumer privacy, some researchers have proposed systems that mount a hash function in the RFID tag which authenticates interrogators (Weis, 2003; Juels.& Pappu, 2003;

Engberg et al., 2004). However, a hash function has too many gates to satisfy user preferences regarding the size of RFID chips, the communication distance, and the need for an anti-collision algorithm (Satoh & Inoue, 2007). Therefore, mounting hash functions in RFID tags is too difficult at present. We think mounting a function that authenticates the interrogator by using a password is more realistic.

The password authentication function mounted in RFID is standardized by international standards specification ISO/IEC 18000-6 Type C. RFID tags that included a read lock function for privacy protection based on ISO/IEC 18000-6 Type C were developed in the Secure RFID Project (Honzawa, 2008) established by the Ministry of Economy, Trade, and Industry in 2006. To read data in the memory of such RFIDs, authentication of a RFID password requires this read lock function as well as a write lock function. Both these functions prevent illegal reading and writing of the data in RFID memory. However, the security of all RFID tags is compromised when one RFID password is stolen if all the RFID passwords are identical. To reduce the severity of this problem requires setting up a different RFID password for every group of RFID tags.

In this paper, we propose a system for using RFID tags that includes an interrogator with an algorithm that generates RFID passwords. This system sets up the grouping of RFID passwords for RFID tags that are used in the secondary distribution stage, and protects both the RFID data and consumer privacy.

2. Problem with RFID password management for RFID system

RFID passwords must be managed rigorously to prevent attacks that illegally rewrite data or threaten consumer privacy when data is stored in the memory of RFID tags conforming to the Secure RFID Project specification based on ISO/IEC 18000-6 Type C. If all RFID passwords set in RFID tags are identical throughout an industry, theft of one RFID password will compromise all RFID tags.

To solve this problem, we considered a system that sets up a different RFID password for each group of RFID tags. Although this system does not improve the security of individual RFIDs tags, it narrows the extent of the risk to the whole system. For example, consider the case in which an RFID tag is illegally accessed and its password is stolen. As Fig. 1(a) shows, if the same RFID password, X, has been set to all RFID tags, anyone with the stolen password will be able to access all the RFID tags by using the stolen RFID password X. However, as Fig. 1(b) shows, when a different RFID password is assigned for each group of RFID tags, even if an unauthorized user has stolen the RFID password they can access only one group of RFID tags; the other groups of RFID tags remain safe. Therefore, as few RFID tags have the same RFID password, the damage from a stolen RFID password is contained.

When setting up a different RFID password for every group of RFID tags, though, one has to be careful regarding this privacy protection. For an authorized interrogator to access RFID tags, it must be able to manage the relation between an RFID tag and a RFID password. The identifier of an RFID tag must not be used for invading privacy even though an RFID tag must be discriminable for interrogators to manage the relation between the tags and an RFID password. Therefore, an RFID system used throughout the entire life cycle of a product should satisfy the following requirements:

a.   The system must manage the relation between an RFID tag and the grouping RFID password of the RFID tag, and be able to generate a grouping RFID password for the RFID tag immediately after inventorying it.

b. The system must use as little item information as possible for the identifier of RFID tags to protect possession privacy.
c. The system must avoid using unique IDs for the identifier of RFID tags, as much as possible, to protect location privacy.
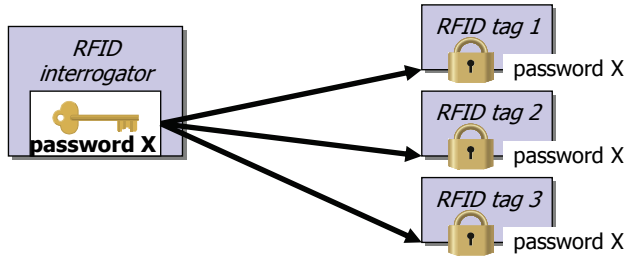
(a) Common RFID Password
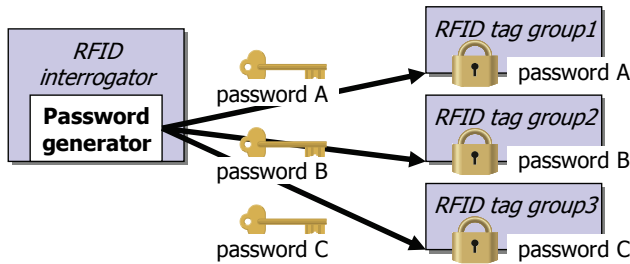
(b) Group RFID Password

Fig. 1. Systems in which interrogators access RFID tags by using RFID passwords

3. An RFID system that generates group RFID passwords

3.1 Group RFID password generation method

An RFID system that generates group RFID passwords only allows authorized interrogators to access RFID tags, and allows those interrogators to read or write data in the RFID memory. Each RFID tag receives an RFID password from an interrogator and authenticates the interrogator; i.e., judges whether the interrogator is authorized for access.

This system sets data called "PASS KEY" for generating a different RFID password for every group of tags, and sets the RFID password as an RFID tag. A group RFID password generation algorithm that finds the right RFID password for each group of RFID tags and sends it to the RFID tag is mounted in an authorized interrogator. The parameters of the grouping RFID password generation algorithm are a master key and a PASS KEY written in an RFID tag.

Figure 2 is a flow chart of the procedure for generating and managing the group RFID passwords.

In the preparation stage, a user chooses a random number as the PASS KEY. The group RFID password generation algorithm calculates this PASS KEY by using a function with collision resistance and pre-image resistance; i.e., a hash function with a master key. The calculation result that this algorithm outputs is used as the group RFID password. The system sends and sets selected PASS KEYs and the generated group RFID passwords to

RFID tags. Since a different PASS KEY is chosen for each group of RFID tags, the RFID password is also set as a different value for each group of RFID tags.
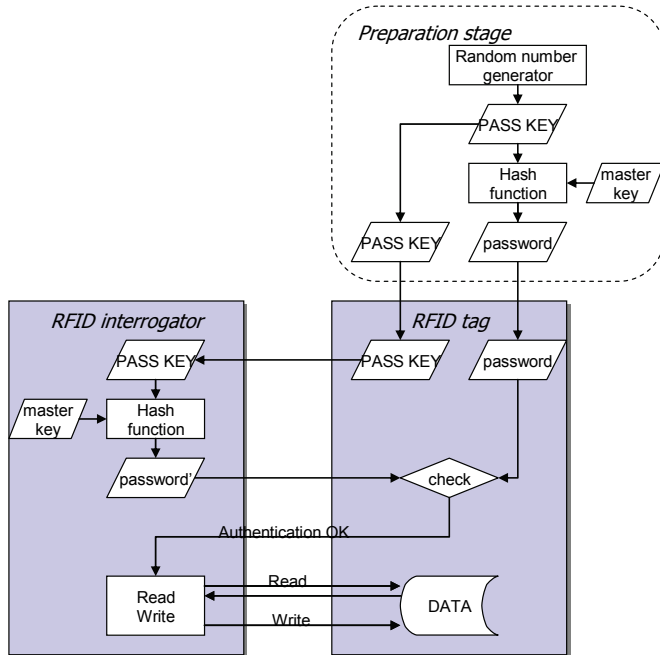
Fig. 2. Procedure for generating group RFID passwords

Whenever a user accesses an RFID tag, the user's interrogator first demands the RFID PASS KEY. The RFID tag receives this demand and reports the PASS KEY to the interrogator. The interrogator first calculates the PASS KEY that it receives from the RFID tag by using a master key and a hash function, and then generates a group RFID password. The interrogator then sends the generated group RFID password to the RFID tag. The RFID tag compares the received group RFID password to the group RFID password that was programmed into it in the preparation stage. If the two RFID passwords are the same, the RFID tag will change to the secured state. When the RFID tag changes to the secured state, the user can read or write to the data in the RFID memory.

Authorized users are not the only ones who can get the PASS KEY from this RFID tag; unauthorized people or agents can also get it. However, since those without authorization do not know the master key, they cannot generate the group RFID password from the PASS KEY, and they cannot read or write to data in the RFID tag.

Generating group RFID passwords requires that the procedure to generate two RFID passwords with the same value from two different PASS KEYs must be made difficult, and decoding a master key from a RFID password and a PASS KEY must also be difficult. Therefore, we adopt a hash function equipped with collision resistance and pre-image resistance as our group RFID password generation algorithm. To construct an RFID system with higher security, an effective method is to use a hash function that has been previously evaluated by the public, such as SHA-1, and to store the master key in a tamper-resistant device.

3.2 Structure of an RFID system with a group RFID password generation method

Here, we provide an example of the structure of an RFID system that uses a group RFID password generation method that sets up and manages group RFID passwords in RFID tags. Figure 3 presents the structure of this system. This system uses RFID tags conforming to the Secure RFID Project specification based on ISO/IEC 18000-6 Type C. The tags are mounted with rewritable memory and an authentication function. The system also includes interrogators, conforming to the Secure RFID Project specification, that communicate with the RFID tags and a tamper-resistant device that restricts users and generates group RFID passwords. The system has middleware that controls the interrogators, the tamper-resistant device, and an RFID application. The middleware and the application can be installed in a terminal. The tamper-resistant device has a user authentication function to prevent unauthorized use of this system and a grouping RFID password generation algorithm that minimizes the damage when RFID passwords are disclosed to unauthorized users.

The user authentication function in the tamper-resistant device applies PIN authentication technology. Users can only use an interrogator after they input an authentic PIN. If they fail to do so, they cannot use an interrogator and cannot access RFID tags. This PIN authentication function can prevent unauthorized use of the interrogator, even if the interrogator is stolen.

The group RFID password generation algorithm is also mounted in the tamper-resistant device, and is processed within this device to prevent leaks and misappropriation of the group RFID password generation algorithm.
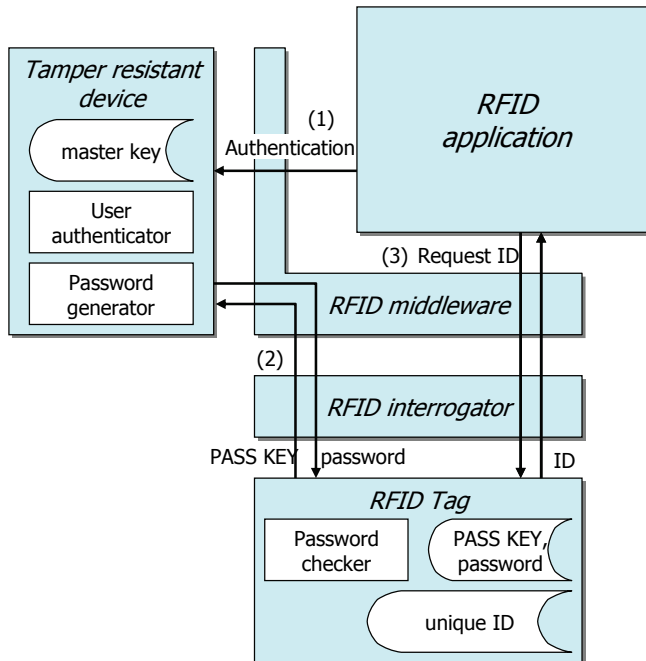
Fig. 3. Structure of system for group RFID password generation

4. Solutions to privacy problems

To protect possession privacy, PASS KEY data should not include any data that identifies items; e.g., an item code or a product number. PASS KEY data should be meaningless data such as a random number. If the PASS KEY is unique and anyone can read it, location privacy is at risk. Moreover, if the PASS KEY of many RFID tags is set up to be identical, many tags will be affected if one RFID password is leaked since the RFID password for every group of RFID tags is also identical. Therefore, some PASS KEYs should be set up as identical to reduce the risk of privacy invasion, and some PASS KEYs must be distributed so that the effects of RFID password disclosure will be limited. We estimated the number of equivalent PASS KEYs that satisfies these two demands by the following methods.

When a PASS KEY is read, the probability of those who are carrying the RFID tag to be specified by that PASS KEY can be calculated as the number of those who can be found out of the entire group carrying an RFID tag that stores identical PASS KEYs. We call this probability the specific probability R.

When we define the number of the tags with the same PASS KEY as the equivalent number M, the specific probability of privacy invasion R can be explained as a reciprocal of the equivalent number M.

$$R = 1/M \qquad (1)$$

On the other hand, the influence level of RFID password disclosure, E, when an RFID password is leaked is calculated as the number N of the RFID tags in the market and the equivalent number M, which is the number of tags with the same RFID password.

$$E = M/N \qquad (2)$$

Risk, F, is defined as the sum of the weight of the specific probability R and the influence level E. To improve the balance of both specific probability R and the influence level E, we calculate the equivalent number M that provides the lowest risk F. Here, the weight is expressed as w.

$$F = R + wE = 1/M + w\,M/N \qquad (3)$$

$$M_{\min} = \sqrt{w^{-1}N} \qquad (4)$$

The weight w corresponds to the probability that an RFID password will be leaked.

Figure 4 shows the relations between the probability of privacy invasion R, the influence level of RFID password disclosure E and the risk F. In this figure, we show that if specific probability R is set too low, the risk F become high because the influence level E becomes high. In the following section, we find the effective equivalent number M_{min} in the case of a shopping mall where RFID tags are used.

5. Evaluation of the proposal method's applicability

5.1 Trail analyzing simulation for invasion of location privacy

In this section, we simulate the probability of someone being able to invade a consumer's location privacy in a shopping mall. We assume that consumers carrying items with RFID tags move about in a shopping mall, and unauthorized people or agents secretly install
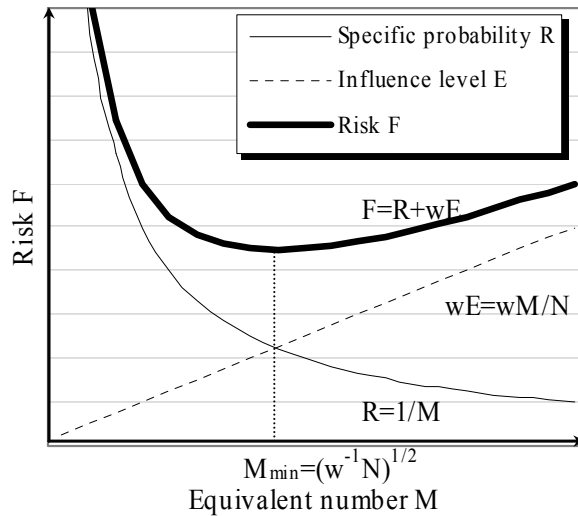
Fig. 4. Balance of both specific probability *R* and the influence level *E*

interrogators and trail consumers by reading the RFID tags. We measure the traceable distance for some equivalent number *M*, and find the equivalent number M_{min} at which the traceable distance becomes the shortest in the case of a shopping mall.

a.   Modelling the shopping mall

We assume four models about the shape of a shopping mall as shown in Table 1 and Fig. 5. The floor space of all models is 40,000 m². There is an entrance in the centre of each neighbourhood of the first floor of the shopping mall. In each model, the shopping mall contains 100 stores. Each store's floor space is 225 m² and one interrogator is installed in each store. The width of all passages in each model is 10 m. Each shopping mall always contains 2,000 consumers. A PASS KEY value of an RFID is recorded along with the position and the time when a consumer comes within the readable range of an interrogator, which is 2 m. Model 1 is a 200 x 200 m square within which consumers can move freely because there are no walls dividing stores. Model 2 is a 200 x 200 m square within which consumers move through passages because there are walls separating the stores. Model 3 is a frame type building, around a central courtyard, with a 1,160 m outside perimeter and an 840 m inside perimeter; there is a single passage with stores on both sides. Model 4 is a building with four 50 x 50 m floors where consumers move between floors using a central escalator or one of four elevators.

Model #	Space	Floors	Walls	Entrances	Interrogators	Visitors
1	40,000 m²	1	No	4 sides of 1F	100	2,000
2	40,000 m²	1	Set	4 sides of 1F	100	2,000
3	40,000 m²	1	Set	4 sides of 1F	100	2,000
4	40,000 m²	4	Set	4 sides of 1F	100	2,000

Table 1. Model parameters
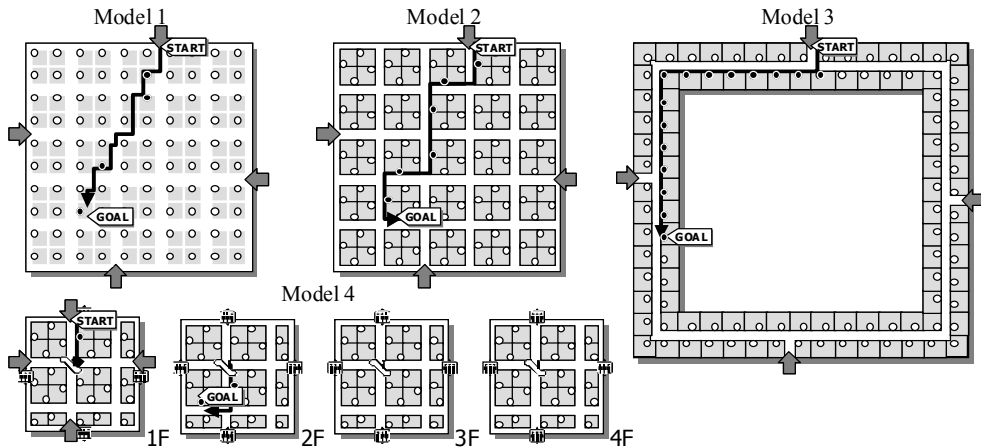
Fig. 5. Types of shopping mall

The consumer movement pattern in this simulation is as follows:

- Each consumer's starting point is randomly chosen from among four entrances.
- The stores to which each consumer goes are chosen at random.
- The number of stores to which each consumer goes varies randomly from 3 to 7.
- A consumer begins by moving to the nearest selected store from the chosen starting point.
- If a consumer arrives at a store, he will stay once and then will move to the nearest selected store from there.
- If a consumer arrives at the last selected store, he will then return to the starting point.
- The time a consumer spends at a store varies randomly from 10 minutes to 30 minutes.
- The distance which a consumer moves in each step is 5 m.
- The speed at which a consumer moves is 1 m/s.

b. Trail analyzing system

This system collects and analyzes log data on the detection of RFID tags with the installed interrogators for consumer trail analysis. The log data consists of an interrogator's ID, the installation position of the interrogator (x, y), a step number, and a PASS KEY value of an RFID. This system creates a consumer's trail by extracting arbitrary PASS KEY values in connection with the consumer out of log data, and sorting these data by time. In this system, there may be some RFID tags with the same PASS KEY values. To trail a consumer as fully as possible, the system disregards data detected at any point at which a consumer cannot physically arrive.

5.2 Result of the trail analyzing simulation

Figure 6 shows a simulation result for the case of five consumers who possess RFID tags with the same PASS KEY value in model 1. This figure shows the route consumer An actually followed and the route for the same consumer observed by the trail analysis system. The routes of the other consumers are also shown. Each white circle indicates an interrogator. In this case, consumer A started from point (110, 10). After moving 135 m, he encountered consumer C at point (90, 130). Therefore, the traceable distance was 135 m since

it became impossible for the trail analyzing system to distinguish consumer A and consumer B after their routes met.
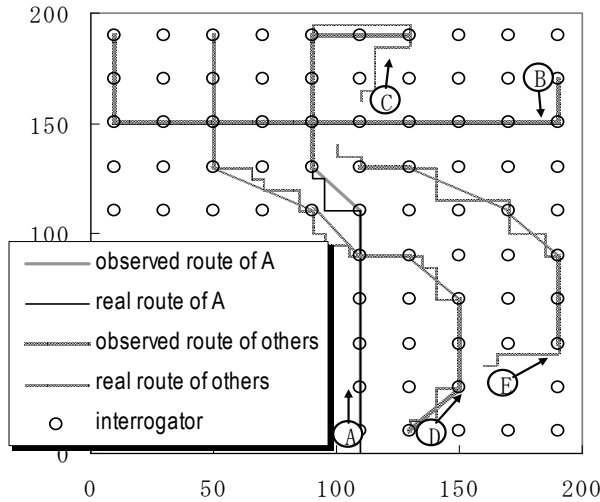
Fig. 6. Flow line analysis simulation result

Figure 7 shows histograms of the traceable distance L acquired through 10,000 simulations when the equivalent number M of PASS KEY was 1, 5, 10 or 20 and the shopping mall type was Model 1. The respective standard deviation was 148, 104, 55, and 27. This figure shows the traceable distance L becomes short if the equivalent number M increases.

Figure 8 shows the average of the traceable distance L as a function of the equivalent number M in each of the four models. When the equivalent number M was 1, the traceable distance L was 817 m; when the equivalent number M was 70, the traceable distance L was 0.9 m. In this simulation there were many consumers possessing RFID tags with the same PASS KEY value, so we know there was a high probability that consumers possessing RFID tags with the same PASS KEY value would meet and these consumers would consequently be hard to trail.

Next, we consider the effect of RFID password disclosure E in this simulation. The influence rate wE when an RFID password is leaked is expressed as follows from equation (2). The probability w of an RFID password being decoded by brute force attack in one year and subsequently leaked is set to 50%. The number N of the RFID tags in the shopping mall is set to 2,000.

$$wE = \frac{0.5}{2000} M \qquad (5)$$

The risk F obtained from this simulation result and equation (5) is shown in Fig. 8. (The right vertical axis in the figure shows the rate of risk F). This figure shows that an equivalent number M of about 45 leads to the smallest risk F. When the equivalent number M is 45, the influence level of RFID password disclosure E is about 2% and the traceable distance L is about 3.5 m although the distance which a consumer walked in a shopping mall is 817 m.
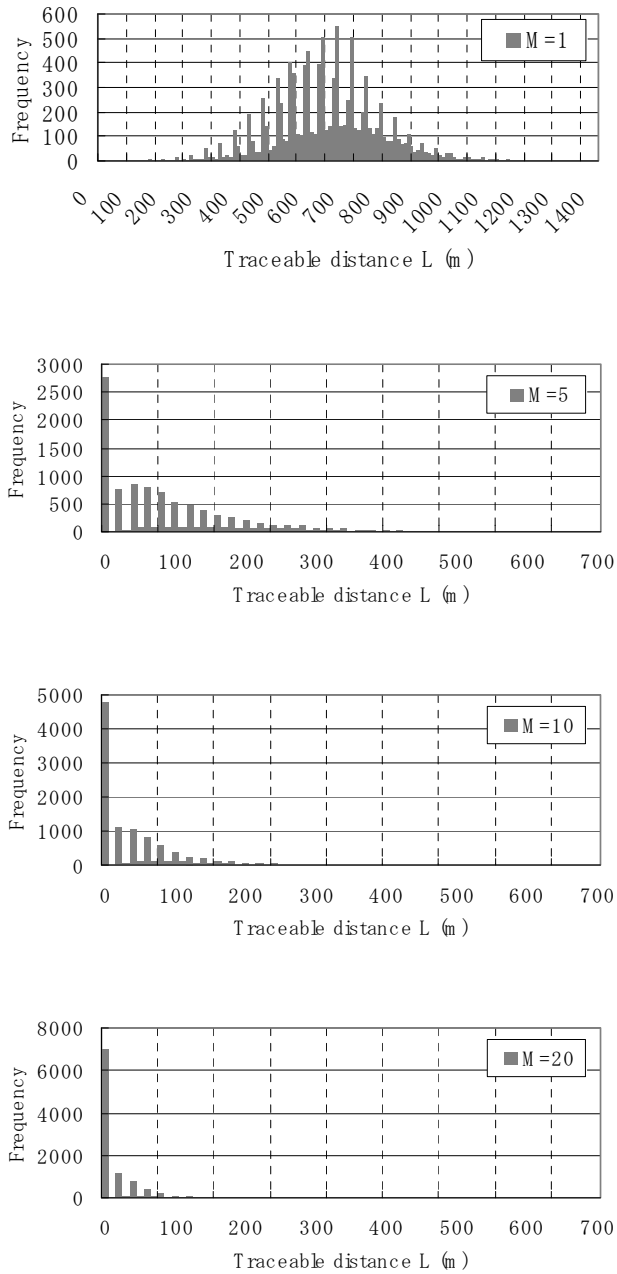
Fig. 7. Traceable distance *L* in case *M* = 1, 5, 10 and 20
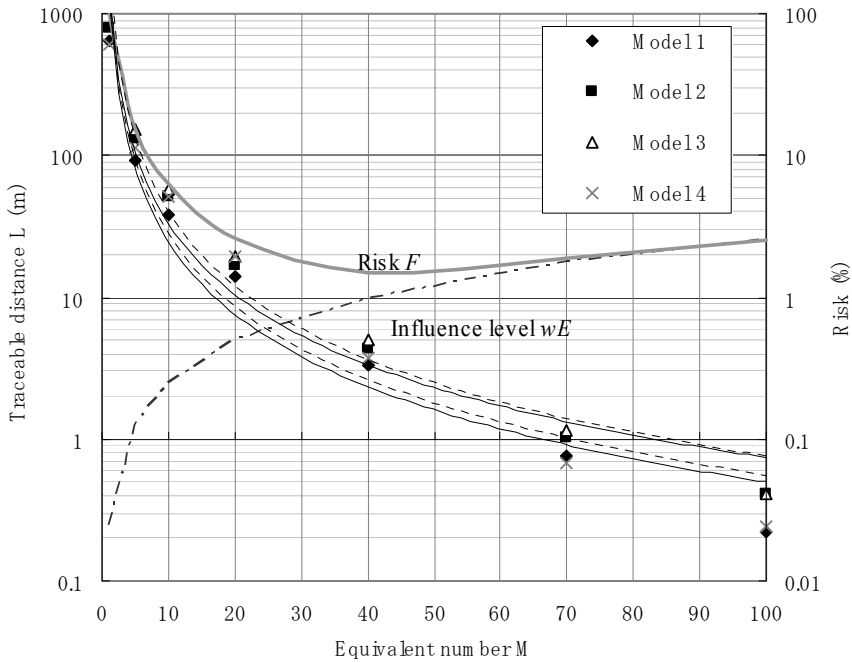
Fig. 8. Traceable distance *L* vs. the equivalent number *M*

6. Conclusion

RFID privacy problems will have to be solved before items with RFID tags can be safely provided to consumers on a large scale. Here, we considered the location privacy problem of unauthorized persons or agents being able to trail a person by tracing a unique ID recorded in an attached RFID tag.

We proposed a method for using RFID tags that include an interrogator with an algorithm to generate RFID passwords. This method groups RFID passwords for RFID tags in a way that protects consumer privacy.

We simulated the possibility of trailing a consumer in a shopping mall. We investigated how much the traceability of a consumer changed when the proposed method was applied. Simulation results showed that the traceability fell by about 0.4% when the influence level of RFID password leakage was 2% in this model.

In practice, it may be difficult to read a consumer's RFID tag from distances like those assumed in this simulation because RFID is easily influenced by various environmental conditions. However, even if invasion of privacy is technically difficult, consumers will remain concerned as long as there is any possibility of invasion of privacy through RFID. Therefore, our proposed method will be useful for RFID system application.

7. Acknowledgment

8. References

CASPIAN; ACLU; EFF & EPIC (2003). "Position Statement on the Use of RFID on Consumer Products," http://www.privacyrights.org/ar/RFIDposition.htm.

Albrecht, K. & Mcintyre, L. (2005). "*Spychips: How Government And Major Corporations Are Tracking Your Every Move*," Thomas Nelson Inc., 1595550208, Tennessee, USA.

GS1 EPCgloval. (2005). "Guidelines on EPC for Consumer Products," http://www.epcglobalinc.org/public/ppsc_guide.

Weis, S. (2003). "Security and Privacy in Radio-Frequency Identification Devices," Masters Thesis, Massachusetts Institute of Technology, Massachusetts, USA.

Juels, A. & Pappu, R. (2003). "Squealing Euros: Privacy-Protection in RFID-Enabled Banknotes," *Proceedings of Financial Cryptography '03*, pp.103-121, Guadeloupe, France.

Engberg, S.J.; Harning, M.B. & Jensen, C.D. (2004) "Zero-Knowledge Device Authentication: Privacy and Security Enhanced RFID Preserving Business Value and Consumer Convenience," *Proceedings of the Second Annual Conference on Privacy, Security and Trust (PST'04)*, pp.89-101, New Brunswick, Canada.

Satoh, A. & Inoue, T. (2007). "ASIC-Hardware-Focused Comparison for Hash Functions MD5, RIPEMD-160, and SHS," *the VLSI journal*, Vol.40, pp.3-10, 0167-9260.

Honzawa, A. (2008). "Secure RFID Project, Spread Use for Product Cycle Management," *Proceedings of GRIFS Workshop*, Halifax, UK.

A Mobile RFID Authentication Scheme Based on the COMP-128 Algorithm

Jia-Ning Luo[1] and Ming Hour Yang[2]
[1]Information and Telecommunication, Ming Chuan University
[2]Information Computer Science, Chung Yuan Christian University
Taoyuan, Taiwan

1. Introduction

Radio frequency identification (RFID), based on the MIT Auto-ID project [1], is a technology that uses wireless transmission to identify an object. RFID is seeing increased use in various industries as an alternative to the bar code. An RFID system consists of three components: the reader, the tag, and the back-end database. Some advantages of an RFID system are that it does not require direct contact with the tag, and can scan multiple tags simultaneously. However, because the reader uses wireless technology to communicate with the tag and the EPC Class 1 Gen 2 protocol [2] does not have a well-designed access mechanism to protect the tag data privacy and location privacy, a malicious attacker is able to retrieve the tag's information by listening to the traffic between the reader and the tag [3]. To protect the information stored on a tag, Juels [5] and Weis [6] proposed methods for a tag to lock or destroy itself when attacked. However, these methods are an inconvenience to normal users. Many studies [7] propose authentication mechanisms in RFID systems, in which only authorized readers can read the correct information storing on the tag. However, due to hardware limitations, an RFID tag cannot perform complex operations, such as traditional symmetric and asymmetric encryption algorithms.

Previous research proposes using the simple XOR operation to encrypt messages in RFID authentication protocols. Some studies use the RFID tag's built-in CRC function to achieve message authentication [8]. Other studies [4][9][10][11] use the one-way hash function to enhance authentication protocol security. This study briefly explains these authentication mechanisms and analyzes existing security issues.

Karthikeyan [12] proposed a mutual authentication scheme that uses two matrices and the corresponding anti-matrix. In this approach, the multiplication of a vector key and the matrix serves as an authentication index for the tag. However, in Karthikeyan's scheme, the tag does not verify reader's return value; that is, the attacker can re-send the message to track tag's location.

Duc [8] used the built-in CRC function of an RFID tag to generate a message authentication code (MAC) consisting of a random number and a secret previously shared between the tag and the reader. Duc uses the MAC to authenticate the tag and update the pre-shared secret. However, Duc's scheme cannot prevent the forge attack and it does not have forward security. To enhance Karthikeyan and Duc's scheme, Chien [13] proposed a synchronization

authentication protocol based on CRC. However, because CRC is a linear function, no protocols based on CRC can resist the forge attack.

Other studies use a one-way hash function in the RFID authentication mechanism [4][9][10][11][14]. Henrici proposed a *hash based scheme* [9] in which the tag sends h(ID) instead of its unique ID to the reader. Henrici's scheme protects the tag's location privacy because the attacker cannot derive the tag's ID from h(ID).

In Henrici's scheme, if the message between reader and tag is lost, the tag will be out-of-sync. To improve Henrici's scheme, Yang proposed a novel mutual authentication mechanism [10] that uses index-pseudonyms and XOR method. In this case, the tag generates a hash value for a random number sent by the reader. This hash value is used as the tag's pseudonym. In Yang's protocol, an attacker can trace the tag's location because the current authentication message sent from tag to the reader can be derived from the last authentication message.

Ohkubo proposed an authentication scheme that uses the hash chain technique to renew the secret information stored in the tag [4]. The tag's ID is derived from two hash functions, *G* and *H*. However, in Ohkubo's scheme, the database must perform an exhaustive search to find the matching tag ID, which creates a computing burden in the database. Further, Ohkubo's scheme cannot avoid replay attacks.

Chan [3] proposed an authentication scheme that uses the Chameleon Hash algorithm to update the tag's ID and protect the tag's location privacy. In Chen's algorithm, the database uses the authentication information from the previous session to derive the tag's current ID, which means an exhaustive search of the database is not required. Lee [16] proposed an authentication scheme based on a hash function to protect communication between the tag and the reader. In this approach, the tag's ID is updated concurrently in the database and the tag. Lee's scheme is resistant to replay attacks and man-in-the-middle attacks, and provides location privacy.

Other studies discuss how to embed the RFID reader into a mobile phone, which then serves as a mobile RFID reader [18][19]. In the mobile RFID environment, any user that holds a mobile RFID reader can retrieve any tag's information. As a result, RFID security problems become even more serious in the Mobile RFID environment [20].

In the Mobile RFID environment, a mobile RFID reader is able to move freely and read any tags nearby. The database must determine the reader's identity before providing it with tag information. Therefore, authentication schemes must be modified to accommodate this feature. For example, in Lee's and Chan's schemes, the reader forwards the authentication message between the database and the tag, and the database always trusts the reader. In the Mobile RFID environment, however, the reader cannot be trusted, and the communication channel between the reader and the database is not secure [3][16].

This paper proposes an authentication mechanism based on the COMP-128 algorithm [21][22], called *COMP-128 in Mobile RFID Authentication Protocol* (C-MRAP), for use in Mobile RFID environments. C-MRAP uses the A3 algorithm in COMP-128 to encrypt messages, and uses the A8 algorithm in COMP-128 to update the authentication key and session key between the database and the tag. In C-MRAP, the database, the mobile reader, and the tag authenticate each other, and the transmission messages between them are encrypted to provide robust security.

This paper is organized as follows. The second section discusses related studies. The third section presents the C-MRAP algorithm. The fourth section performs security analysis and performance analysis, while the fifth section draws conclusions.

2. Related works

The previous section briefly discusses some RFID authentication protocols and their security issues. This section describes the Mobile RFID architecture, the authentication protocols used in Chan [3] and Lee [16], and the COMP-128 algorithm used in the current GSM architecture.

2.1 Mobile RFID architecture

Figure 1 illustrates the typical Mobile RFID environment, in which each user can read the product information of RFID tags through a combination of mobile phone and RFID reader devices. For example, a consumer using a mobile phone's RFID reader can read the tag on a movie poster, and then link to the RFID database to download movie-related information and release dates, and reserve tickets online.

In Figure 1, the communication between the authentication server (AS) and back-end database is secure. But the channel between the tag and the mobile reader, and the channel between the mobile reader and the database are insecure.

The operations of a Mobile RFID system are as follows:

1.   The mobile reader sends a request to the tag. The tag generates a message containing the authentication message, and sends it to the reader. The reader then forwards the message to the authentication server to validate the tag's identity.
2.   If the tag is valid, the authentication server sends the key updated messages through the reader to the tag.
3.   The tag replies with a successful update message through the reader to the authentication server.
4.   The authentication server sends the tag's information to the reader as soon as it receives the acknowledgement message from the reader.
5.   The reader connects to the back-end database through the AS to get extra services, e.g., booking a ticket.
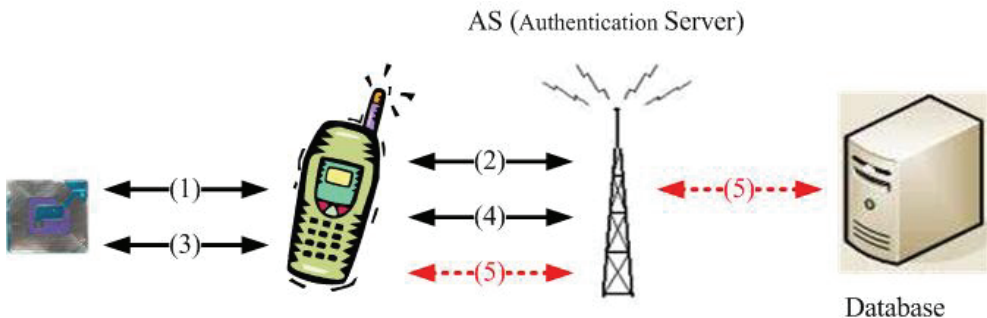
Fig. 1. The Mobile RFID architecture

2.2 Chan's protocol

Chan [3] proposed an RFID authentication protocol based on the Chameleon hash algorithm [26]. A chameleon hash function is associated with a pair of public and private keys. A user R generates a key pair, a public key HK_R and a private key CK_R, according to a given

generation function. The chameleon hash functon, denoted $CH_R(m_1,r_1)$, can be computed easily by using R's public key HK_R, where m_1 and r_1 are two strings. The chameleon hash function has two important properties: collision resistant and trapdoor collisions. For two messages m_1 and m_2, where $m_1 \neq m_2$, it's hard to find a collision that $CH_R(m_1,r_1) = CH_R(m_2,r_2)$ by using R's public key HK_R (the collision resistant property). However, it is easily to find a collision that $CH_R(m_1,r_1) = CH_R(m_2,r_2)$ by using R's private key CK_R (the trapdoor collisions property).

Table 1 shows the terminology of Chan's protocol. The database and every tags shares five variables: a unique serial number CID, a transaction counter TID, the last transaction counter LST, and two random numbers SN_1, and SN_2. The TID increases in each transaction, and the LST will be set to the current TID if the authentication procedure is done successfully.

CID	Tag's identification
TID	The transaction counter of a tag
LST	The previous TID that authenticated successfully
SN_1, SN_2	Random numbers
REF	A pointer stored i-1th authentication data

Table 1. Terminology of Chan's protocol

Figure 2 shows Chan's protocol. When a reader sends a read request to a tag, the tag generates three random numbers, r_1, r_2, and r_3, and sends them to the reader (step 1). The reader forwards them to the database (step 2). The database uses the trapdoor property of Chameleon hash to calculate r_4 that satisfy $CH_R(r_1,r_2) = CH_R(r_3,r_4)$. Database sends r_4 to the tag (step 3). The tag checks if $CH_R(r_1,r_2) = CH_R(r_3,r_4)$. The tag then performs the following operations:

1. Increases TID_i by 1.
2. Calculates $\Delta TID = TID_i - LST_{i-1}$
3. Generates three chameleon hash values: $K_i = CH_R(r_1,r_2)$, $HID_{i-1} = CH_R(CID_{i-1}, SN_2)$, and $CH_R(CID_{i-1}, TID_{i-1})$.
4. Uses A5/1 algorithm [21] to encrypts the two variables ($HID_{i-1}||\Delta$ TID) and $CH_R(CID_{i-1}, TID_{i-1})$ by the key K_i to construct $M_1 = E_{Ki}((HID_{i-1}||\Delta$ TID)$|| CH_R(CID_{i-1}, TID_{i-1}))$.
5. Sends M_1 to the database (step 4).

After the database receives M_1, the database uses K_i to decrypt the message and gets ($HID_{i-1}||\Delta$ TID) and $CH_R(CID_{i-1}, TID_{i-1})$. Because the database does not know tag's identity, it searches HID by calculating $CH_R(CID, SN_2)$ for all tags. If there is a match, the database performs the following operations:

1. Updates $TID_i = HID_{i-1}||\Delta$ TID
2. Verifies $CH_R(CID_{i-1}, TID_{i-1})$
3. Calculates $M_2 = CH_R(TID_{i-1}, CID_{i-1})$.
4. Sends M_2 to the tag (step 5).

When the tags receives M_2, it verifies whether $M_2 = CH_R(TID, CID)$. Finally, both the database and the tag update CID_i and LST_i.

In a transaction of Chan's protocol, a tag should do six Chameleon hash operations and one $A5$ encryption. The database should do $2n+5$ Chameleon hash operations, one $A5$ decryption, and a collision finding of Chameleon hash.
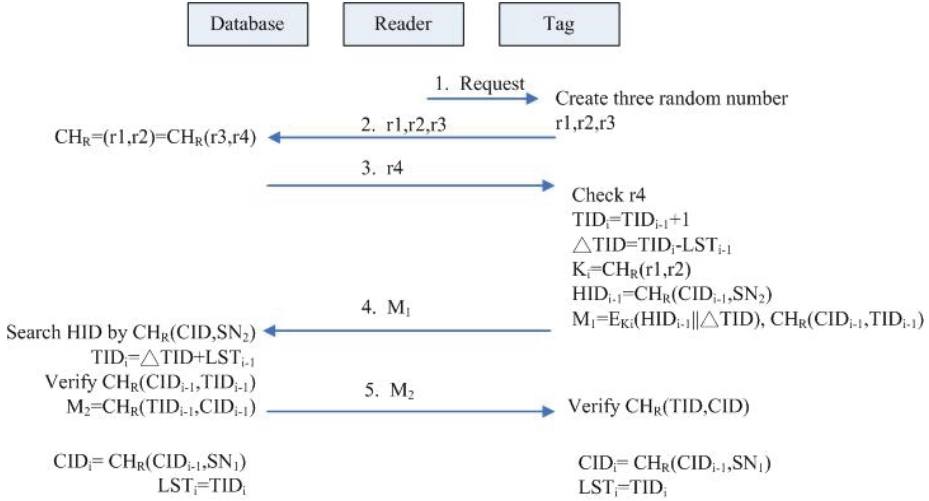
Fig. 2. Chan's Protocol

2.3 Lee's protocol

Lee proposed another RFID authentication protocol by using one-way hash function [16]. In Lee's protocol, the database and every tags shares four variables: a unique serial number CID, a transaction counter TID, the last transaction counter LST, and a random number SN. The TID increases in each transaction, and the LST will be set to the current TID if the authentication procedure is done successfully.

Figure 3 shows Lee's protocol. When a reader sends a read request to a tag, the tag performs the following operations:

1. Generates a random number N.
2. Increases TID by 1.
3. Calculates $\Delta TID = TID_i - LST_{i-1}$.
4. Calculates the hash value of CID_{i-1}, where $HID_{i-1} = H(CID_{i-1})$.
5. Calculates another three hash values: $H(SN \oplus HID_{i-1} \oplus N)$, $H(SN \oplus N)$, and $H(CID_{i-1} \oplus TID_{i-1})$.
6. Constructs $M_1 = N || H(SN \oplus HID_{i-1} \oplus N) || \Delta TID \oplus H(SN \oplus N) || H(CID_{i-1} \oplus TID_{i-1})$, and sends M_1 to the database through the reader (step 2).

The database performs the following operations:

1. Searches SN by $H(SN \oplus HID \oplus N)$
2. Checks if the condition $LST + \Delta TID > TID_{i-1}$ holds
3. Updates $TID_i = LST + \Delta TID$
4. Verifies the tag's identity by checking $H(CID_{i-1} \oplus TID_{i-1})$
5. Generates a random number R and updates HID, CID, TID and LST in the database if the tag is valid.
6. Constructs $M2 = R \oplus H(SN \oplus (N+1)) || H(R \oplus CID_{i-1} \oplus TID_{i-1})$, and sends M_2 to the tag (step 3).

The tag then verifies $H(R \oplus CID_{i-1} \oplus TID_{i-1})$ by using R. If the value is correct, the tag updates CID_i and LST_i: $CID_i = H(R \oplus CID_{i-1})$ and $LST_i = TID$.
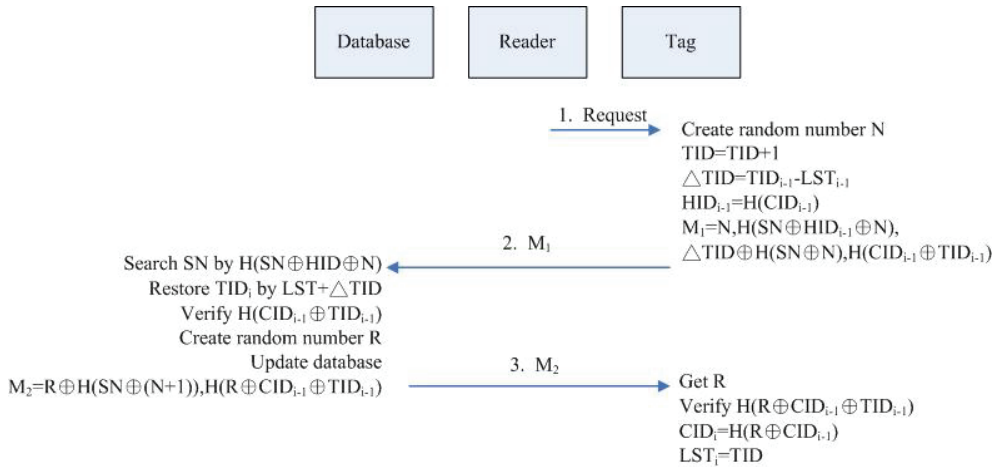
Fig. 3. Lee's protocol

2.4 COMP-128 algorithm

The GSM authentication architecture uses the A3 algorithm of COMP-128 for authentication, the A8 algorithm for generating session keys, and the A5 algorithm for encryption. Table 2 shows the components used by the COMP-128 algorithm in the GSM network.

MS (Mobile station)	The mobile phone
SIM(Subscriber Identity Module)	The smartcard put into the mobile phone, to store the session key and perform simple operations
AuC (Authenticaton center)	The *AuC* authenticates each SIM card
BS(Base station)	The station communicates with the mobile phone
K_i	The key used for authenticatoin

Table 2. COMP-128 Terminology

In the GSM network, each mobile station shares a key K_i with the authentication center. A malicious attacker cannot get the K_i by sniffing all the packets in the air. Figure 4 shows the operation flow of the COMP-128 algorithms (A3, A5, and A8).

When the AuC wants to authenticate a SIM card in a mobile station, it generates a 128-bit random number (RAND) and delivers it to the MS through the BS. The MS then forwards the random number to the SIM card module. The SIM module computes *SRES = A3(K_i, RAND)*. The SIM module forwards SRES to the AuC to authenticate itself. If the SRES is correct, both the AuC and SIM module generate a session key *K_c = A8(K_i, RAND)*, which is used to encrypt all the messages between the MS and the BS.

3. COMP-128 in Mobile RFID Authentication Protocol (C-MRAP)

To improve Lee and Chan's schemes, this paper proposes a mutual authentication scheme, called the COMP-128 in Mobile RFID Authentication Protocol (C-MRAP), for the Mobile
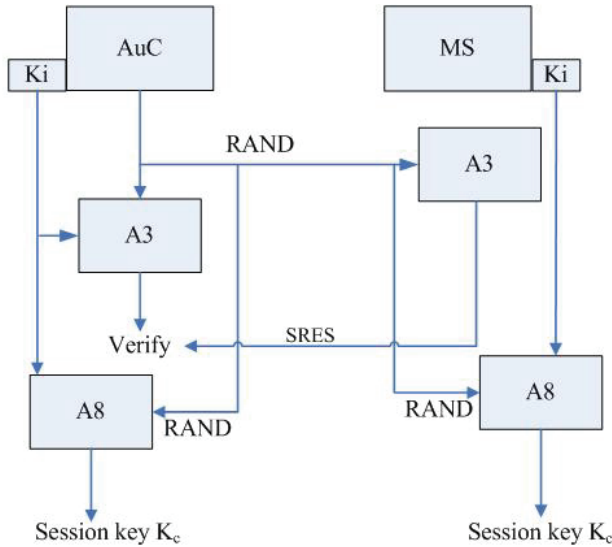
Fig. 4. COMP-128 Algorithms

RFID environment. There are three phases in the C-MRAP protocol. In the first phase, the database authenticates the mobile reader and the tag. The reader queries the tag and then sends a read request to the database by forwarding the tag's identity message. The database uses the session key shared with the reader to authenticate the reader's identity. The database then uses the information sent from the tag to verify the tag's identity. In the second phase, the database updates the authentication key with the tag after the database successfully authenticates the tag. The third phase is used to confirm the key update. The tag sends an update confirmation message to the database, and the database then sends the tag's information to the reader. Table 3 shows the information stored in the database, the reader, and the tag. In this approach, the tag shares four secrets with the database: SN, Kc_i, UN, and PIN. These variables are used to authenticate the tag and to perform key update. Table 4 lists the terminology used in C-MRAP scheme.

Shared information between the database and the tag	
SN	The unique serial number of the tag.
PIN	The access password of the tag.
Kc_i	The key used to authenticate the tag in the ith round.
UN	A parameter used in the key update process
Shared information between the database and the reader	
RID	The unique serial number of the reader.
The extra information stored in the database	
Kc_{i-1}	The key used in the i-1 round.
Nr, Nt	Random numbers generated by the reader and the tag in the previous authentication message. They are used to foil replay attacks.
$DATA_x$	The detailed information of a tag_x

Table 3. The variables stored in the database, the reader, and the tag

$r_1\, r_2$	The random numbers generated by the reader.
r_3	The random number generated by the database.
N	The random number generated by the tag.
Kc_i	The tag's authentication key used in the ith round
$Auth$	The tag's authentication information, which is derived from the A8 algorithm. The database uses this variable to search for the tag in its memory.
M_1	The message generated by the tag.
M_2	The message generated by the database.
m1 ∣∣ m2	The message combines m1 and m2.
$A_3(m_1,m_2)$	Encrypt m_1 and m_2 using the A3 algorithm
$A_8(m_1,m_2)$	Encrypt m_1 and m_2 using the A8 algorithm
$f(.)$	The pseudo random number generator
$H()$	A one-way hash function
$Cert_{RID}$	Reader's certificate

Table 4. C-MRAP terminology

3.1 The C-MRAP protocol

Figure 5 depicts the C-MRAP protocol, which includes three phases. The following section describes each message in detail.
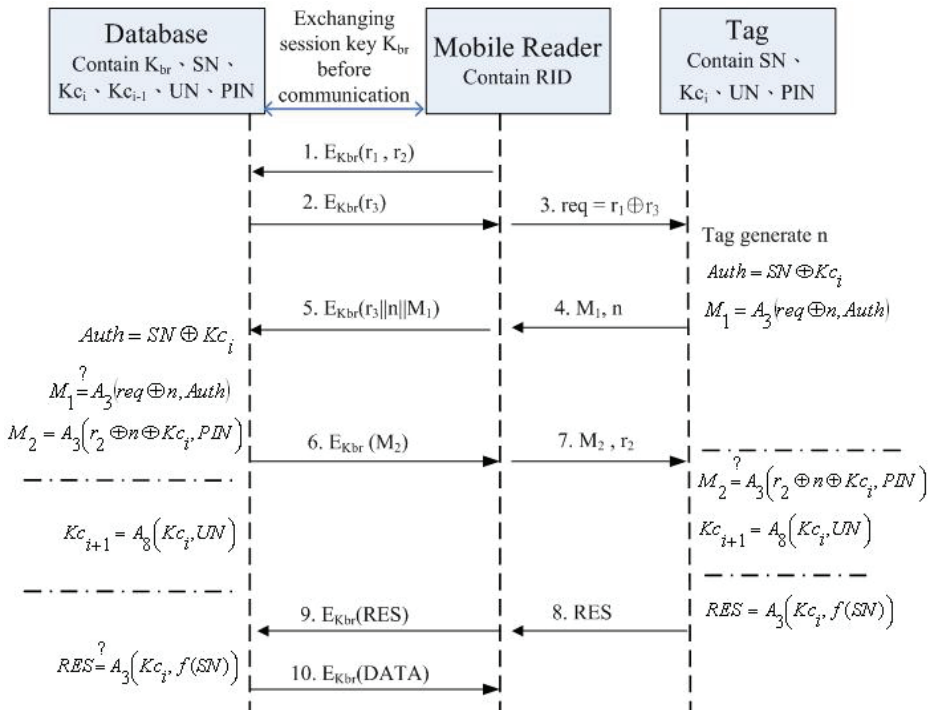
Fig. 5. The C-MRAP protocol

Phase 1: Tag authentication

In the first phase, the reader and the database exchange their own certificates and establish a shared session key K_{br}. When the reader sends a read request to the tag, the tag sends the authenticated messages to the reader. The reader then forwards the message and two random numbers shared with the database to the database. The database searches its records to verify if the tag is valid.

1. When a reader sends a read request to a tag, the reader first generates two random numbers r_1 and r_2, and encrypts them using the session key K_{br} shared by the reader and the database. The reader then sends the encrypted values to the database.
2. When the database receives the request, it generates another random number r_3, encrypts it with K_{br}, and sends the encrypted value back to the reader.
3. The reader calculates $req=r_1\oplus r_3$, and sends req to the tag.
4. When the tag receives req, the tag generates a random number n, and calculates two variables: $Auth = SN\oplus Kc_i$ and $M_1=A_3(req\oplus n, Auth)$ The tag then forwards M_1 and n to the reader.
5. The reader combines r_3, n, and M_1, encrypts it with the session key K_{br}, and sends the encrypted message to the database.
6. The database decrypts the message using the session key K_{br}. The database perform an exhaustive search of all the tags by calculating $M_1'=A_3(r\oplus n , SN\oplus Kc_i)$. If there is a matched M_1, the database uses the A3 algorithm to calculate $M_2=A_3(r_2\oplus Kc_i , PIN)$, encrypts M_2 with K_{br}, and sends it to the reader.
   Furthermore, the database calculates $Kc_{i+1}=A_8(Kc_i , UN)$, and backs up the Kc_i to Kc_{i-1}, and Kc_{i+1} to the Kc_i, as Figure 6 shows. If the database cannot find a matching tag, the database searches its records by calculating $Auth'=A_8(SN , Kc_{i-1})$ and $M_1'=A_3(r\oplus n , Auth')$. If a match is found, the database and the tag are out of sync. At this time, the database checks req and n with the random variables Nr and Nt. If the variables are not the same, the database updates the tag's key because it is not a replayed message.

Phase 2: Synchronized Key Update

The reader decrypts M_2, and sends M_2 and r_2 to the tag.

The tag computes $M_2'=A_3(r_2\oplus Kc_i , PIN)$, and compares it with M_2. If they are equal, the authentication process is complete. The tag generates its new key by calculating $Kc_{i+1}=A_8(Kc_i , UN)$.
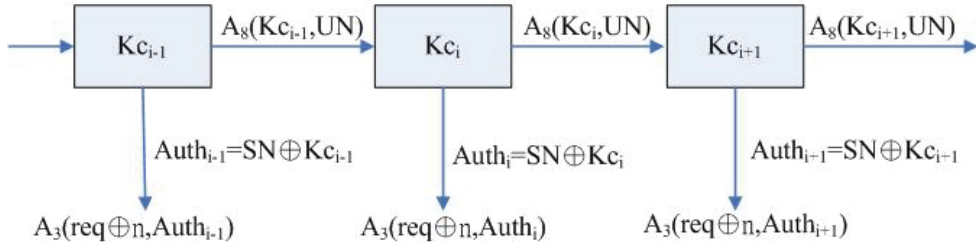
Fig. 6. Key Update

Phase 3: Key Update confirm

The tag calculates $RES = A_3(Kc_i , f(SN))$ and sends it back to the reader.

The reader encrypts RES using the session key K_{br}, and sends the encrypted message to the database.

The database compares *RES* with $A_3(Kc_i, f(SN))$. If the value is correct, the database sends the tag's information to the reader.

Using secrets shared between the database, the reader, and the tag, the proposed protocol updates the tag's authentication key during each session to protect the tag's privacy in a mobile RFID environment. Because Kc_i is not transmitted on the air, the protocol is secure and the reader can rapidly obtain a tag's information from the database.

4. Security analysis and performance evaluation

This section analyzes all the transmitted messages in the proposed protocol, and explains why this protocol is resistant to security attacks and can continue its operations without falling out of sync. Possible attacks include packet sniffing attacks, replay attacks, the man-in-the-middle attacks, and message dropping attacks. This section also compares the proposed protocol with other methods.

Section 4.2 implement three algorithms, including the Chameleon hash, COMP-128, and SHA1 algorithms, and evaluates the performance of Chan's, Lee's, and the proposed protocols. Results show that our protocol decreases the computation time of a tag and the database.

4.1 Security analysis

Message sniffing attacks

Assume a malicious attacker collects message 3 (*req*), message 4 (M_1, *n*), message 7 (M_2, r_2), or message 8 (*RES*) which are sent between the reader and the tag, and attempts to perform a guessing attack to retrieve tag information. The attacker cannot succeed in this attempt because he cannot guess the *Auth* value after obtaining *req* and *n* in message 3 and 4 because $Auth = SN \oplus Kc_i$, and the *SN* and Kc_i are only known by the database and the tag. The attacker must perform a brute force attack to guess these two values. Because Kc_i is updated in every session, it is hard to guess both *SN* and Kc_i at the same time. In addition, the attacker cannot retrieve messages transfered between the database and the reader because these messages are encrypted by the session key K_{br}.

Replay attacks

Using several random numbers, an attacker can attempt to replay message 3 (*req*) and message 7 (M_2, r_2). However, this is not possible because the messages are different in each session. For example, an attacker cannot replay message 5 ($E_{Kbr}(r_3 \mid\mid n \mid\mid M_1)$) because the database will verify it with the previous *req'* and *n'*.

Message dropping attacks

Next, consider the situation if the authentication message between the reader and the tag is lost during the transmission. In the proposed protocol, if message 3, message 4, or message 7 is lost, the reader waits for a timeout period and performs another reading request.

Man-in-the-middle attacks

If an attacker plays a role between the tag and the reader, and attempts to modify the value of *req* or *n*, the authentication process will fail because the *req* value is generated from the original reader, and not by an attacker.

If an attacker collects message 3 and message 4, and attempts to generate a new message 5 and send it to the database, this attack will fail because the attacker does not know r_1 and r_3.

If an attacker attempts to modify message 7 (M_2 , r_2), or message 8 (RES), the attack will fail because the attacker does not know the value of PIN and Kc_i.

Data privacy

The previous analysis indicates that an attacker cannot retrieve any valid information from data transmissions between the reader and the tag. In this protocol, only the variable n is not encrypted. Furthermore, all the transmission messages between the database and the reader are protected by the session key E_{kbr}.

Location privacy

An attacker can trace a tag's location if he can send the tag a specified value, and the tag returns a predicted value to the attacker. This type of attack will fail because the value of message 4 (n and M_1) changes every time. If an attacker wants to trace the tag by re-sending message 7, he will fail because the Kc_i is different.

Forward security

The proposed protocol satisfies the forward security because the COMP-128 algorithms it uses are one-way functions. Thus, an attacker cannot derive the previous messages using current messages.

Table 5 compares our protocol with other RFID security protocols.

	Anonymity	Location Privacy	Resisted to Replay attack	Resisted to man-in-the-middle attack	Forward security	Mobile RFID
Karthikeyan [12]	X	X	X	X	X	X
Duc [8]	O	O	X	X	X	X
Chien [13]	O	O	O	X	O	X
Henrici [9]	X	X	X	X	X	X
Yang [10]	X	X	O	O	X	X
Ohkubo [4]	O	O	X	X	O	X
Chan [3]	O	O	O	X	O	X
Lee [16]	O	O	O	X	O	X
Our scheme	O	O	O	O	O	O

Table 5. The Security Analysis

According to Table 5, Karthikeyan and Henrici's protocols cannot protect the location privacy, and are not resistant to replay attacks or middleman attacks. Chien's protocol cannot resist replay attacks because it uses the CRC function. Yang's protocol is resistant to replay attacks and man-in-the-middle attacks but it cannot protect the location privacy [15]. Chen and Lee's protocols are not suitable for mobile RFID environments because they trust all readers. Our protocol performs mutual authentication between the tag, the reader and the database, and is therefore suitable for use in mobile RFID environments.

4.2 Performance evaluation

In the Ohkubo protocol [4], the database must perform an exhaustive search to retrieve tag information. If there are n tags, the database complexity is $O(mn)$ after m operations. The

database complexity of Lee, Chan, and our protocol are the same, which is $O(n)$. However, Chan's scheme executes many Chameleon hash operations in the database and the tag, which decreasing overall performance.

Table 6 and Table 7 compare the operations of the three protocols. These tables assumes that the database is operated on a P4-2GHz personal computer, and the reader is a PDA equipped with a StrongARM SA-110 32-bit 233MHz CPU. We also assume that the CPU inside the tag is a 8-bit 12MHz processor. Table 6 lists all the operations required by the three protocols. In Chan and Lee's protocols, the reader only forwards messages between the tag and the database. We assume the packets transmitted between the reader and the database are encrypted by AES algorithms. Table 7 lists the average processing times for the tag and the reader to perform a single transaction in various approaches.

Table 8 lists the average execution times that it takes the database to search for a tag and perform key updates. Table 7 shows that the proposed protocol has better performance than Chan's scheme. Lee's scheme offers better performance than our protocol, but in Lee's scheme, the reader is trusted, rendering this scheme unsuitable for a mobile RFID environment. In the mobile RFID environment, the identity of a mobile reader must be authenticated to ensure protocol security. Finally, the proposed protocol provides better protection than Lee or Chan's protocols.

Protocols	Database operations	Reader operations	Tag operations
Chan	$2n*CH_R$ search + $5*CH_R$ + $1*$collision + $2*$AES encrypt + $3*$AES decrypt	$2*$AES encrypt + $2*$AES decrypt	$6*CH_R$
Lee	$2n*$SHA1 search + $3*$SHA1 + $1*$AES encrypt + $1*$AES decrypt	$1*$AES encrypt + $1*$AES decrypt	$7*$SHA1
Our scheme	$2n*$COMP-128 search + $4*$COMP-128+ $3*$AES encrypt + $3*$AES decrypt	$3*$AES encrypt + $3*$AES decrypt	$4*$COMP-128

Table 6. The operations required by the three protocols

Protocol	Tag execution time	Reader execution time
Chan	0.0034	0.000945
Lee	0.0001	0.00047
Our scheme	0.0004	0.00141

Table 7. A comparison of execution times
(Unit: second)

Protocols	100 tags	1000 tags	10000 tags	100000 tags
Chan	0.0300	0.2368	2.1127	24.4873
Lee	0.0008	0.0064	0.0552	0.6451
Our scheme	0.0053	0.0420	0.3725	4.4791

Table 8. The average database execution times for various schemes
(Unit: second)

5. Conclusion

Mobile RFID technology offers more advantages than traditional RFID. However, because mobile RFID technology uses wireless communication, a secure authentication protocol is required to protect user privacy.

The proposed protocol is resistant to forge tag attacks, man-in-the-middleman attacks, packet sniffing attacks, replay attacks, packet dropping attacks, and out-of-sync attacks. In addition, the shared private key stored in the tag and the database is updated after each successful transaction. Compared to other protocols, this method provides a more secure protocol that enables all users to use a more secure Mobile RFID environment.

6. References

[1] MIT Auto-ID, retrieved Sep. 10, 2009 from World Wide Web http://autoidlabs.mit.edu.

[2] EPCGlobal, Class 1 Generation 2 UHF Air Interface Protocol Standard, retrieved Sep. 10, 2009 from World Wide Web http://www.epcglobalinc.org/standards/uhfc1g2.

[3] M. Chan, "Protect Mobile RFID Location Privacy Using Dynamic Identity," in *Proceedings of the National Computer Symposium*, Taiwan, 2007.

[4] M. Ohkubo, K. Suzuki, and S. Kinoshita, "Cryptographic approach to privacy-friendly tags," in *Proceedings of the RFID Privacy Workshop*, 2003, pp. 624-654.

[5] A. Juels, R. L. Rivest, and M. Szydlo, "The blocker tag: selective blocking of RFID tags for consumer privacy," in *Proceedings of the 10th ACM conference on Computer and communications security*, 2003, pp. 103-111.

[6] S. A. Weis, S. E. Sarma, R. L. Rivest, and D. W. Engels, "Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems," in *Proceedings of the Security in Pervasive Computing*, 2003, pp. 201–212.

[7] M. Lehtonen, T. Staake, F. Michahelles, and E. Fleisch, "From identification to authentication — a review of RFID product authentication techniques," in *Printed handout of Workshop on RFID Security — RFIDSec*, vol. 2006, 2006.

[8] D. N. Duc, J. Park, H. Lee, and K. Kim, "Enhancing Security of EPCglobal Gen-2 RFID Tag against Traceability and Cloning," in *Proceedings of the 2006 Symposium on Cryptography and Information Security*, 2006.

[9] D. Henrici and P. Muller, "Hash-based enhancement of location privacy for radio-frequency identification devices using varying identifiers," in *Proceedings of the Second IEEE Annual Conference on Pervasive Computing and Communications Workshops*, 2004, pp. 149-153.

[10] J. Yang, J. Park, H. Lee, K. Ren, and K. Kim, "*Mutual authentication protocol for low-cost RFID,*" in *Proceedings of the Ecrypt Workshop on RFID and Lightweight Crypto*, 2005, pp. 17-24.

[11] I. J. Kim, E. Y. Choi, and D. H. Lee, "Secure Mobile RFID system against privacy and security problems," in *Proceedings of the Third International Workshop on Security, Privacy and Trust in Pervasive and Ubiquitous Computing (SECPerU 2007)*, 2007, pp. 67-72.

[12] S. Karthikeyan and M. Nesterenko, "RFID security without extensive cryptography," in *Proceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks*, 2005, pp. 63-67.

[13] H. Y. Chien and J.H. Chen, "A secure authentication mechanism suitable for EPC Class 1 Generation 2 RFID standard," in *Proceedings of the 16th Information Security Conference (ISC2006)*, 2006, Taiwan, pp. 206-213.

[14] C.-L. Lin and K. C. Chang, "Security Analysis of the EPC Class 1 Generation 2 RFID authentication protocol," in *Proceedings of the 17th Information Security Conference (ISC2007)*, 2007, Taiwan, pp. 600-606.

[15] G. Avoine, "Cryptography in Radio Frequency Identification and Fair Exchange Protocols," *PhD Thesis of Swiss Federal Institute of Technology (EPFL)*, Lausanne Switzerland, 2005.

[16] L.-a. Lee and S. Shieh, "Protecting User Privacy with Dynamic Identity-Based Scheme for Low-cost Passive RFID Tags," in *Proceedings of the CISC 2008*, Taiwan, 2008, pp. 206-218.

[17] S. Dominikus, E. Oswald, and M. Feldhofer, "Symmetric authentication for RFID systems in practice," in *Proceedings of the ECRYPT Workshop on RFID and Lightweight Crypto*, Graz, Austria, July, 2005, pp. 14-15.

[18] N. Park, H. Kim, K. Chung, and S. Sohn, "Design of an Extended Architecture for Secure Low-Cost 900MHz UHF Mobile RFID Systems," in *Proceedings of the IEEE 10th International Symposium on Consumer Electronics (ISCE'06)*, 2006, pp. 1-6.

[19] Nokia Co., "Nokia Unveils RFID Phone Reader," *RFID Journal*, retrieved Sep.10, 2009, from World Wide Web http://www.rfidjournal.com/article/articleview/834/1/1/.

[20] K. Rhee, J. Kwak, S. Kim, and D. Won, "Challenge-Response Based RFID Authentication Protocol for Distributed Database Environment," in *Proceedings of the Second International Conference on Security in Pervasive Computing (SPC 2005)*, Boppard, Germany, 2005, pp. 70-84.

[21] ETSI/GSM, Recommendation GSM 11.11, version 3.16.0, 1994.

[22] ETSI/TC and SMG, Recommendation GSM 03.20. Security Related Network Function, Version 3.3.2, 1991.

[23] L. Gong, R. Needham, and R. Yahalom, "Reasoning about belief in cryptographic protocols," in *Proceedings of the IEEE Symposium on Research in Security and Privacy*, 1990, pp. 234-248.

[24] R. Housley, W. Ford, W. Polk, and D. Solo, "Internet X. 509 Public Key Infrastructure Certificate and CRL Profile," *IETF RFC 2459*, January 1999.

[25] H. Lee and J. Kim, "Privacy threats and issues in mobile RFID," in *Proceedings of the First International Conference on Availability, Reliability and Security (ARES'06)*, 2006, pp. 510-514.

[26] H. Krawczyk and T. Rabin, "Chameleon signatures," in *Proceedings of Network & Distributed System Security Conference (NDSS 2000)*, 2000, pp. 143-154.

RFID System Integration and Application Examples

Ming-Shen Jian

Dept. of Computer Science and Information Engineering, National Formosa University
Taiwan, R. O. C.

1. Introduction

RFID today is the popular wireless induction system. Each RFID tag in RFID system is given a unique ID (UID). The RFID tag with memory also records the on demand information. When an independent RFID tag approaches the RFID antenna, the induction between tag and antenna happens. The information and content recorded in the tag is transmitted to the RFID antenna and translated into the computational data. Following up the data translation, the tag recognition can be completed and related applications are provided.

Due to the popularity of RFID, many applications based on the local or small area were proposed. According to the short-distance wireless signal, the RFID tag users can be monitored within the specific area. In other words, the RFID systems are generally used to be the hardware identification in many applications. Most of these applications are based on the indoor environments or be a tiny area service and independent of the existed system.

Some of the RFID systems were proposed to be used in hospital or health care (Munoz et at., 2003). Each patient is given and equipped the designed RFID tag. In addition, each patient should always wear every time and everywhere. Therefore, all the patients' current location and conditions are monitored by the hospital. Some entrance guard systems are also based on RFID system. The RFID ticket or RFID card [5-7, 12] (Pala & Inanc, 2007) is used to identify that a user is legal or not.

In addition, since the RFID tag can be used as the identification, it means that the applications which adopt software encryption as the identifications to protect the intellectual property of the applications or files can also use the RFID tag. Some researches presented that the embedding RFID can be plugged into a small device such as handheld host [1]. The handheld device users can plug in the SD or CF interface of RFID reader card. Hence, the users can scan and induct the RFID tag everywhere. Since the RFID systems are popular and ripe for distinguishing treatment of individual target [8,9], the unique characteristic or identification of RFID can be the solution of intellectual property protection. Many researches proposed the possible way to protect the intellectual property, products, or applications. In some applications [10], the RFID chips are embedded in the cap of bottle. The medicine or other objects can be differentiated between fake and true (Jian et at., 2009).

However, there are many RFID related products. To manage the RFID information from different RFID products and the communication with different applications will be the important issue.

The remainder of this paper is organized as follows. In Section 2, the RFID system is presented. The concepts of RFID system integration are shown in Section 3. Some integration examples of RFID applications are introduced in Section 4. At last, the conclusion is given in Section 5.

2. RFID system

Generally speaking, the RFID System consists of
- At least one RFID antenna for RFID reader,
- An RFID reader,
- RFID tags.

The RFID tag is composed of two essential elements: designed antenna and an RFID chip. Some RFID tags also equip memory. According to the requirement, the RFID tag can be designed as different contours or shapes such as: card, wrist belt, button, ornament, 3D toy, tattoo, etc. Each of these RFID tags records a unique identification (UID) and finite information. The antenna of the RFID tag is designed and used to absorb the electromagnetic wave for the power supply of the RFID tag and communicate with the RFID reader. In addition, according to the size and design of the antenna, the induction distance between RFID tag and RFID reader will be limited. Based on the power of the RFID tag, three basic types of RFID tag are proposed:
- Passive RFID Tag
- Active RFID Tag
- Semi-Active RFID Tag

The Passive RFID tag is triggered when a user with the RFID tag approaches the antenna of RFID reader. Then, the information recorded in the RFID tag is transmitted through the antenna to the RFID reader. The RFID reader will parse the signal into the digital and computing content. At last, the gained content from RFID tag can be further utilized. Typical applications of passive RFID tag are tickets and guard cards.

An Active RFID Tag indicates that the tag owns a battery and can actively broadcast the information about this tag even there is no RFID reader which inducts this tag. Since there is a battery in the tag, more functions such as temperature sensing, pressure sensing, humidity sensing, etc., are embedded. The information gained from the embedded functions is transmitted actively. When the RFID reader approaches the active RFID tag, the reader can obtain the information. Typical applications of passive RFID tag are wireless sensors.

A Semi-Active RFID Tag seems an RFID tag with an on-off switch. In general, the semi-active RFID tag also equips a battery and some embedded functions. For the most part, this RFID tag works as a passive RFID tag. When an RFID reader approaches and inducts the tag, this tag is triggered. After triggered by the reader, this tag turns on the battery and executes the functions. Then, the information from the functions can be translated to the RFID reader. At last, the RFID tag turns off the battery for power saving.

In addition to three basic types of RFID tag, the frequency of RFID system used can be classified as LF (low frequency, 125~134KHz), HF (high frequency, 13.56 MHz), and UHF (ultra high frequency, 915MHz). The characteristics of these RFID systems are different. In addition to the operation frequency, the communication protocol standard may be different. Most RFID tags communicate based on the standard of ISO-14443A or ISO-15693. Some RFID tags are even designed as dual frequency tags.
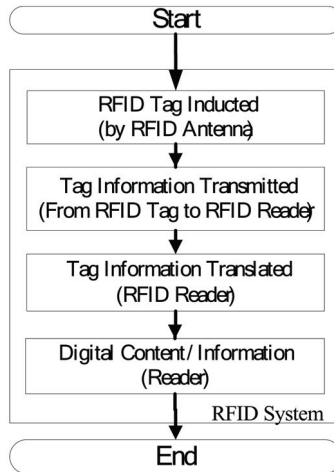
Fig. 1. Procedure of RFID System.

In addition, there are different antenna sizes of these RFID systems. Due to the power and size of RFID antenna, the induction distance between antenna and tag changes. Generally speaking, most RFID applications adopt the suitable frequency according to the required induction distance of the application.

	Low Frequency	High Frequency	Ultra High Frequency
Induction Distance	<2 Feet	<3 Feet	<10~30 Feet
Normal Application	Keyless entry	Smart Card	Electronic Toll Collection
Data Rate	Low ←-------------------------------→High		
Tag Size	Large←-----------------------------→Small		
Performance Near Metal / Liquids	Better←-----------------------------→Worse		

Table 1. The characteristics of different RFID systems

RFID reader is the basic element of the RFID system. All induction and parsing are made by the RFID reader. An RFID reader is composed of at least one antenna and a microprocessor. The RFID reader uses the antenna to send the radio frequency wave for inducting and communicating with the RFID tag. The antenna also receives the radio frequency wave from the RFID tag. The size and contour of the antenna affects the distance of communication range and accuracy.

Although the RFID reader owns a microprocessor, most applications are based on the integration of several systems which the RFID reader may not manage independently. Therefore, most RFID readers provide some I/O port for integration or communication with other systems. Some RFID readers provide the RS-232 serial port as the I/O (especially output) port for other hardware or system. Some RFID readers with more powerful processor supply the TCP/IP protocol or Internet access (RJ45). Some readers only give the USB connection for end applications or hardware.

According to the procedure of the RFID utilization, the RFID applications can be defined and divided into three types: 1) emphasis on standard objects with fixed RFID utilization procedure, 2) emphasis on defined and specific area with defined RFID utilization procedure, and 3) emphasis on third party applications or services based on RFID induction.

3. Integration

Since the RFID reader may not manage independently, to integrate with other systems or embedded in an existed applications becomes an important issue. First, the application designer has to know that the integration of the application is based on the software, hardware, or both. If the application is a new system, the RFID system can be embedded in initially. However, if the RFID system is integrated with the existed system, to define and decide the interface for integration is important. In this section, the integration mentioned is based on the existed systems or applications though the new applications also applicable.

According to the communication interface of the RFID reader, hardware and software communication is available. Even the microprocessor of the RFID reader is not powerful, general logic computing based on electric circuit can be implemented. By controlling the voltage of the circuit, the primary circuit can implement the On/Off action or signal. After receiving the signal from the circuit combined with the RFID reader, mechanical action can be realized such as door locking or opening.

In addition to the simple On/Off signal, further information may be required for the applications. Corresponding to the RFID reader selected, simple circuit, RS-232, USB, or RJ45 Internet access can be used.

3.1 Simple circuit for RFID system integration

Most hardware for simple mechanical control or action is based on the designed circuit. According to the requirement or action of the machine, some mechanical actions are triggered when receiving an On/Off signal. The reader of the RFID system equips the control circuit such as the MOSFET of simple IC control circuit. Sometimes the under-controlled applications or systems only need a trigger signal. In other words, the reader of the RFID system provides only an electric wire for signal transmission.

In this type of integration, the RFID system acts as a signal sender. When the reader of RFID system inducts the RFID tags, the reader determines that the inducted RFID tag is the pre-defined (Ex: legal, valid, permitted, etc.) tag or not. If the inducted RFID tag is the pre-defined RFID tag, the RFID reader sends the control signal to trigger the hardware or mechanical action such as unfasten the lock of door, open a lock gate, etc. In other words, the RFID system is the active controller of the integrated system. The integrated system will act based on the decision of the RFID system.

3.2 RS-232 for RFID system integration

RS-232 serial port is the general communication interface. Most appliances or computers support the communication based on RS-232 (D-sub). The RS-232 (EIA232) consists of DTE device (Data Terminal Equipment, usually a computer or terminal) and DCE device (Data Circuit-terminating Equipment, usually a terminal or receiver such as a modem). By sending the control signal, two devices can connect each other vial RS-232 connection. In addition, according to the standard of the RS-232 communication, the reader of RFID system can 1)

send the pre-defined command via RS-232 to drive the machine or systems, or 2) send the emulated signal as the command to drive the systems.

In this type of integration, to implement the RS-232 interface of the RFID reader, the RFID system has to equip at least one of the two functions: a simple electric wire for simple action of driven systems or a simple computing unit (or IC chip) for serial port control and command ordering.

Sometimes, the connection between RFID system and the controlled machine will add the middleware (or hardware). The command from the RFID system via RS-232 connection can be translated to the digital signal.

3.3 USB and internet access for RFID system integration

For most integration with the existed applications or systems, a host PC (Computer) is the main platform for all information management. Due to the computing ability and the easy maintenance, many applications provide service and control other systems based on PCs. In addition, most applications today consist of different software, applications and database. To integrate the RFID system with the existed applications or systems, a main platform for dealing with all requirements and messages are needed. According to the hardware of the computer, the RFID reader can connect to the PC via USB port or RJ45 Internet connection.

When the RFID reader connects to the PC via the USB connection, the information from the RFID tag can be transmitted to the PC directly. Since the computing ability and processing performance are better than the RFID reader, the applications which gain the information from the RFID reader can enhance the functions or capabilities of the services. The control signal, function executing, or further information management can be done by the applications.

If the RFID system communicates with the integrated systems via Internet, the RFID reader has at least the network component and sufficient centre processing unit for information computing. The RFID system works as a network device belongs to the platform. In other words, the RFID system works independently. The Internet access is only for data and information transmission.

No matter communication based on USB port or network connection, the RFID system is just the role of information gathering. The main platform which manages all information, defines the corresponding actions, and gaining service from the third party applications, is independent from the RFID system. In this case, the RFID system is selected for replacing some identification procedure of the existed systems.

4. Example of RFID system integration

The characteristic of the RFID system is to identify the RFID tag and exchange the information with the RFID tag. If an application needs no identification, to integrate the RFID system becomes useless. Therefore, to recognize whether an application or a system needs for RFID system integration or not is the first important thing. Then, considering the object served by the applications, to select the suitable RFID system is an important issue. The object can be the human, animals or goods. Most objects follow pre-defined action functions or fixed procedures when served by applications. Only the procedure which is used to identify and differentiate the objects can be replaced by the RFID system. Therefore, based on different frequency of RFID system, different size of RFID tags, and different way

for integrations, there are different integrated systems and applications. In this section, some integrated systems are introduced.

4.1 Guard system

In opposition to creating new execution or service environment, there were many existed systems or applications such as guard system or application deployed. Since these existed systems or applications run for a long time and present the stability themselves, to include the original systems or applications can reduce the time for stability testing and cost of new infrastructure establishment.

In this section, a realistic application for parking guarding (Jian et at. (a), 2008) is presented. Via using the proposed system, the main contributions are:

1. the efficiency of management can be improved,
2. the is modular and can be embedded in other similar parking system and hardware without additional re-modification,
3. the procedure of passing the Inlet & Outlet can be simplified via using RFID,
4. the costs of the real construction for the proposed system can be decreased and estimated.

The RFID System, original gate hardware, and other business management system colored blue in the framework are independent.
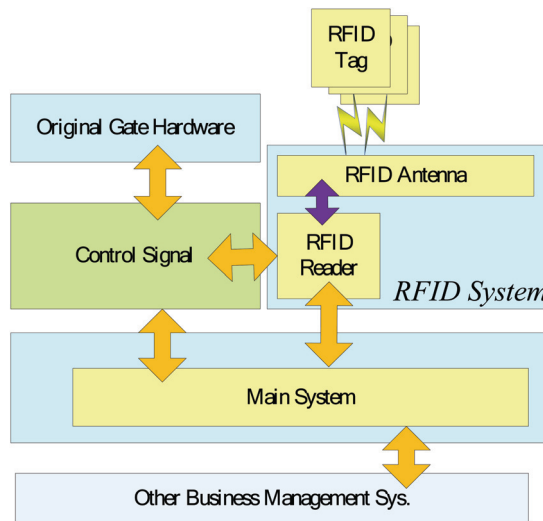
Fig. 2. The framework of modular RFID embedded parking gurad system.

These independent systems are the already existed systems. Each existed systems can independently and individually work. For example, the lane gate management can be controlled by the manual operation or parking ticket machine without RFID. It means that these independent sub-systems can be substituted. The gate hardware can be the product of any possible company. There are also many RFID hardware providers. Moreover, to suitably manage and monitor the parking place, the manager may need the attendance information of different users according to each business application. Hence, different type hardware or products need the general interface to communicate with the main

management system. In this example, the Main System provides the middleware software and hardware for the interaction.

In the presented system, the RFID antennas and reader are deployed at the gate. In addition, the RFID tags are placed in the car. Considering the practicability, the RFID System should overcome the accuracy affection of weather and sunshade-paster of car, and the RFID tag type. To increase the usability of the proposed system, the UHF type of RFID tag in this paper is selected. When a user's car approaches the gate, the induction and communication between RFID tag inside the car and antenna of RFID System is automatically established. Then the reader of RFID System translates the signal information to the digital content.

If there is no further action or information required, the RFID system can send a signal to the gate directly. In other words, even without the Main System, the RFID system can communicate and control the gate (Ex. Via wire, simple circuit integration) directly.

If the information from the RFID tag is required by other systems or applications such as database, the information will be sent to the Main System first. In this case, the Main System communicates with the hardware of gate via RS-232 link (RS-232 for RFID Integration). The ADAM digital I/O module as the middleware to construct the computing_commands / voltage_signal module is selected. ADAM-4520 is the RS-232/RS-485 converter module that communicates with host PC via RS-232 link. The digital computing command from the host PC is converted into the RS-485 type data stream. Then, the converted data is inputted to the module ADAM-4050. The output DATA+ of ADAM-4520 is connected to the DATA+ of ADAM-4050 and also is the DATA-. In addition to hardware, a software program is executed. This program is designed corresponding to ADAM. The program sends the commands from host PC to the ADAM via RS-232. Then, to command the gate hardware, the voltage_signals are sent from the data output, DO0, DO1, DO4, and DO5 of ADAM-4050 to the gate hardware.

To really replace/join the original control hardware, four states of the lane gate should be known first: 1. Inlet gate open, 2. Inlet gate close, 3. Outlet gate open, and 4. Outlet gate close. Hence, to match the control requests of these four states, four individual voltage-controlled IO hardware such as: 1) InletGate_open, 2) OutletGate_open, 3) Expansion_1, and 4) Expansion_2 are defined. The InletGate_open is used to transmit a voltage signal to open the inlet gate. The OutletGate_open is used to transmit a voltage signal to open the outlet gate. Considering the real gate controller, most gates are closed after counting down an on demand time period. In other words, the control IO for closing the gate can be needless.

To control the original and existed gate hardware, the four individual voltage-controlled IO hardware are linked. If the InletGate_open which connected to the DO0 of the ADAM-4050 is set a signal with the voltage 12V, the inlet fence of the gate is opened. After 6 seconds counting down the inlet fence of the gate closes automatically. The OutletGate_open which connected to the DO4 of the ADAM-4050 controls the outlet fence of the gate and opens it when is set a signal with voltage 12V. In addition, the Expansion_1 and Expansion_2 are connected to the DO1 and DO5 of the ADAM-4050 individually. If the Expansion_1 is set a signal with voltage 12V once, the counter which counts and presents the total number of current available parking space subtract 1. In opposition to Expansion_1, the Expansion_2 is set a signal with voltage 12V once to add 1 from the current total number of available parking space. When a valid car approaches the inlet gate, the Main System sends commands to set the DO0 and DO1 a signal with voltage 12V.

In addition, the communication between the database (other business management system) and Main System is based on Ethernet or Java server socket. The connection between ADAM and Main System on server PC is RS-232.
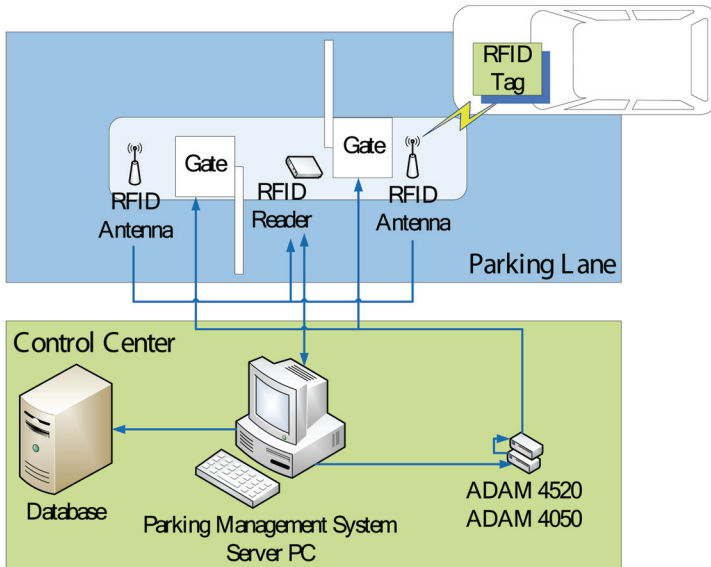
Fig. 3. The real implementation of RFID parking system.

To guarantee the stability and accuracy of RFID tag detection and identification within the finite time, the power of antenna is set as 30 dBm and the power state of antenna and reader are always on. The protocol for RFID antenna to communicate with RFID tag is EPC Global Generation 2. Considering the performance of RFID tag, two types of the RIFD tag with size 4.40"X4.125" that for polyester and that adhesive to glass are used.

The verification shows that the distance from antenna to the RFID tag depends on the type of tag. The material and weather take affection. RFID tag assembled by polyester has the better ability of weather resisting. When test in the rainy day, there is a layer of water and mist. It apparently reduces the transmit distance about 16~33% especially more than 50% when there is a layer of water on the glass with the RFID tags that adhered on glass. In addition, the verification also shows that the distance from antenna to the RFID tag is normally about 4 m of polyester type tag and about 2 m of that adhered on glass. In other words, there are at least 6 m from the fence of the gate to the car since the antenna is located 2 m before the fence of the gate. It means that there will be more than 0.7 seconds (if the mobility of the car is limited and lower than 30 km/hr) for the system to open the fence of lane gate. Therefore, in most cases, the fence of the lane gate can open in time and the car can enter the gate into parking lot smoothly. The RFID tag assembled by polyester can achieve 99.75% identification accuracy. On addition, the RFID that adhered on glass is affected by the material and thickness of sunshade. Under the situation of car window closed, the identification accuracy is only 45% when dark or thick sunshade used. In opposite, the accuracy reaches 85% if only limpid or normal sunshade used.

4.2 Bio-information management system

In opposition to the normal RFID tag, the tag for bio-information gathering which is embedded into the animal or human should be designed safeness. The RFID tag can be used as the growth-record or supply chain stage history. In this case, the RFID system focuses on the information gathering and updating. Hence, to control the hardware directly is not the main function of the RFID system.

However, most RFID Tags with the limited memory cannot provide and record many information. To enhance the limited memory of RFID tag, all the information should be simplified according to the code conversion. Each code may indicate that "What event located at Where (area, location) at When (time, date, etc.)".

For example, the aquiculture or livestock industry (husbandry, breeding) creates the records or history of each livestock (such as pig, cow, etc.) or plant. In the following case, the breeding of pig is the example presented.

In the past, the live stock in the farm is marked by each farmer. The livestock in the farm wears the specifically designed RFID tag. For example, an ear tag is the RFID tag which is stabbed into the pig ear. When the information such as protective inoculation, weight, etc., should be updated, the manager can induct the RFID tag via the handheld RFID system or device.
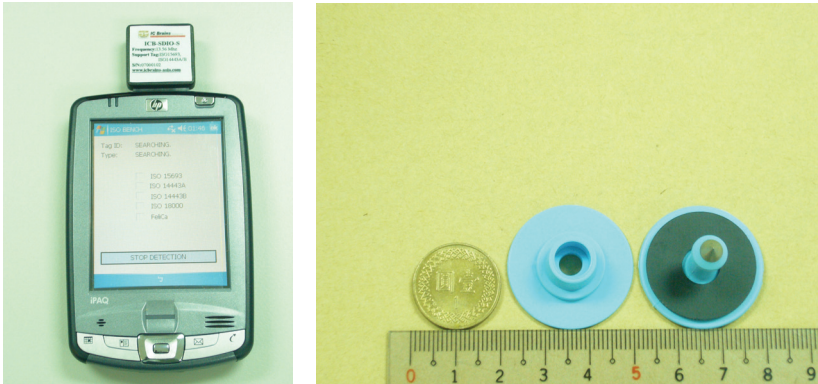
Fig. 4. (a) The RFID system embedded in the handheld device. (b) The ear tag (blue object) for pig.

Similar to the modular RFID embedded parking gurad system, when the RFID systm gains the information from the RFID tag, the RFID reader passess the information to the Main System. The Main System acts as the bridge for the different third party applications. For example, when the gaining the weight of a pig, the RFID system inducts the RFID tag for the identification of this pig. Then, the weight value and the unique ID of the RFID ear tag is written into the third party application such as database. Each unique ID of RFID ear tag relates with the corresponding data recorded in the database. In addition, RFID system also writes the information into the ear tag. Therefore, the supply chain of the livestock can gain the information immediately and trace the possible information such as the infection disease, current situation of the transmission, etc.

4.3 Human interface and services system

Since the RFID system provides the possibility of identification, individual services for each served individual are available. There were many existed systems or applications about

context-aware or location-aware deployed. These applications use the GPS to locate the user's location (Ashbrook, D. & Starner, T., 2002). Then, according the record of GPS, the service application server provides the location related information to the user. Although the GPS hardware can be plugged-in many handheld devices, to enable that every mobile device or user equips the GPS is not practicable. In addition, it also consumes the power of the mobile devices when GPS is used. Furthermore, the users of context-aware or location-aware services exactly need the direction or information they required but not the exactly value of longitude and latitude in the world. Hence, to provide users with the fitting local information and the related direction of the required personal service without too much useless or unnecessary information gained is more important.

In addition to GPS, according to the orientation made by the station of wireless cellular system (Bahl, P. & Padmanabhan, V.N., 2000), the related information according to the user's location can be given to the user via cellular system. Not only supply the public services but also give the personal services, the context aware researches (Han et al., 2008) were also proposed.

Research in (Ciavarella, C. & Paternò, F., 2007) was proposed that considering the user's related location. The services and information of user-location-related public places such as the museum (Tesoriero, R. et al., 2008) are provided. According to the requirement of users, different services are given through wireless network or cellular system to different users even they are in the same places.

However, in (Jian, M.-S. (b) et al., 2008), what kind of the context, the corresponding context services, and the context-aware RFID system are important to be provided for user is still an issue of the existing system. In addition, there is no standard of operation modes of the RFID systems implemented for the context-aware services.

Hence, only the concept of context and location-aware service based on RFID system is introduced in this section. The Middleware Platform is the main system to manage the internal and external system connections. This platform also makes the information connection to other business management system or database via software API and Internet network. In addition, the related information to the RFID tag inducted is presented by user interface.

In opposition to the RFID service based on server PC, some handheld devices also support the embedded RFID system. The RFID tag can be used as the commercial advertisement. Every user can use their handheld devices to induct the RFID tag of the advertisement to gain the information. In addition, if the user requests the further information, the handheld device can obtain the services or information via Internet network connection. The handheld device can also communicate with the PC based server. Therefore, the further services such as database query can be obtained via the server.

For example, people who locate in the different area may require the individual services. The services can be actively provided to the users via local area server. Or, the user can use the mobile handheld devices to actively access the services from local area server or main server.

In this example, the RFID systems are deployed 1) at the specific area or location such as the entrance of the rapid transit system or the information service machine, or 2) within the handheld devices such as PDA or mobile phone. When a user is given an only readable RFID tag, the related information or the user's on demand service conditions about the user is given by himself and on demand recorded in the database.
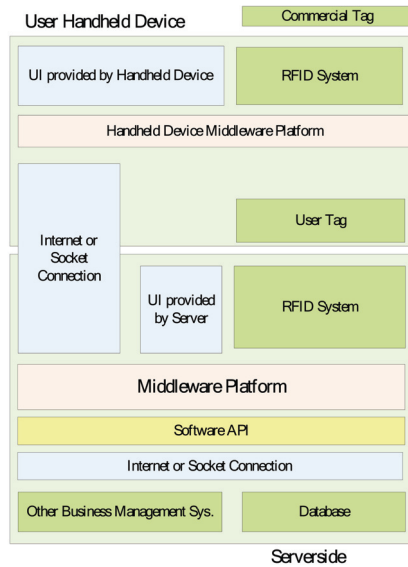
Fig. 5. The framework of service application with RFID system.
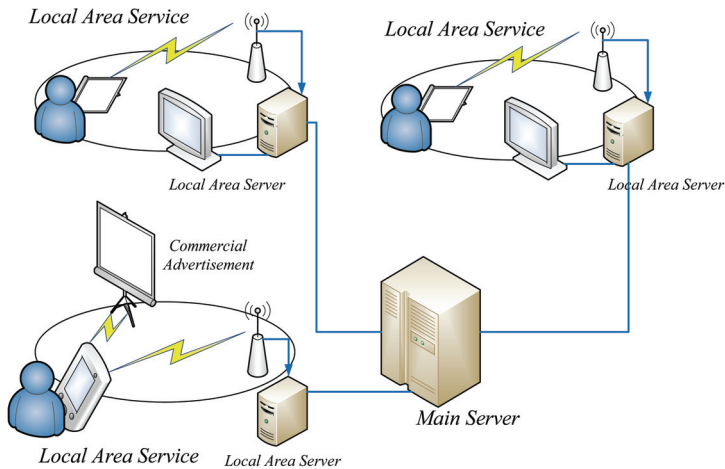
Fig. 6. The concept of service system.

When the user requires the local area public or personal services, the user should be at the tiny induction area such as a local area information center or a service station. Then, the RFID system placed in the specific area inducts the RFID tag and gain the information such as unique ID number from the RFID tag. The reader of RFID system then sends the information to the local area server via Internet.

After receiving the information, the local area server responses the on demand required services corresponding to the specific local area that the on demand required services were

recorded in the database before. At last, the user can gain the location-aware information or services via user interface. In addition, the database can record the history of the user's requirements. The statistic user requirements can be used to classify that what kind of the service the user requests most. Next time the service server can provide the personal services according to the classified results. In other words, the users can be served with the services they most pay attention to. Fig 7 indicates the flowchart of the RFID tag utilization.
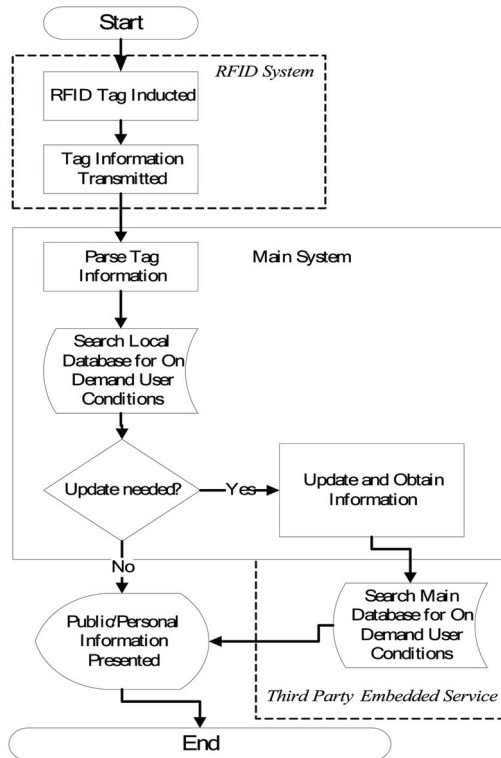
Fig. 7. The flowchart of end user RFID tag utilization in the service application.

Considering the popularity of handheld devices such as PDA and mobile phone, the devices which powered by battery with portable ability can be used as the service devices. There are many handheld devices that capable of plugging in the SD or CF type of appliances. These handheld devices can also access the Internet and communicate with other service applications. In addition, there are RFID systems that sized as a SD card. Hence, a handheld device can be the RFID system.

As the only readable RFID tag is used on the commercial advertisement, an individual and unique ID, and business related information are recorded in each commercial advertisement RFID tag. When the advertisements with the commercial RFID tags are placed in public, an end user device with RFID System user can actively read the commercial RFID tag information of the advertisement interesting in. Then, through the Internet, the requested service or detail of the advertisement according to the read commercial RFID tag information can be obtained.

After obtaining the RFID information of the commercial advertisement, the handheld device can 1) present the requested services according to the information scanned from the RFID tag via on demand defined data format such as XML, or 2) present the requested services according to the database that built in the handheld device, or 3) access the Internet for the further services searching and presentation.

If the requested services can not provided directly by the handheld device (such as that the RFID tag without XML format or no related service recorded in the database of handheld device), the communication between the handheld device and local area server via wireless network is established. Then, the local area server provides the requested location-aware services or business of the related sent RFID tag on the commercial advertisement are presented in the user's mobile device.

7. Conclusion

In this section, several applications and services based on RFID system integration are proposed to integrate the existed service systems, devices, and third party business database. The proposed integration system may need to provide the interface or module that can easily embed different types of RFID systems in. In addition, this section presents the three possible conditions of integration which correspond to the applications. The verification shows that the integration systems are realistic and can provide the different services or applications. The total cost of infrastructure establishment for these services can be also reduced.

8. References

Munoz, M. A.; Rodriguez, M.; Center, J. F.; Martinez-Garcia, A. I. & Gonzalez, V. M. (2003). Context-Aware Mobile Communication in Hospitals. *IEEE Computer*, Vol. 36, No. 9, 2003, pp.38-46, 0018-9340.

Pala, Z. & Inanc, N. (2007). Smart Parking Applications Using RFID Technology. *Proc. of 1st Annual RFID Eurasia*, pp. 1 – 3, 9789750156601, Istanbul, Sept. 2007, IEEE, Istanbul.

Jian, M.-S.; Chou, T. Y. & Hsu, S. H. RFID Encryption/Decryption Technology Aided Multimedia and Data Intellectual Property Protection. *WSEAS Trans. on Communications*, Vol. 8, 7, Jul. 2009, pp. 734-743, 1109-2742.

Jian, M.-S. (a); Yang, K. S. & Lee, C.-L. Modular RFID Parking Management System based on Existed Gate System Integration. *WSEAS Trans. on Systems*, Vol. 7, 6, Jun. 2008, pp.706-716, 1109-2777.

Jian, M.-S. (b); Yang, K. S. & Lee, C.-L. Context and location aware public/personal information service based on RFID system integration. *WSEAS Trans. on Systems*, Vol. 7, 6, Jun. 2008, pp.774-784, 1109-2777.

Bahl, P. & Padmanabhan, V.N. RADAR: An inbuilding RF-based user location and tracking system. *Proc. of Infocom*, pp.775-784, 0-7803-5880-5, Tel Aviv, Mar. 2000, IEEE, Tel Aviv.

Han, L.; Jyri, S. J. Ma, & Yu, K. Research on Context-Aware Mobile Computing, *Proc. of 22nd Inter.Conf. on Adv. Infor. Net.g and App. – Workshops*, pp.24-31, 9781424442331, Okinawa, Mar. 2008, IEEE, Okinawa.

Ashbrook, D. & Starner, T. Learning significant locations and predicting user movement with GPS. *Proc. of Inter. Symposium on Wearable Comp.*, pp.101-108, 0-7695-1816-8, Washington DC, Oct. 2002, IEEE, Washington DC.

Baptista, C.S.; Nunes, C.P.; de Sousa, A.G.; da Silva, E.R.; Leite, F.L. & de Paiva., A.C. On Performance Evaluation of Web GIS Applications. *Proc. of the IEEE 16th Inter. Workshop on Database and Expert Sys. App.*, pp. 497-501, 0-7695-2424-9, Aug. 2005.

Ciavarella, C. & Paternò, F. The design of a handheld, location-aware guide for in-door environments. *Springer Verlag Personal and Ubiquitous Computing*, Vol. 8, Apr. 2004, pp.82-91, 1617-4909.

Tesoriero, R.; Gallud, J. A.; Lozano, M. & Penichet, V. M. R. A Location-aware System using RFID and Mobile Devices for Art Museums. *Proc. of 4th Inter. Conf. on Autonomic and Autonomous Sys.*, pp.76-82, 978-0-7695-3093-2, Gosier, Mar. 2008, Gosier.

RFID System Integration

Hamid Jabbar and Taikyeong Ted. Jeong
Myongji University
Korea

1. Introduction

This chapter explores the systems and their benefits achieved from efficient RFID system integration. RFID is not a product, its a technology that has opened up a wide range of new opportunity in direct and integrated form for different technical fields and areas. Success key in RFID systems is well defined strategy and results in simple maintenance and easy scalability. Requirement for effective RFID system implementation requires specific RFID products, services and solution which resonate with the business requirement and scale.
RFID systems are integrated with Information and Communication technology (ICT) infrastructure and enterprise systems for automated managerial tasks. One of the key application areas for RFID systems is supply chain management, where they are sometime integrated with barcode readers. RFID system is also used for tracking persons, equipment, work orders, tools etc. RFID is doing, and can do variety of things, alone or in combinations of verity of sensors and sometimes these applications and implementation is not obvious.
Difference between the integrated systems being useful or useless expenses is the proper application of these smart integrated systems. While explaining the RFID system integration this chapter will also discuss the methodology, hardware and software requirements for developing an integrated system.

2. RFID integration benefits

RFID offers many features which make it viable for efficient integration in variety of industrial, consumer and commercial concerns. RFID System Integration requires multi disciplinary collaborating among IT professionals, management, system designer etc. Some problems and lacking in traditional barcode or Unified Product Code (UPC) readers is mitigating migration towards more rich in information; RFID and in some case both technologies are combined to achieve added advantages)[R. G. Paul 2007]. RFID tags, also known as Electronics Product Codes ePCs, generate value due to following

- RFID Codes and unique and generic, it associates and uniquely identifies a manufacturer, an object and specific item with a unique serial number.
- RFID doesn't required visual line-of-sight reading, making it to identify pallets in a box.
- It also offers encrypted read/write capabilities with user required data storage.
- Real-time monitoring using intranet/internet offers inventory control, less waste, tighter supply-chain integration.
- RFID offers automated wireless readable identification system

- RFID tags can survive for number of years in harsh environment.
- Several types of RFID tag readers are available such as hand-held's and printers, smart antennas, stationary readers, multi-protocol readers, and others.

3. RFID integration process

For constant flow of information, smooth and efficient processes, value generation using RFID integration with other systems require a comprehensive knowledge and understanding of different systems. Functioning and reliable RFID systems, requires a meticulous knowledge of business, physics and RF system design. To be able to integrate RFID functions within a system and with other technologies such as vision, scan, control and information technologies requires the experience of hardware and technology integration. In applications which requires input of masses such as contact less ticketing, personal verification etc, social and society values and norms also gains important consideration. The contactless data transmission guarantees a high suitability for industrial conditions and large scale implementation.
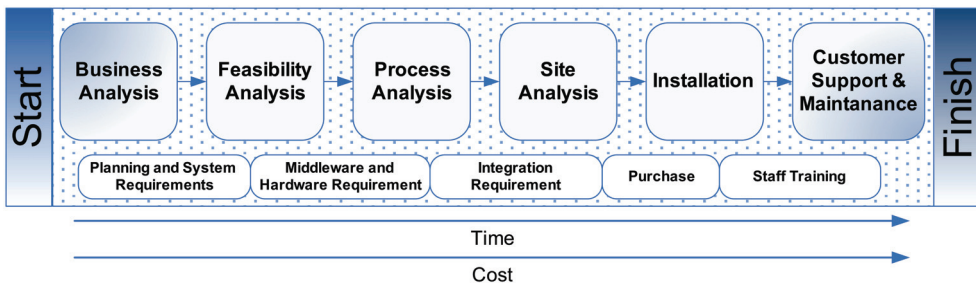
Fig. 1. Process for RFID Implementation and Integration

Each business workflow has its own set of unique requirements and technical hurdles that sets the requirement and customization of RFID system. First, it is important to conduct a business analysis followed by the feasibility analysis of the environment. Usually a conceptual model with thoughtful definitions are set, which help to analyze the process, customer and stakeholders. To conduct the analysis of the sites, small scale test are conducted.

Many companies outsource the implementation to a professional services partner, to reduce possible problems during implementation and their own exposure to risk. To iron out any kinks in the system it is always recommended to accomplish RFID installation in phases, with a test or pilot site. In implementation process every step is checked, re-checked and revisited to improve and tweak the system. In some environments depending on physical proximity the mobile RFID readers are used to enhance or replace stationary models.

One important technical issue in integration process is to diagnose the RF environment for a site, and to install readers and testing tag performance. The types of tag and reader also depend on the type of material which will be identified by tag. In some cases the system requires read/write capability to provide more flexibility to the system. Planning and implementation of reconfigurable, optimized storage, security and authentication are needed so that the reliability of system can be assured.

4. Components for RFID integration

RFID typically compose of reader and tag for the user but mainly it is integrated with other systems to perform the desire tasks. This makes many small hardware or software components, which are considered less thoughtful to gain more importance especially in large scale industrial and commercial applications. This section explains the brief component details which are needed to be considered in RFID system integration.
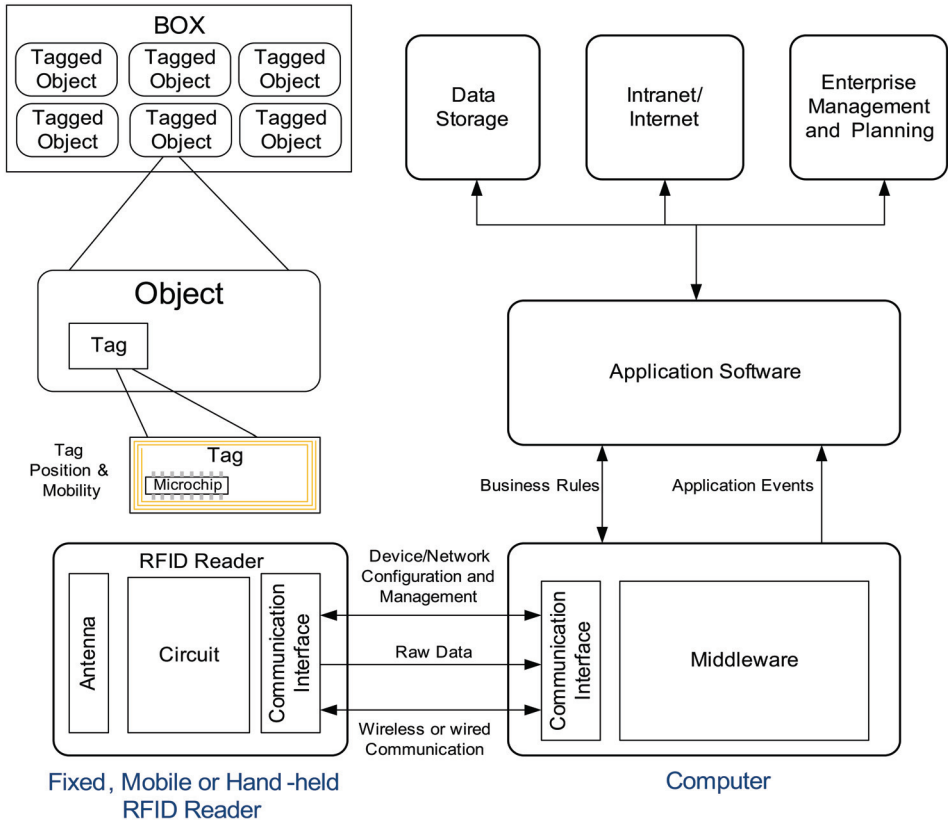
Fig. 2. Main components to consider while RFID and Integration

4.1 RFID tags

Selecting the tags is one the important feature in the integrated systems, as it depends on cost, range, data storage, size, shape, type of material in which tag will be attached. Based on the attachment with identified objects, RFID tags are identified as attachable, implantable, digestible, insertion tags. We also need to decide either to use active or passive tag.

4.2 Tag position and mobility

Two other factors need to be considered for optimal performance while integration is tagging position and mobility. Mobility is important when tag or reader is moving. For

successful identification of tag velocity of movement and change in direction or mobility path also needs to be considered.

Tagging position decides the optimal operation of tag depending on Effective Radiated Power (ERP) which is decisive in case of passive tags. The locations for passive tags depending on ERP are termed as Resonance-Spot, Live-Spot, and Dead-Spot [Adi Tedjasaputra, 2006].

4.3 RFID reader

To decision for RFID reader depends on feature the eneprise, compnay or customer is looking for. Choice is vey broad from simple to intelligent readers, some have self monitoring or integrated software. The size, shape, packaging, power supply are other features which can narrow down the selection for design, cutomization or purchase of RFID reader. Three genral type of readers are hand-held, mobile nd fixed readers.

4.4 Reader antenna

The selction for antenna mainly depends on weather the business workflow requires integrated or external antenna. Many application requires the antenna customization to increase speed, accuracy, effectiveness of RFID data capture process. For customization consideration are environmental operating factors, standard compliant, resonnat frequency, transponder size, antenna size, the capabilities of the RFID reader module, transponder support, read distance, communication with reader, and its business requirements.

4.5 Communication module

The communication between the reader and server or computer dpends on type of connectivity required by the customer, it can be wired communication or wireless. Different protocols and stanadards are available which depends on type of communication: wireless/wired, range, easiness of installation, cost, connector type, connectivity with exsisting systems, future updates, security etc. Application requirements and RFID constarints are studioed indetail by [Folerkemeier & Lampe, 2005]. Table-1 list the type of communication used in differnt RFID systems with some specifications.

4.6 Middleware

The middleware captures the raw data from tag, filters it, and aggregates it; to be processed by the software application and it resides in communication server or ordinary computer. In other word middleware is the software translation layer between the RFID reader and enterprise system. The exact definition of middleware is not agreed upon and in many cases it is difficult to separate the middleware from the application software due to the fact that filtering of RFID data can also be performed on the reader before transmitting it to the enterprise network.

The choice of middleware varies from simple data transceiver to intelligence capable which can provide data processing, decision making capabilities. Middleware implements and integrates with application software using standards such as JMS, MSMQ, SMTP, SOAP, UDP, TCP, etc.RFID middleware functions can be broke down as below:

- **Reader Interface**: Middleware implements drivers to receive and/or transmit data from the readers. This also requires the support for plug and play devices.

Standard	Range (m)	Data Rate	Remarks
RS-232	15	20kbps	5 or 9 wire serial communication, discontinuing in new Computers
RS-485	1200	35Mbps up to 10m, 100kbps at 1200m	Two-wire, half-duplex, multipoint, differential serial communication
USB	5	12 or 480Mbps	Most widely used computer peripheral connection method
Parallel (LPT)	6	2Mbytes/s	Decreasing use
Ethernet	100 to 2000	10/100/1000Mbps	Widely used, large range
Zigbee	Between 10 and 75	20, 40, 250 kbps/channel	For wireless application requiring a low data rate, long battery life, secure networking
UWB	10	100-500Mbps	Target wireless sensor data collection, precison locating and tracking information
WiFi	32 to 95	11 and 54Mbps	Wireless technology supported by computers, mobile phone etc.
Bluetooth	1 to 100	1 and 3Mbps	Short range wirless communication
Profibus		31kbps & 12Mbps	Popular fieldbus in process industry
Firewire	4.5	400 -3200Mbps	Wired high speed communication

Table 1. Different Communications standards used today between reader and computer.

- **Data filtering**: Data read from tag can be incorrect or noisy. Data filtering is performed to aggregate, purge and filter data for application layer.
- **Reader Coordination**: One main task of middleware is to provide inventory movement when tags move from one reader to another. Some middleware can process data from multiple RFID readers. Multiple reader reading capability and intelligence in reader is due to advancement in embedded processor technologies but this may add to cost and space.
- **System Monitoring:** To ensure effective and reliable connectivity and real-time views of network and location of tags, monitoring system detects one or more tagged items and publish the event to one or more routers. The software generated events can be tag identifier, reader identifier and a time stamp.

RFID middleware needs to provide configuration or off-the–shelf solution to define business roles for a wide range of business scenarios. Tag reading is inherently unreliable, meaning that a tag that is within an antenna's read field may not be sensed during each and every read cycle. This requires a more elaborate technique for generating tag presence events, such as multiple read for which tag needs to be present for certain time interval.

4.7 Application software for system integration
Application software runs on ordinary PCs or server communicates with the middleware for RFID, controllers and automation equipment data and process them to control workflow and business transactions and pass it to other systems if needed such as Enterprise Resource Planning (ERP) and backend database systems.

RFID systems require software that manages devices, networks, data and processes to enable continual information flow, alerts, decision support and real-time response to an existing host. Application software is usually designed with function libraries, function blocks or drivers for the quick and easy integration into the respective system. Tools, libraries, API's (application programming interfaces) speeds up the integration of RFID equipment in to existing enterprise system regardless of equipment type, manufacturer, enterprise system application or operating environment. This shields system integrators from the details of low-level protocols, standards, and proprietary hardware interfaces, providing instead a single API for a wide range of hardware.

4.8 Data storage server
Using appropriate networking infrastructure systems, the data obtained by middleware and application can be stored and used for developing, deploying and servicing productivity solutions.
The central server runs a database application, with functions that include matching, tracking, and storage. The software runs on ordinary PCs or servers for a backend database system (e.g., Oracle, SQL Server, Postgres, MySQL) for storing information about the tags. The presence of a robust TCP/IP stack and the availability of SQL database engines greatly reduce an otherwise major integration burden in the development process. In many applications, an alarm or alert function is also present to re-order, for supply chain and inventory management systems, or an alert to a guard, for security applications.

4.9 Enterprise management and planning connectivity
To extracting knowledge from large volume of data, enterprise and higher level management and planning applications are usually developed especially in large scale companies. These software peformanalyze supply chain mangement, Productivity growth, operational superiority and competitiveness.

4.10 Security
While managing number of hardware devices, large volume of data with high speed the biggest risk is security of the data and inventory. Deployment of RFID is usually by leveraging existing IT infrastructure which provides security protocols, secure communication, protected database and authorized services and secure transactions. All components have built-in functionalities that can have pre-defined business rules to execute relevant transactions at business levels.
To derive a business event and execute a business transaction, especially money transaction requires high level of security at software as well as at tag level. Validation and verification services are implemented to get best value from application.
In addition, our cryptography knowledge provides us with the capability of risk and threats analysis. Cryptography techniques are used in RFID for tag identification and security and to secure them from attacks [Karthikeyan & Nesterenko (2005)].

5. Regulatory compliance testing and standards

In integration process and while desiging a prodcut certain regulatory compliance needs to be taken underconsideration for product safety, EMC testing and certification for the major world markets standards.

Region	Electromagnetic compatibility (EMC) and Saftey Standard
U.S.	EMC - FCC Rule Part 15 or 90
	Safety - UL 60950 for Tag Interrogators and NRTL Certification
Canada	EMC - RSS-210
	Safety - CSA 60950 and SCC Certification Body
Europe	EMC testing in accordance to ETSI EN 301 489-1 and ETSI EN 301 489-3
	Radio testing in accordance to ETSI 300-220
	Safety testing in accordance to EN 60950
	Declaration of Conformity for CE marking requirements
Asia	

Table 2. Product safety and EMC testing and certification for the major world markets.

RF conformance tests are critical to assure reliable interoperability among tags and readers. Also the tags and readers also follow the standards such as ISO (International Standards Organization) and IEC (International Electrotechnical Commission).

Standard	Description
ISO-18000	Air Interface frequencies
ISO-15961/62	Data protocols and encoding
ISO-15963	Unique Tag Id
ISO/IEC-18046	RFID tag and interrogator performance test methods
ISO/IEC-18047	RFID device conformance test methods

Table 3. ISO and IEC standards for RFID

Electronic Product Code Information Services (EPCIS) standard provides a data model for tracking events, including shipping and receiving of uniquely identified objects, as items move through the supply chain. ISO standard for supply chain are also availble such as,

Standard	Description
ISO-17358	Application Requirements, including Hierarchical Data Mapping
ISO-17363	Freight Containers
ISO-17364	Returnable Transport Items
ISO-17365	Transport Units
ISO-17366	Product Packaging
ISO-17367	Product Tagging (DoD)
ISO-1734.2	RFID Freight Container Identification

6. Example: RFID integration with IPTV for viewer identification and authentication

For parental control, we can specify how much time children can play games, restricting his channels and viewing time with reminders and memos added in menus[Jabbar; Jeong 2008]. As shown in Figure-3, the RFID reader can be directly connected to the STB using the serial port; if a serial port is not available a USB port can be used for the purpose. The STB should be programmed to identify the Reader with plug and play capabilities and load its driver.

After the successful installation specific menus can be downloaded from the server by Electronic Program Guide (EPG). The menus will guide the user for specific input from his RFID tag and will keep track of all his activities.

 Server can be assigned task such as the encryption, authentication, program installation, user profiles, user contents etc.
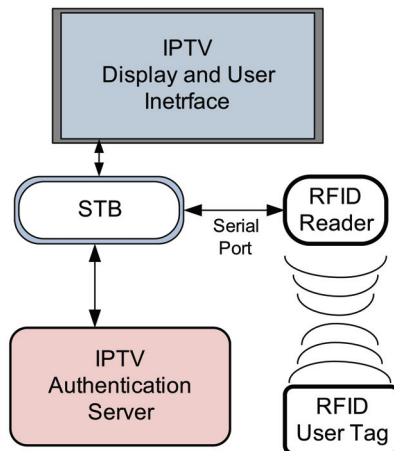
Fig. 3. System Interface for IPTV

6.1 Data transmission

For the testing purposes the RFID serial communicating device was supposed to be detected by the STB. No service label was shown on screen using Java Xlet if the RFID reader was not connected with the STB. After the device detection the user specific menus were loaded from the server as shown in Figure-6 and Figure-7, respectively.

STB middleware was given some file handling and sharing capabilities. Whenever a user was identified by the STB, the java Xlet wrote down a file in a specified format. It was supposed initially that only two account are of super-users and rest are made by the viewers or user, like the children accounts were made by the parents, a guest account option can also be created. A file contain the information related to the user

- Name of the user
- User Type
- Favorite Channels
  - Channels Viewed Last Time
  - Favorite Channels List
- History
  - Previous Videos On demand
  - Channels list
  - Pay per View Orders
- Parental Control
  - Allowed/ Not allowed
  - Time allowed to watch TV
    - User Name

- Other Settings
- Transaction allowed or not
- Personal Profile
  - New User Settings
  - Profile Updates
- Shopping
  - RFID card Verification
  - Make Payment

Whenever the viewer was identified by the STB, the file containing the above information was requested from the server. The server transfers the file to the STB which store the file temporarily and keeps on updating the file, the Xlet was programmed for file read/write operation and when user exits from the menu or STB was turned off the file was saved and transferred to the Server for storage.

Type of file		File size (Kbyte)	Transmission Time (sec)	Viewer Identification Time (sec)
video	.avi	398	486	0.87
	.asf	450	504	1.23
audio	.wav	246	232	0.34
	.wmv	234	239	0.43
	.midi	198	212	0.25

Table 4. Test Results of Data Transmission

Table 4 shows that test results of STB design which includes some parameters such as file type, file transmission time and viewer identification time. The viewer identification time means that duration of waiting time before the file actually identified from the Server on TV screen.
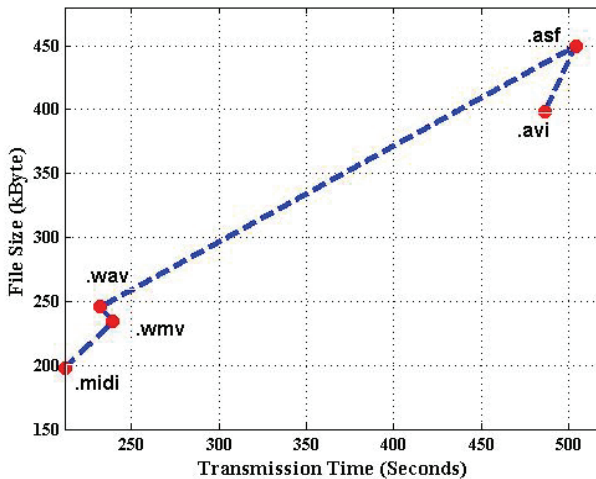
Fig. 4. File transmission time vs. File size

From the test results, we found that video files takes more time to transmit than audio files because of file size, and also viewer identification time is very little after we finally implemented RFID technology with IPTV interface.

The viewer IPTV contents were saved in the server and when required by the viewer after authentication was transmitted to the viewer. The transmission time taken by different media contents, video and audio with file size is shown in Figure-5.
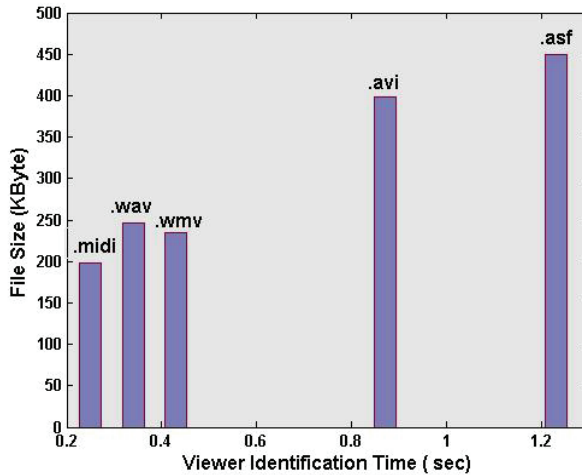
Fig. 5. Viewer identification time vs. File size

Before some secured contents to be transmitted, the viewer was again required to identify and authenticate himself. The time taken by the server to identify the viewer for specific media content size is shown in Figure-5.

6.2 Screen display

Application is an application that is powered by a Presentation Engine (e.g. HTML Browser, Flash) and it support interactive services such as EPG, VOD, games, news, etc. For this case the application layer was EPG and through server Java Xlet based menus and applications were loaded in to the STB for viewer experience as shown in Figure-7.

Although RFID has found much application, one good example in consumer electronics is the integration of RFID system with Internet Protocol Television (IPTV). The system combines the RFID reader, IPTV Set-up-Box, IPTV server, payment server and data storage. Main purpose of such system is to authenticate and identify the Viewer of IPTV for parental control, payment, media storage, and other features offered by the IPTV.

7. Example: RFID integration with Programmable Logic Controller (PLC)

Programmable logic controller (PLC) is a specialized industrial computer used for automation of real-world processes. Most of the leading processes, oil and gas, food, beverage, and similar manufacturing companies have sophisticated automation systems in place that control the high-speed packaging lines in their manufacturing operations and
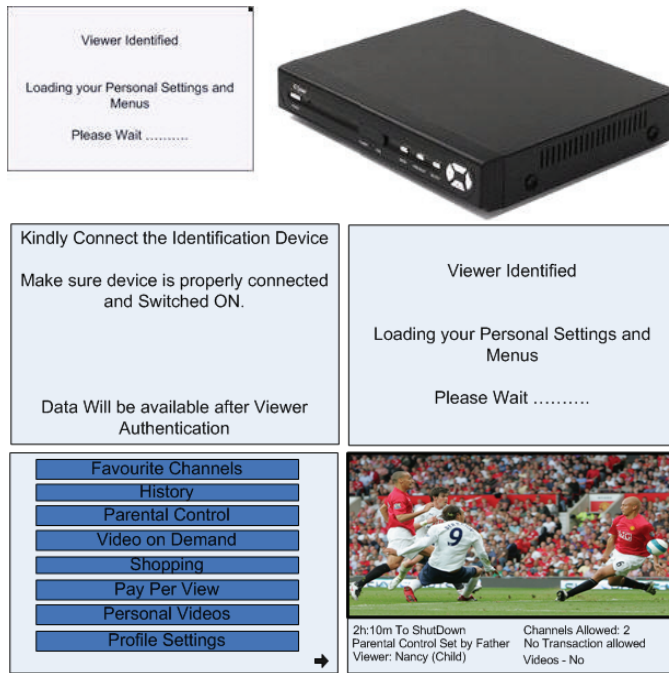
Fig. 6. (a) IPTV Viewers Identification Screen Capture (b) Experimental Platform with Screen Capture and Display.

high-speed conveyors in their distribution facilities. These systems are typically controlled by Programmable Logic Controllers (PLCs), which are dedicated automation systems programmed and maintained by electricians or technicians.

As RFID becomes more ubiquitous, is integrated with the mainstream production process with PLC-centric architecture enabling engineering managers to maintain and upgrade the incremental RFID infrastructure using their existing personnel skill set. One such techinque is utilized to trace fish in supply chain by [Hsu et. Al (2005)].

RFID is widely adopted in Automotive industry. An RFID tag is attached to each vehicle or skid and programmed in production line, this data can be read out and processed directly by means of a PLC. At each manufacturing station, this data is remotely read out by the PLC and then processed to control the production step with PLC updating the data or status information on the RFID tag at end of each station.

7.1 RFID interface with PLC

For interafce with PLC, RFID reader has to communicate with stanadard module which can be plugged in to the backplane of PLC rack. Usually module communicates data between the RFID Tags and the host PLC via a simple ladder logic program in the PLC. The program in module offers normal operations such as Reading and Writing to a Tag and returning status of operations to the PLC. Serial port is usually available with such modules to download and debug the software. These industrial modules are designed to read/write multiple RFID readers, some have ports for antenna and reader resides in module. To have compatibility with PLC system, the module has 24VDC supply.
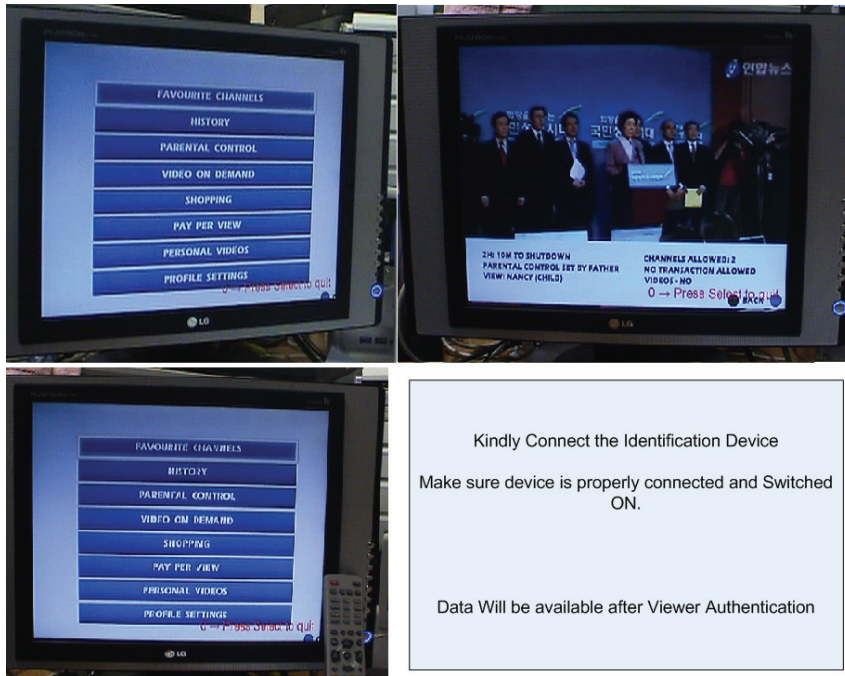
Fig. 7. Screen showing the Interface for users and Menus displayed on IPTV

8. Example: RFID based guidance and object detection for blind and visually impaired persons

Many RFID, image, robots type devices are coming in the market which employs the high tech technology and excellent features to help the blind and visually impaired people [1]. No doubt the devices and features are extraordinary and when developed as a system can help lot many of the visually impaired people of the society. But few are there who are of the low cost. The main requirement to develop a low cost device is because the 90 percent of the blind and visually impaired people in world belongs to the developing countries. Majority of these people cannot afford this costly equipment and most government and institutes in developing countries cannot develop and maintain the system to help the visually impaired people.

This paper presents an idea by going further, taking inspiration from the simple low cost Ubiquitous RFID technology developed for the blood distribution system. First we have shown how the RFID reader developed for blood distribution system can be used for detecting the objects and path for the guidance of blind and visually impaired person. Then we purposed some hardware changes in the system to make it an effective guidance and object detection product by keeping the cost at minimum.

The system consists of short range passive type RFID transponder and receiver developed already and proposed new added hardware. The design of the system needs to be simple and easy to use keeping in mind the low literacy rate and easy system maintenance. When develop this system can be used at an individual home, schools, public places and can become an integral part of the Ubiquitous health care system.

Tags are fitted in to the objects and are programmed to transmit when they are in the interrogation range of the reader. The object tag transmits its data or identification number when the RFID reader is brought near the 140mm area of the tag; object was identified by watching its Identification number in the computer application. As soon as the reader was brought out of the identification area the communication with the tag was lost. Moving the reader away to another object with tag embedded in it, we were able to identify the object using that object Identification number in the computer application. Figure-3 explains the process of object and path detection mechanism.
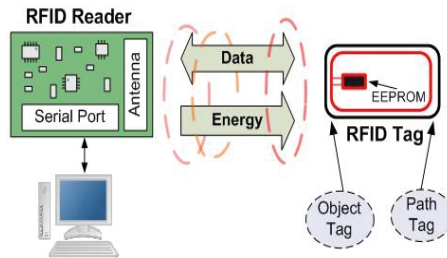
Fig. 9. Object and Path Detection between RFID Reader and Tag

For the path tracking and guidance the tags can be fitted or stick to the carpet or floor respectively. The distance between the tags needs to be greater than twice the interrogation range, greater than 280mm in our case to avoid collision. This was done because the tags used for path or tracks recognition has the same number accept the corners. This was done to keep the system simple and easy to identifiable by the user.

8.1 Proposed RFID detection system

Modifying the above system with already existing hardware and techniques, we can easily make the system to perform the tasks of object detection and path tracking together and informing the person using his/her sense of listening through headphone. Achieving above can make a cost effective, easy to use guidance system for the blind and visually impaired person. With some practice this new system can perform well under certain specifies conditions.

8.2 Proposed hardware changes

The new purposed system consists of four antennas, which are fitted in each hand and feet of the person. To make the cost lower and the system simple we prefer to use one RFID reader and all the antennas communicate with the reader through wires. The speech or voice output can be achieved by using the techniques used in the "Talk Aid" or "An Affordable Digital-Display-to-Natural-Voice Converter for Visually Impaired Radio Amateurs", both the technique employs the PIC microcontroller. New technique requires a microcontroller with greater memory, PIC16F84 memory is of only 64 bytes and it is not enough to store the different tags and there corresponding object names. In this case other microcontroller can be choosing from the PIC microcontroller series.

The system works by keeping in mind its short reading range. Figure 4 explains the block diagram of new proposed system with location of tag and reader on human body. The tag programming is easy using the computer and via serial port reader can programme the tag EEPROM. The Analog Switch (or Analog Multiplexer) can be used to switch between the different antennas, by switching the different antennas in regular interval we can detect the
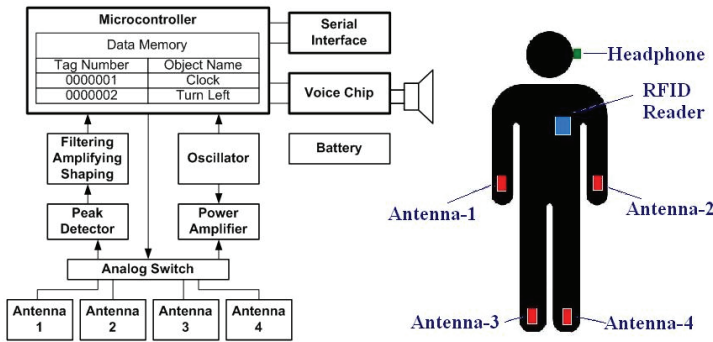
Fig. 10. Block Diagram of Proposed New Detection Methodology

tag in each antenna's interrogation range, this will also make the reader to continuously speak out the object name in range after the specific interval. A comparison table can be made in the internal microcontroller memory or in external memory within card if used to locate the object name using the tag identification number. After locating the object name, a specified sequence of signal can be used to generate the sound to inform the person about the object. A battery can be used to keep the system working all the time. Reader can be designed to fit in the pocket of the person.

8.3 Object detection technique

The antennas in the hands can be worn using the straps as shown in the Figure 5. For the objects detection a person can take out his hand and by moving his hand in one direction all the objects which will be in the interrogation zone of the hand will start to communicate with the reader, as soon as the hands will leave the interrogation zone the communication will be stopped and using his direction of hand, person can get the idea where the object is. As the distance between the object and hand is small, 140mm, accurately catch the object won't be difficult also as the reader will keep on calling the object name with certain interval, person can smoothly reach the desire object. Using both the hands and moving them slowly and listening to headphone all the object distance and position can be estimated by the blind and visually impaired person thus giving him the picture of his environment.
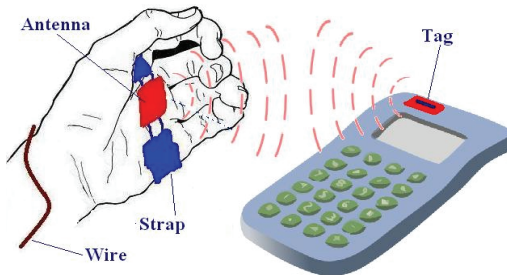
Fig. 11. Object Detection Examples

8.4 Path detection technique

The antennas can be fitted in the shoes. For the path tracking the 1-bit tags can be used in the paths. This means that only two information can be represented by system based upon a

1-bit tag: "*tag in interrogation zone*" and "*no tag in interrogation zone*"[2]. Reader will just transmit BEEP signals via headphone to inform the person that he is going in the right path. As soon as the person will go off the track the BEEP will stop telling him, he is away from the track and he can step back to follow the path again. Tags are to be placed in such a way that the interrogation areas of the tags don't interfere with each other to avoid collision as shown in Figure 6. Identifiable tags can be used in the turning and at the stairs. Railing and the walls can be fitted with the tags so that the hand and feet tags can coordinate well in walking.
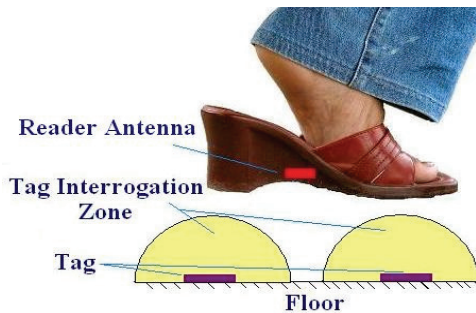
Fig. 12. Path Detection Methodology

Tags are to be placed in such a way that the interrogation areas of the tags don't interfere with each other to avoid collision as shown in Figure 6. Identifiable tags can be used in the turning and at the stairs. Railing and the walls can be fitted with the tags so that the hand and feet tags can coordinate well in walking.

8.5 Cost estimation

Globally, in 2002 more than 161 million people were visually impaired, of whom 124 million people had low vision and 37 million were blind. Visual impairment is unequally distributed across age groups. More than 82% of all people who are blind are 50 years of age and older, although they represent only 19% percent of the world's population. Due to the expected number of years lived in blindness (blind years), childhood blindness remains a significant problem, with an estimated 1.4 million blind children below age 15. Visual impairment is not distributed uniformly throughout the world. More than 90% of the world's visually impaired live in developing countries.

The cost is one of the main issues in developing the RFID system for Ubiquitous-Healthcare. Because this system is designed for the low income people it cost need to be of lower price. A large production volume will make possible to lower the price as well. The system is developed by keeping the number of components minimum and of the low cost. Tags purposed are the lower cost especially the 1-bit tags, person can buy the number of tag according to his need and price. Greater the number of tags will be the environment impression and realization.

The previous developed RFID blood system cost around $150 and keeping in view the cost of new microcontroller, antennas, battery, headphones the approximate cost of the new system is estimated to be around $200. By choosing some standard systems and mass production of these system can greatly reduce the cost for the people still waiting for desire help.

9. RFID integration basic theory

One other example - RFID system composes of two parts reader and transponder or tag as shown in Figure-13. The magnetic field, generated between reader antenna coil (primary coil) and tag antenna coil (secondary coil), transmits powers from reader to tag and data both ways. Reader RLC serial resonance type circuit supplies enough energy using small voltage to generate voltage in tag to enable it for transmitting its data. The resonance frequency, f_0 and f_B of the circuit are shown in Equation 1 and Figure-9.

$$f_0 = \frac{1}{2\pi\sqrt{L_R C_r}}, f_B = \frac{f_0}{Q_R} \tag{1}$$

Frequency of the signal V_D for the reader coil is required to match with the resonance frequency f_0. At time of resonance the voltage on each end is $V_R = Q_R V_D$. Here, Q_R, in Equation 2 is the Q factor of reader coil.

$$Q_R = \frac{2\pi f_0 L_R}{R_R} \tag{2}$$

If Q_R gets too small the voltage of reader coil V_R becomes too small so the energy transferred to the transponder also reduces, hence, the recognition distance gets smaller.

(a) Reader board   (b) Tag
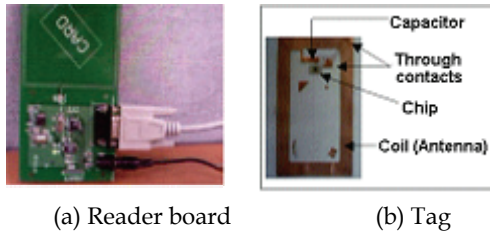
Fig. 13. The Reader and Tag of RFID System

Using front-end impedance modulation method we modulate impedance on each end of the coil depending on the data that it wants to transmit using the Damping circuit. Therefore the voltage on each coil end will change and this leads to the impedance change on reader antenna. And the change in voltage will be detected in the reader section.
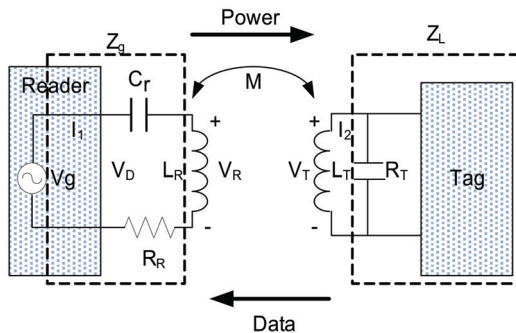
Fig. 14. Basic Inductive Coupled Circuit

In Table 1, the variables related to inductive coupled circuit in Figure-8 are arranged. Z_{11} is total impedance of reader circuit when the tag circuit is open and Z_{22} is impedance of tag circuit when the reader circuit is open. M is mutual inductance that expresses the coupling level between two coils and the relationship with coupling coefficient, k, is shown in the table.

Z_{ab} is driving-point impedance and Z_r is coupled impedance that is created by coupling with tag circuit. Z_r is also called as reflected impedance. When the power V_g is impressed the flow of electric current I_1 is created. By mutual inductance the voltage, V_T is induced in the tag circuit.

$Z_{11} = sL_R + Z_g$	$Z_{12} = sM$	$Z_{21} = sL_T + Z_L$
$Z_{ab} = L_{11} + Z_r$	$Z_r = -\dfrac{Z_{12}^2}{Z_{22}}$	$M = k\sqrt{L_R L_T}$

Table 5. The Variables related to Inductive Coupled Circuit

The electric current, I_2 in the tag circuit is created by the induced voltage and, with this current; I_2 the voltage in the reader circuit is inducted again.

$$I_1 = \frac{V_g}{Z_{ab}} = \frac{V_g}{Z_{11} + Z_r}, \quad I_2 = -\frac{Z_{12}}{Z_{22}} I_1 \tag{4}$$

$$V_R = sL_R I_1 + sM_2, \quad V_T = sM_1 + sL_T I_2$$

Summarization of the formula for voltage and current that was derived using Equation. 4 and the variables is shown in Table 5.

10. Trends in RFID system integration

With emergence of 2-D DataMatrix barcode solution, wireless barcode reader and lower cost of barcodes as compared to RFID tag, current and future trend is the continuation of co-existence of RFID and barcode technologies.

RFID represents research, technology as well as big business opportunities. The RFID readers should become 100% reliable (at present they are typically between 80-95% reliable, depending on environmental conditions) to be able to capture the entire market [R. G. Paul 2007]. One of the major advantages in RFID is the easiness in integration of RFID reader with any type of emerging and current communication standards.

With increasing research and solutions it is expected that future will see increase in proximity scanning, convergence toward standards, processing of all material type and in all type of environment of RFID technology.

11. Conclusion

Radio Frequency Identification (RFID) is finding many applications and ways to help the disable people, and relation with consumer electronics, i.e., IPTV, and/or PLC, etc. As we have a significant benefit of cost, RFID technology can be used in Ubiquitous Network system including Healthcare, Transportation, and Consumer market. This technology can be utilized in any places such as schools, market and road to help and guide the blind and visually impaired people and authorize his/her identification.

Product design is based on the RFID reader and tag communicating at 13.56MHz with RFID reader RS-232 serial port as the interface for STB as an example of usage. The tag contains a reprogrammable memory and works without a battery. Radio Frequency from the Reader triggers and power up's the tag for communication.

With ever increasing applications of RFID in human life, we have connected the RFID systems we developed with IPTV STB. In which Viewer, the person who is watching the TV is identified and authenticated using RFID tag wirelessly.

The IPTV STB transmits this information to the server for authentication, verification, and identification of the viewer with the tag he owns. Already existing RFID tag's like office or ATM or Mobile phone based RFID tags can also be used. As compare to Digital TV, Data storage and e-commerce based applications in IPTV requires the viewer authentication to access network feeds, stored media, communication links and live studio sources, shopping etc. System and device presented is of more interest of Service Providers, who can use the system presented to safely operate their IPTV systems, also the systems requires easy maintenance.

For future compliance with STB's a USB interface is required with RFID reader. The major drawback is that person might needs to move from is sitting place to get himself authenticated for some features, causing inconvenience, this can be avoided using long range reader or implementing RFID reader in remote control.

12. References

Paul, G. R. (2007). Engineering Management-Focused Radio Frequency Identification (RFID) Model Solutions, *IEEE Engineering Management Review*, vol. 35, no. 2, Second Quarter, 2007, pp 20-30, ISSN: 0360-8581

Qiu, R. G. (2007). RFID-Enabled Automation in Support of Factory Integration, *Robotics and computer-integrated manufacturing, 16th International Conference on Flexible Automation and Intelligent Manufacturing,* vol. 23, no.6, December 2007, pp. 677-683

Cox, Jr.; George, D. T. (2007). System and method for RFID System Integration, *Unites States Patent, US 7267275 B2,* Date of patent Sep. 11, 2007

Folerkemeier, C.; Lampe, M. (2005). RFID middleware design – addressing application reqirements and RFID constraints, *Proceedings of SoC-EUSAI 2005 (Smart Objects Conference)*. Grenoble, October 2005

Karthikeyan, S.; Nesterenko, M. (2005). RFID Security without Extensive Cryptography, T*he Third CCS ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN'05)*, pp. 63-67, Washington, DC, USA, November, 2005

Hsu, Y. C.;Chen, A. P.;Wang, C. H. (2008). A RFID-enabled Traceability System for the Supply Chain of Live Fish, *IEEE International Conference on Automation and Logistics, ICAL 2008*. Qingdao, China, 1-3 Sep, 2008, pp. 81-86

Jabbar, H.; Jeong, T.; Hwang, J.; Park. G. (2008). Viewers Identificaion and Authenticaion in IPTV using RFID Technique, *IEEE Transactions on Consumer Electronics*, vol. 54, no. 1, pp. 105-109, Feb. 2008.

RFID Data Management

Sapna Tyagi[1], M Ayoub Khan[2] and A Q Ansari[3]
[1]Institute of Management Studies, Ghaziabad
[2]Centre for Development of Advanced Computing, NOIDA
(Ministry of Communications and IT, Govt. of India)
[3]Department of Electrical Engineering, Jamia Millia Islamia, New Delhi,
India

1. Introduction

An Auto-Identification (Auto-ID) technology has achieved significant growth in various verticals as industries, purchasing and distribution technologies, manufacturing companies, defence and material flow system. Auto-ID is the term used to describe the process of automatic data collection and identification that occurs in real-time. Automatic identification procedures exist to provide information about people, animals, goods and products in transit.

Radio frequency identification (RFID) is a general term that is used to describe a system that transmits the identity (in the form of a unique identification number) of an object wirelessly, using radio waves without any line-of-sight between tagged objects and readers (Auto-ID Technical report, 2002; Khan M Ayoub et al., 2009). RFID is based on Radio Frequency, which operates in different frequency bands viz. low frequency (LF), high frequency (HF) and ultrahigh frequency (UHF). The frequency band is determined by the requirement of application like read range, sensitivity etc. The RFID Devices are capable of operating in frequency ranging from 125 KHz to beyond 2.5 GHz, however, due to regulatory restrictions (typically country specific) on use of radio–frequency spectrum, only few frequencies are commonly used. The two most common are 13.56 MHz in the HF band and frequency around 900 MHz in UHF band. The frequency affects the characteristics of the resulting sensing environment, for instance HF signal propagate more easily through plastic, paper and moisture as compared to UHF, where as UHF signals having longer range. RFID tags may derive the energy to operate either from an on-tag battery or by scavenging power from the electromagnetic radiation emitted by readers. The most obvious technology that is comparable to RFID for many application areas is Barcode. Both these technologies involve the addition of a 'tag' or 'label' to an item that contains information about that item which allows it to be identified by a computer system.

A system designed to identify objects based on RFID tags has two advantages over conventional Barcode systems:

1. Barcodes are fixed once they have been created, whereas the data contained within an RFID tag can typically be augmented or changed as required. This means that:

    a.   It is possible to separate the time at which an object is tagged from the time at which information is stored on the tag – it may be advantageous, for example, to apply the tag at some point in an item's manufacturing process, before the information to be associated with the tag is known. This is not possible with a Barcode.

    b.   Information can be updated as a tagged item moves through a process, keeping the important information with the tag (and the item) and so making it available at any point in its lifetime.

2.   Barcodes have to be scanned deliberately by a person in a process that is difficult to automate. RFID tags, on the other hand, can be readily scanned automatically without human involvement. This reveals that:

    a.   The data can be obtained continuously and thus they are more up-to-date than data obtained only at specific intervals (like inventory counts) and specific points in the supply chain (like shipping or receiving)

    b.   Not involving a human in the process means that the readings can be less expensive and generally more accurate – incremental readings are virtually cost-free once the system has been set. It also means that there may be fewer misreads.

    c.   Speed – many tags can be read simultaneously into a computer, rather than reading a single tag at a time.

3.   Barcodes require line-of-sight to read, while RFID tags can be read (in any orientation) as long as they are within the reader's range. This implies that:

    a.   The content of various conveyances (such as trailers, cases, pallets, shopping carts) can be read automatically without opening and sorting the conveyance.

    b.   Barcodes do not work well when exposed to weather elements, when dirty, or if damaged in any way that interference with clear line-of-sight reading. RFID is much more suited to operation in harsh environments.

This chapter explores fundamentals of data management in RFID applications so that the data retrieved out of RFID application is non-redundant and filtered. The chapter is organized as follows: characteristics of the RFID data is discussed in section 2. Section 3 presents data flow and modeling of RFID data. Section 4 explores the scope of data warehouse for RFID data. This section also focuses on the filtering of noisy data. Section 5 has a focus on the role of RFID middleware. Finally, a conclusion and further research directions is presented in the last section.

2. RFID data characteristics

The RFID systems are being used in variety of applications; despite of this diversity, the data generated out of the RFID application share some common characteristics. The characteristics of RFID data is as follows (Oleksandr Mylyy, 2006):

Uniformity in data: Data emerging out of an RFID application is in the form of (tag_id, reader_id, timestamp) where tag_id and reader_id are the identification code that uniquely identifies the object and reader.

Tremendous amount of Data: This is one the biggest concern as RFID system generates terabytes of data in single day on an average. Thus to deal with such flood of data is challenging task. Adopters of RFID technology must ensure that their IT systems are dimensioned accordingly.

Time based: Each RFID observation is associated with timestamp. In such scenario, it is prerequisite to deal with order and sequence of the RFID observation in which they arrive.

Noisy Data: The RFID system has parallel transponders and receivers. Therefore, the huge information is generated every second that may not be reliable. Sometimes, the information generated from RFID tag is mingled with other tag values or other environmental hindrances.

The challenging issue in the RFID is to identify the presence of tag correctly because RFID environment is not clean. Therefore, let us classify the type of observations that the reader encounters which are as follows (Selwyn Piramuthu et al, 2008).

1. True Positive Readings: These readings refer to the case where the reader identifies the tag to be present while it is in the field of reader.
2. True Negative Readings: These readings refer to the case where the reader is reading the tag as being absent and it is truly not in the field of the reader.
3. False Negative Readings: In this Scenario, the reader might not detect RFID tags, which are in the vicinity of readers. This situation can be raised because of collision of RF signals or due to physical hindrance in the environment.
4. False Positive Readings: In an RFID system there are parallel transponders which have to be detected, so many times while reading one tag, unexpected extra readings from other tags is mixed which leads to inaccurate data.
5. Duplicate Readings: The same tag generates duplicate readings due to multiple readings cycle and multiple readers.

Readings	Tag presence	Acceptance	Narration
True Positive	+	True	Tag is being identified
True Negative	-	True	Tag is not being identified as tag is not in field of reader
False Positive	+	False	Tag is being identified but reported as inaccurate data
False Negative	-	False	Tag is not being identified even it is in field of reader
Duplicate readings	+	True	Read by multiple readers

Table 1. Observation (Reading) types

2.1 Electronic Product Code (EPC) format

RFID tags used in the supply chain are encoded with an Electronic Product Code, or EPC, which is a globally unique identifier for the object being tagged. There are a number of different encoding formats; which one a particular tag uses depends on the tagged item. These formats can be specific to groups of goods, such as shipping containers, or can be specific to each individual asset type. To ensure that each EPC is unique, EPCglobal (the organization driving standards for EPC) assigns each company a unique manager number.

Each company is then responsible for assigning the other fields required by the encoding format being used (EPCglobal, 2005).

EPC, the unique code across the globe, is stored into RFID tag's memory. The code is generic and follow universal numbering scheme for physical objects. The EPC identifies every single, individual product item where barcode only identifies the product. A 96 bit EPC code has structure as follows (EPCglobal, 2005; Khan, M Ayoub, 2009):

Header	EPC Manager	Object class	Serial number
8 Bit	28	24 bit	36 bit

Table 2. EPC Structure (96-Bit)

The first field in the header defines the coding schemes in operation with the remaining bits providing the actual product code. The Manager Field is responsible for identifying the product manufacturer. The object class defines the product class itself. The Serial number is unique for an individual product class. The length of EPC may be of 64, 96, 128,256,1K, 4K Bits. The 96-bit EPC can identify 268 million manufacturers uniquely. Each manufacturer can have 16 million unique object classes and 68 billion unique serial numbers within each object class. Such tags typically operate on the UHF band and are popular with retail and distribution industry (e.g. Wal-Mart). These 96-bit tags are commonly used because of their low cost. Other application may demand HF tags with enhanced capabilities. For example the airline industry is using HF tags, that can easily operate in the environmental extremes. These tags store not only an EPC but also the supplementary data such as repair and service history of part. There are various types of EPC class of different bit-length as shown in table 3.

Class	EPC Length (Bits)
Class-0	64
Class-I	96
Class-II	128/256
Class-III	256-1Kb
Class-IV	4K

Table 3. EPC Class (Khan, M Ayoub, 2009)

RFID readers typically return the raw HEX or binary representation of an EPC, values which must be decoded using bit-level programming to derive a useful representation of the information that a tag holds. As an example, an RFID reader may read and output a HEX value of 30700048440663802E185523. This value must be converted to binary, then decoded programmatically according to the EPC specification to extract the decimal field values, and finally, formatted to return a meaningful representation of the EPC called the Uniform Resource Identifier (URI) representation. The binary representation of the tag HEX value is shown as follows.

0011000001110000000000000100100001000100000001100110010000000000000001011100001100001010100100011

The EPC tag specification outlines the decoding process, which you can follow by interpreting the binary string bit by bit to get a more useful representation. After decoding the binary value, the URI representation of the tag above is as follows:

<div align="center">urn:epc:tag:sgtin-96:3.0037000.06542.773346595</div>

That value must be processed further to determine the item it actually represents. The URI representation is often used for reporting as it is easier for programs or individuals to extract meaningful information about the tagged item from that representation than from HEX or binary values, by filtering or grouping on the various fields.

3. RFID data flow and modelling

The flow of RFID data in the supply chain management is an important aspect of modelling. The RFID tagged object moves from one location to another intermediate locations. At every location, RFID tag identity is matched with the related business data (i.e. requisition document number) in the receiving system so when a RFID tag identity is read, it can be processed further as an automated business event.

To describe this data process further, one needs to understand that the data flow process is composed of two subsets. The first subset is the transmission of RFID data from source to intermediate facility centres. The second subset is the transmission of RFID data from intermediate facility centre to destination.

3.1 Data flow in RFID

In an RFID system, there are two basic categories of data: inactive data and active data. Inactive data are related to commercial entities and product/service groups, such as location information, product level and serial level information. Active data are specific to individual items. There are two types of active data: instance data such as serial number and date of manufacture, and temporal data such as observations, location and containment changes of objects, which are all captured through EPC-tag readings. Among all the data, the temporal data are directly related to the fundamental business logic in RFID applications such as the movement and transaction of products. By examining RFID system, we summarize the following primary entities that interact with each other and generate business processes.
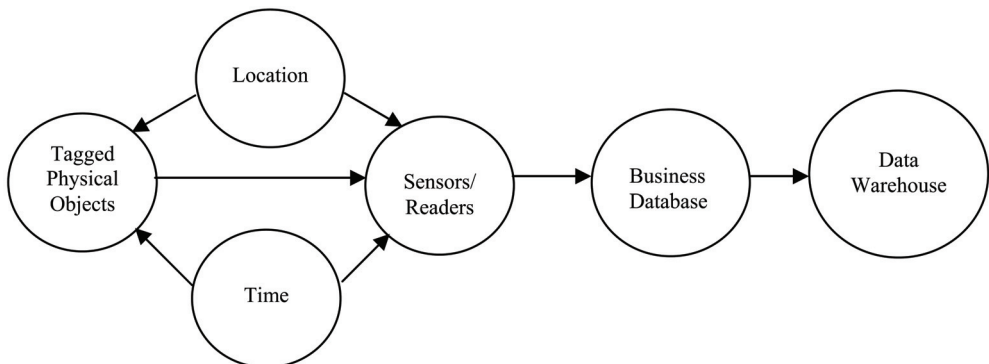

Fig. 1. Data flow in RFID

Objects: These include all EPC tagged objects as items, pallets, cases, and trucks.
Sensors/Readers: RFID readers use radio frequency signals to communicate with EPC tagged objects and read the EPC values. The reader also has unique identification code.

Locations: A location determines the current position of EPC tagged objects. It can be weaving factory, then distribution center and finally retail as shown in figure 2. The granularity of locations can be defined according to application needs.

Transactions: There can be business transactions in which EPC is involved. For example Checkout involves credit card transaction with many EPC readings.

3.2 RFID data modelling

Data modelling is a way to structure and organize data so that it can be used easily by the databases. Unstructured data can be found in word processing documents, email messages, audio or video files, and design programs. Data modelling doesn't want these "ugly" data; rather, data modelling wants data that is all made up in a nice, neat package for processing by a database. So in a way, data modelling is concerned with how the data looks.

Data modelling is routinely used in conjunction with a database management system. Data that has been modelled and made ready for this system can be identified in various ways, such as according to what they represent or how they relate to other data. The idea is to make data as presentable as possible, so analysis and integration can be done with as little effort as necessary. We can also think of data modelling as instructions for building a database. To make a "pretty" database, you have to follow a model as a means toward your desired end. Most of the defined entities (Objects, sensors, and readers) are static by nature but when they interact with each other they generate new observations that are required to be modelled along with static entities. These interactions generate an event that changes state. However, current RFID systems incorporate only event changes and state information has to predict implicitly. One of the essential goals of a RFID–enabled application is to track objects and monitor the system at any locations, at any time, or both. Thus, RFID applications require such data models that are enough capable of modelling these state changes and event changes. But, before explaining the RFID data model let us understand what are the general event changes and state changes (Fusheng wang & Peiya Liu, 2005).

3.2.1 State change

The value associated with the entities defines the state of the object. The change in the values leads to the change of the state as follows (Fusheng wang & Peiya Liu, 2005):

Object location change: For instance, the carrier (truck) and its loaded pallets leave the warehouse. This would change the location of the object.

Object Containment relationship change: Initially all the product items are packed into pallets, then all the pallets are loaded into truck as shown in figure 2.

Reader Location change: Reader 1 is installed at weaving factory, reader 2 is installed at distribution center and reader 3 is at retail.

Ownership change: Ownership changes as the product moves from manufacturer to retail.

Ownership location change: As location is always associated with owner so the detail is required to be captured. Thus, the information about during which period an object is in certain state is essential and has to be acquired.

3.2.2 Event transition

The events are generated time-to-time by the system or based on the interaction between reader and tag to accomplish a particular task as follows (Fusheng wang et al, 2005).

Observation: These are generated when readers interact with tagged objects.
Transacted items: These are generated when an object participates into transactions.

3.3 Dynamic temporal entity relationship model

Dynamic Temporal Entity Relationship Model (DTER) model is a dynamic and temporal based extension to ER model that can be efficiently used to model the entities and relationships discussed above with various new functionalities. There are two types of temporal relationships among RFID entities that we have already discussed: relationship that generates events and relationship that generate state history. For an Event based relation we use an attribute timestamp to represent the occurrence timestamp of the event. For a state–based temporal relationship, we use an attribute tstart and tend to represent the lifespan of the state. It also incorporates nested relationships like the application that uses Read/write tags, an onboard reader records the current temperature measurements or any other location based parameter like humidity etc in the tag. Thus, a reader observation contains both the EPC of the tag and the measurement history, i.e. nested relation
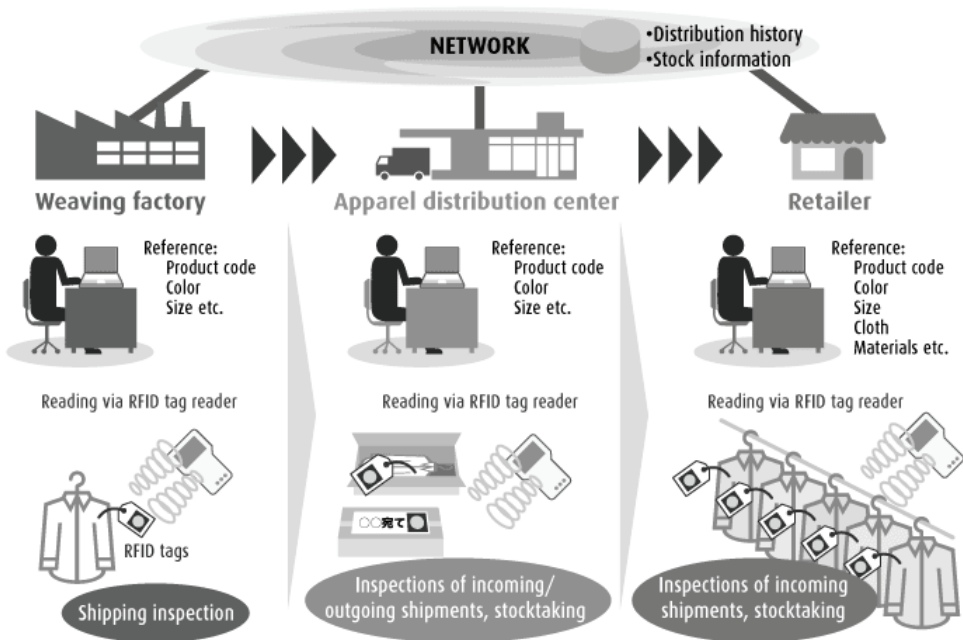
Fig. 2. Object movement chain

4. RFID data warehouse

Data warehousing in RFID is an emerging technology that facilitates in gathering, integrating heterogeneous data from distributed sources and extracting information that can

be utilized as knowledgebase for decision support. The amount of information that would be generated by RFID tags is on the verge of exploding. RFID observation contains redundant, missed and unreliable data because of the various parallel transponders. Thus, it requires cleaning and filtering of the incoming data before warehousing. Thus, it requires cleaning and filtering of the incoming data before warehousing. Before discussing further about data warehousing, a brief architecture of RFID system, some filtering techniques and other data management practices must be well understood.

4.1 Architecture of RFID system

The Figure 3 represents layered system architecture of data movement in RFID environment. The lowest layer consists of RFID tags that are placed on the object to be identified such as cases or pallets.

The next layer is called Data Capture Layer (DCL). The data emerging from this layer can be considered as RFID data streams. They are usually in the form (tag id, reader id, timestamp). Both tag and the reader are identified using a global naming scheme called EPC (electronic Product code) by analogy with the UPC standard that is used for the bar codes.

Application
ONS & EPC Discovery
EPC Information System
RFID Middleware
RFID Hardware (Readers, Antenna)
RFID Tagged Object
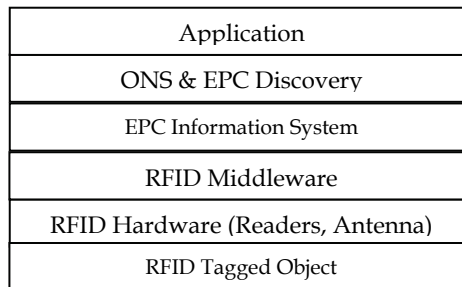
Fig. 3. Object movement chain

The third layer of the architecture is responsible for mapping the low-level data stream from readers to a more manageable form that is suitable for application level interaction. This is also called "savant" that is subject to standardization effort under the name middleware. This layer plays the primary role in RFID data management. RFID middleware systems typically deployed between the readers and the applications in order to correct captured readings and provide clean and meaningful data to application logic. In addition to cleaning data and coping with the idiosyncrasies of different kinds of reader. Application may interact with savants or middleware by issuing simple queries as well as by installing standing queries that result in a stream of matching data. We will study more about middleware in next section.

The fourth layer provides high-level service that is easier for application to use. For example this level maps EPC code to the type of object it represent (individual item, case, pallet) and provides information such as product names and manufacturers, It is also responsible for providing time specific information, such as expiration date of any frozen product represented by EPC code.

The fifth layer of the architecture is part of object Name Service (ONS). The ONS is essentially a global look up service that maps an EPC to a URL that describes the item represented by the EPC. The design of the ONS services uses NAPTR facility of the standard Domain Service (DNS) to rewrite EPC's into URLs. The mapping may be dynamic. For example, as a product moves from manufacturer to distributor and further down the supply chain, the ONS mapping changes to reflect the current custodian of the product.

The last layer of the architecture is the application layer where desired functionality achieved from the filtered RFID data. This application may be written in any high-level language using the library provided by the specific RFID reader vendor.

4.2 Filtering and cleaning RFID data

Due to the low-power and low cost constraints of RFID Tags, reliability of RFID readings is of concern in many circumstances. We have already discussed the type of reading that the reader encounters that leads to various undesirable scenarios i.e. false negative readings, false positive readings and duplicate readings.

In practice, readings are often performed in multiple cycles to achieve higher recognition rate. In this way, false negative readings can be significantly reduced. The noisy readings (or false readings) generally have a low occurrence rate compared to normal true readings. Thus, only those readings that have significant repeats within certain interval are considered to be true readings. However, this will produce much more duplicate readings. To understand the basics of multiple read cycles, a sliding window filtering technique is presented below.

4.2.1 Sliding window filtering technique

A sliding window is a window with certain size that moves with time. Suppose the window size has time coordinate of [t1, t1+window_size], after s time, the coordinate will become [t1+s, t1+window_size+s]. RFID reading tuples will enter the window and get expired as time moves. Therefore, the noise readings are reading with count of distinct tag EPC values below a noise threshold. Denoising essentially performs the following operations: within any time window with size of window_size surrounding an RFID reading, if the count of the readings with same tag EPC values appears equal to or above threshold, then the observed EPC is not noise and needs to be forwarded for further processing: otherwise the reading is discarded. Two parameter used here are window size of a sliding time window, and a threshold for noise detection.

An RFID observation (reading) is in the form of (reader_id, tag_id, timestamp) which refers to the EPC of the RFID reader, EPC of the tagged objects and the timestamp of the observation.

4.2.2 Baseline filtering technique

In this algorithm, intuitively, for each incoming reading of value R, we perform a full scan of the preceding sliding time window of size window size. If R appears more than threshold value within the window, then this is not a noise reading thus we output every R in the window. To ensure a particular reading is never output more than once, we keep a state-of output with each reading in the window buffer and set it to true once it produces the output.

Function Baseline denoise (window size, threshold)
      WINDOWBUFFER   empty queue;
      Loop {loop forever for next incoming reading}
      INCOMING   the next reading
      append INCOMING to the end of WINDOW- BUFFER
      EXPIRETIME   INCOMING.timestamp – window size
      while the head of WINDOWBUFFER is older than EXPIRETIME
      do
            remove the head of WINDOWBUFFER
      end while
            COUNT count of readings in WINDOW-BUFFER whose key equals to
            INCOMING.key
      if COUNT > threshold then
      for each of the reading R in WINDOWBUFFER
            with key equals to INCOMING.key do
            if R has not been output before then
                  output R
                  set STATE-OF-OUTPUT as true
            end if
      end for
      end if
      end loop
      print reading of value R, w
End Function

4.2.3 Dynamic threshold based Sliding-Window filtering

In order to reduce the false negative and false positive reading, all the existing literatures has discussed about the increase or decrease the size of window with some probability based on the circumstances. Some of them has considered concept of multiple readers. We approached this problem in a different manner. Consider a situation where threshold value t_h is six. This means after six occurrence of the raw data in a given time window period this will recognize it as a tag otherwise discard it by considering it as a noise. In the table 4 all black entries are the tag data and red entries are noise. If we consider, reading_of_tag_3 column, where the raw tag data "B2C1C2BA2FD1FA1E" occurs only three times while as the occurrence of noise is much larger and passes the threshold value. This increases false-negative rate. We are proposing following modification to sliding-window filtering (Y. Bai et al., 2006) technique.
1.   Threshold value shall be updated periodically.
2.   RFID data format and associate values (Header information) shall be examined, after recognizing it as a tag.
Former will help in changing the threshold value t_h as the environment will change. Typically, if the error rate is going up then t_h has to be decreased. Later would help in eliminating a noise that is being recognized as a tag. This happens because of sufficient number of occurrence of noise and passes through the threshold value.
Let's formulate the problem of filtering with few assumptions as follows:

S: window Size (In time domain)

$S = r \times i$ Where $\begin{cases} r \text{ is count(repeat count)} \\ i \text{ is interval between readrepeats} \end{cases}$

```
Struct EPCPacket
{
EPC EPCData;
Time T;
Reader R;
}
```

t_h: threshold value
e: error rate

```
DThreshold_SW_Filter(S, T)
{
        EPC Window_Buffer[S]; // Buffer holds EPC data
        Time ArrivalTime [];
        EPCPacket currentEPC;
        Integer EPCCount;
While (TRUE)
{
EPCList    =    CreatEPCList (EPCPacket);    //    create    a    list    to    hold    EPCPacket
data=GetEPCReading ()// get next reading from reader
EPCList.AddEPCPacket (CurrentEPC);
LifTimeofEPCPacket = S – CurrentEPC.T;
EPCCount= FindEPC (currentEPC.EPCData ());
If (EPCCount >= th)
{
At= GetArrivalTime ();
ArrivalTime [] =At; // this will preserve the out-//of-order // sequence problem
If (CheckEPCHeader (CurrentEPC) == TRUE)
        {
        Sort (ArrivalTime [])
        Print (ArrivalTime);


        }
Else
        {
        EPCList.RemoveEPCPacket(LastEPC)
        //Remove that data from the EPC list, because it is a noise
        }
}
If(GetErrorRate() > e)
{
Decrease(th);
}
}//end-of-while
}//end-of- DThreshold_SW_Filter function
```

In the algorithm, to preserve the arrival sequence we have introduced a queue to store the entry time of the tag with the help of GetArrivalTime( ). Then this queue is sorted. The problem of noise is eliminated by introducing CheckEPCHeader ( ) that will examined whether a tag is a tag in actual or a noise. If the value returned is true then only it will display as a tag otherwise discard it. Threshold value th as the environment will change. Typically, if the error rate is going up then threshold has to be decrease. The data for RFID has been generated with the help of EPC Generator. This is variable length EPC data generator i.e. 64, 96, 1128, 256, 512 etc. But, we have generated 64-bit data as show in table 4.

Time	Reading_of _Tag_1	Reading_of_Tag_2	Reading_of_Tag_3
0	FF3CD4FB8ED4FB8E		
100	FF3CD4FB8ED4FB8E	CC4FC3AC2FD1FE8E	
200	FF3CD4FB8ED4FB8E	CC4FC3AC2FD1FE8E	A1B4C2BA2FD1FA1E
300	3FFCE1FC5FA11C8E	CC4FC3AC2FD1FE8E	3FFCE1FC5FA11C8E3
400	FF3CD4FB8ED4FB8E	CC4FC3AC2FD1FE8E	3FFCE1FC5FA11C8E3
500	FF3CD4FB8ED4FB8E	3FFCE1FC5FA11C8E	3FFCE1FC5FA11C8E3
600	3FFCE1FC5FA11C8E	3FFCE1FC5FA11C8E	3FFCE1FC5FA11C8E3
700	FF3CD4FB8ED4FB8E	CC4FC3AC2FD1FE8E	3FFCE1FC5FA11C8E3
800	FF3CD4FB8ED4FB8E	CC4FC3AC2FD1FE8E	3FFCE1FC5FA11C8E3
900	FF3CD4FB8ED4FB8E	FFFCE1FF5FA11B8E	3FFCE1FC5FA11C8E3
1000	FF3CD4FB8ED4FB8E	FFFCE1FF5FA11B8E	FFFCE1FF5FA11B8E3
1100	3FFCE1FC5FA11C8E	CC4FC3AC2FD1FE8E	A1B4C2BA2FD1FA1E
1200	3FFCE1FC5FA11C8E	CC4FC3AC2FD1FE8E	A1B4C2BA2FD1FA1E
1300	FF3CD4FB8ED4FB8E	CC4FC3AC2FD1FE8E	A1B4C2BA2FD1FA1E
1400	FF3CD4FB8ED4FB8E	FFFCE1FF5FA11B8E	A1B4C2BA2FD1FA1E
1500	FF3CD4FB8ED4FB8E	CC4FC3AC2FD1FE8E	A1B4C2BA2FD1FA1E
1600	FF3CD4FB8ED4FB8E	CC4FC3AC2FD1FE8E	A1B4C2BA2FD1FA1E
1700	FF3CD4FB8ED4FB8E	FFFCE1FF5FA11B8E	B2C1C2BA2FD1FA1E
1800	FF3CD4FB8ED4FB8E	CC4FC3AC2FD1FE8E	B2C1C2BA2FD1FA1E
1900	3FFCE1FC5FA11C8E	CC4FC3AC2FD1FE8E	B2C1C2BA2FD1FA1E

Table 4. RFID raw data generated

4.2.4 Multiple readers filtering technique

It's an approach different from the sliding window that caters problem of false reads. This technique is based on the belief that a certain extent of the false reads problem can be caused when communication between tag and the reader is achieved somehow regardless of the presence of signal-blocking entities such as metal shielding. For example a tag might be "visible" to a reader at one orientation but might be "invisible" to a reader in another orientation because the obstacle (e.g. metal shielding) affects communication between tag and reader in one orientation but not in the other. Hence the method deploys multiple readers or tags in order to take advantage of varied signal orientation. The basic idea is that tagged object can be identified to be confirmed as present or absent if consistent reads are

generated by both readers: otherwise the tagged object is identified using a pre-determined probability P.

4.2.5 Duplicate elimination

When noise in the readings is eliminated, duplicate readings for the same tag have to be recognized and only the first one among all duplicates should be retained. The duplicate elimination algorithm takes parameter Max-distance in time domain. If a reading is within max distance in time from the previous reading with the same key (reader id, tag id), then this reading is considered a new reading and is output.

Raw RFID Records
(r1; l1; t1) (r2; l1; t1) (r3; l1; t1) (r4; l1; t1) (r5; l1; t1) (r6; l1; t1) (r7; l1; t1) : : : (r1; l1; t9) (r2; l1; t9) (r3; l1; t9) (r4; l1; t9) : : : (r1; l1; t10) (r2; l1; t10) (r3; l1; t10) (r4; l1; t10) (r7; l4; t10) : : : (r7; l4; t19) : : : (r1; l3; t21) (r2; l3; t21) (r4; l3; t21) (r5; l3; t21) : : : (r6; l6; t35) : : : (r2; l5; t40) (r3; l5; t40) (r6; l6; t40) : : :... (r2; l5; t60) (r3; l5; t60)

Table 5. Raw RFID records

In order to reduce the large amount of redundancy in the raw data, data cleaning should be performed. The output after data cleaning is a set of clean stay records of the form (EPC, location, time in, time out) where time in is the time when the object enters the location, and time out is the time when the object leaves the location. Data cleaning of stay records can be

EPC	Stay(EPC; location; time in; time out)
r1	*(r1; l1; t1; t10)(r1; l3; t20; t30)*
r2	*(r2; l1; t1; t10)(r2; l3; t20; t30)(r2; l5; t40; t60)*
r3	*(r3; l1; t1; t10)(r3; l3; t20; t30)(r3; l5; t40; t60)*
r4	*(r4; 1; t1; t10)*
r5	*(r5; l2; t1; t8)(r5; l3; t20; t30)(r5; l5; t40; t60)*
r6	*(r6; l2; t1; t8)(r6; l3; t20; t30)(r6; l6; t35; t50)*
r7	*(r7; l2; t1; t8)(r7; l4; t10; t20)*

Table 6. Cleaned RFID records

accomplished by sorting the raw data on EPC and time, and generating time in and time out for each location by merging consecutive records for the same object staying at the same location. Table 6 presents the RFID database of Table 5 after cleaning. It has been reduced from 188 records to just 17 records (Hector Gongalez et al, 2006).

4.3 RFID data management practices

The amount of information that will be generated by radio frequency identification (RFID) tags is enormous. That leaves us with questions like "What happens to data quality? What data should we capture, and how often should we capture it? What about 'white noise'?" While we can't address every issue regarding the incoming data avalanche, we can highlight some of the more "front of mind" concerns surrounding RFID. In the effort to address these many issues, adopters of RFID technology are overlooking various important aspects of RFID deployment like how back-end databases and business application can handle the massive amount of new data that RFID systems will produce. In the rush to implement

RFID, users are overlooking the implication to their IT system. Too much focus is placed at present on the price of tags and abilities of readers but not enough on the data, how it is going to be used. If IT infrastructures are not updated to handle the new load they will suffer and shaky infrastructure would collapse.

4.3.1 Turning raw data into information

When designing an RFID system, we should first understand and consider two key aspects of turning RFID data into useful information. First, we need a way to convert the raw incoming RFID data into a meaningful context for further processing and subsequent actions. Because today's marketplace provides an abundance of RFID tag choices, data encoding formats, and custom data options, we'll need a powerful and flexible encoding and decoding architecture to support applications now and into the future. Second, while it might be relatively easy to build an RFID data acquisition and analysis system for the number of tags your business uses today, you have to consider the future. The system must be able to avoid data overload when your system collects data from hundreds of thousands of RFID tags. Filtering and smoothing are important concepts to understand; early in the design process you need to identify architectures that provides flexibility in processing data at the point of activity (M. Palmer, 2004).

4.3.2 Well defined business processes

Let business requirements drive the collection of RFID data. It should be up to the business managers to define what constitutes a business event and how this translates into a read or write transaction on a tag. Adjust the frequency of read or write events to the needs of the business. For example, asset tracking within an Army maintenance and repair facility may require tracking items as they move from one maintenance and repair service area to another, as opposed to installing readers on shelves where parts are stored. In other words, the granularity of data collection should be driven by business requirements not by what is technically possible (M. Palmer, 2004).

Try not to deploy an RFID system directly connecting RFID readers to your central IT systems that may lead to disaster. A better approach is to digest your RFID event traffic close to the source i.e. at the edge of the enterprise and forward only meaningful events to central IT system. For that, devices like network routers and hubs will need to become "smart" and run filters to get rid the network of bad feeds and undesirable information. Transformation will occur in two stages: on the transponders (readers) themselves and on the warehouse receiving the RFID transmission information, Time and date stamping will move to the forefront of database processing necessity (M. Palmer, 2004).

4.3.3 Transform simple data into meaningful data

A simple data stream has to be converted into meaningful data streams that can be directly stored into database. This Process is known as Complex event processing in RFID environment that extract actionable knowledge from discreet events.

4.3.4 Determine business rule

While RFID technologies have the ability to provide a massive amount of data, the first step in a successful data management strategy is to ensure that only meaningful information is passed on from the edge server-the server connected to the readers-to your back-end

applications and data repositories. It's critical that business rules are well defined up front to help separate meaningful information from unwanted data as close to the readers as possible. This will help to reduce the burden on the network and on data storage systems. Additionally, since RFID opens up the capability for unique item-level tracking as opposed to tracking at the part number or stock-keeping unit (SKU) level, changes may be necessary to both data repositories and to enterprise applications in order to accommodate this level of granularity. Determine changes to database schemas that will help ensure that events and attributes specific to unique items can be accurately captured. In addition to data about unique items, you will also want to prepare for data about your RFID infrastructure itself. Information about the physical location and settings of your RFID reader infrastructure must be carefully managed so that you can correlate events with physical locations.

4.3.5 Leverage existing architectures and framework for data integration
When integrating RFID data with enterprise applications, one of the challenges is to leverage the infrastructure already in place to minimize costs. This challenge can be addressed by using existing service-oriented architectures and vendor-neutral integration frameworks to help provide the appropriate IT and business services. Be sure to delineate business services and IT services within your technical architecture. The IT services, such as routing and transformation, should provide a framework for integrating your data irrespective of your business scenarios. Your business services, such as specific business rules, can provide the layer of business functionality that uses the underlying technical service layer.

4.3.6 Data buffering
An RFID data concentrator is software which actually responsible for buffering of the data. There are three primary elements in it: RFID middleware, event processing and an in-memory data cache. RFID middleware provides the interface for applications to receive RFID data from readers. Event Processing handles high-volume, high-performance flows of data by organizing raw data into pipelines (M. Palmer, 2004).

4.3.7 Business dynamics, data ownership and privacy
Over the next three to five years, RFID will force companies to redefine the rules of engagement for collaboration in terms of the how supply chain data is exchanged and protected. Today, many participants in the supply chain are able to benefit from process inefficiencies that are subsidized by their partners. For example, manufacturers don't penalize retailers for stocking too many items within a store. Many stores actually receive merchandise credit plus a service fee when they return expired items to the manufacturer. Electronic tagging can help to smooth out the balance of power in the supply chain by increasing visibility into operations for all companies involved. Some will benefit; others may not. Be certain to understand the business dynamics across all entities that handle your goods or assets, and determine data ownership or privacy issues that may arise.

4.3.8 Analytical information
Having all the data in the world will not help improve a company's profitability if the data is not interpreted correctly or if no one is able to act upon it. Determine business

requirements, such as key performance indicators, that will help you understand and take action based on the data that's collected by RFID systems. In some cases, such as in supply chain performance management scenarios, you may need to be alerted in real time or near-real time when key events or exceptions have occurred or are about to occur. In other cases, the response time may be less critical, and you can employ more asynchronous or batch-oriented techniques in order to process and interpret your data. A business intelligence dashboard can help to monitor key metrics and key processes and allow you to drill down into individual events and transactions for further detail. If you want to automate some of this sense-and-respond activity, consider emerging technologies, such as the Semantic Web standards, which can help computers better interpret data and take actions themselves. In essence, the Semantic Web standards allow computers to better understand the "meaning" of data; this is vital for improved search accuracy and for improved machine-to-machine automation of complex tasks. RFID technologies can provide information that gives companies a greater visibility into their supply chain and a better understanding of their operations, but the decision as to how to respond to this information is ultimately a human one.

4.3.9 Data context
Generally RFID data is simple and straightforward, unless we incorporate complex information using sophisticated, expensive tags; all we get is an identification number of the item, a time and location. Determining in detail data from simple data requires context and context typically comes from "Reference" data in a variety of forms. For example, context can come from information in advanced shipping notice (ASN) as provided a manufacture plant can use the ASN used to confirm that tagged items sent by the manufacturers when actually received.

4.3.10 Age RFID data gracefully
On an Average RFID system requires 7 terabytes of disk capacity daily to accommodate the RFID data, so it is mandatory for us to reduce data continuously, so that we can get manageable working set. The RFID middleware can delete data that are superfluous (e.g. redundant reads of tagged items at different location in the supply chain). Thus Age RFID data to keep your working set of data manageable, enrich raw data with required context, and reduce the load on down-stream systems.

4.4 Data warehousing for RFID applications
Data warehouse is a subject-oriented, time-variant, nonvolatile and integrated technique for organizing data. The components of a data warehouse are the source systems, operational data stores (ODS), data warehouses, data marts, Business Intelligence (BI) reporting and analysis tools, and data movement tools (also called ETL tools). Both the RFID and BI/DW technologies get integrated seamlessly into an architecture that not only puts all the pieces of the jigsaw puzzle together but also helps to develop other tangible architectures in an enterprise framework. Shown below is one such architecture that depicts the use of multiple ODSs and a centralized DW for the capture, processing and analysis of the RFID data.
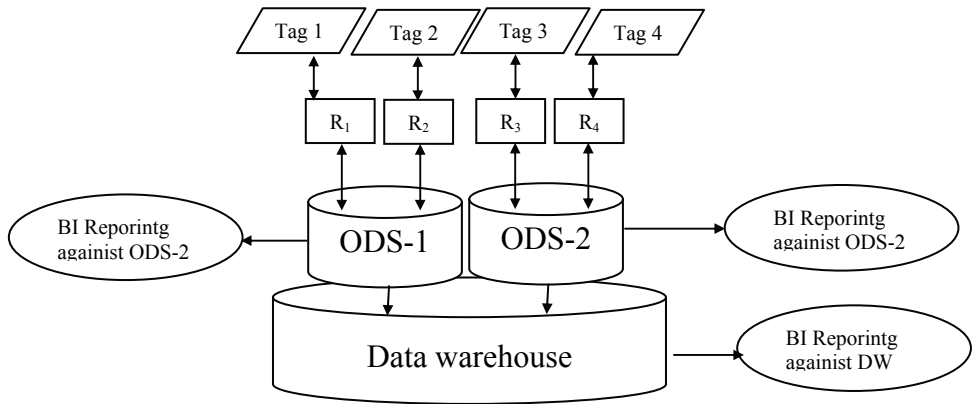
Fig. 4. RFID Data Warehouse and BI

In the above architecture (Figure 4) the data is captured via the RFID tags and passed onto the ODS via the RFID readers. The data from the distributed ODS is then moved to a centralized DW. BI reporting systems can be built to report against the localized ODS and also the central DW as per the reporting needs.

It is very interesting to note that both conceptually and technically there are a number of parallels between the RFID technology components and the BI/DW components and hence they neatly map onto each other, as shown in table.

Now that we have a proper architecture in place, let us discuss some of the BI/DW concepts that are going to be challenged by the onset of the RFID data into the DW/BI systems.

The most crucial point of impact of any RFID-enabled BI/DW initiative is the RFID data sources. RFID technology will bring in a dynamic exploding data in the data source layer of the DW/BI initiative. This will in turn demand a more dynamic analysis of the RFID data, for it to be of any use.

DW Dimensions and Facts	How RFID Answers it
Which (product)	Using the EPPC on the RFID Tag
When (time)	By the RFID Reader Device
Where (time)	By the RFID Reader device
Where (Geography)	By the RFID Reader Device)
Who (Customer)	By the RFID Reader/Tag combination
How much (Quantity)	By the RFID Reader/Tag combination

Table 7. RFID and BI/DW Parallels

The next crucial impact is on the data modeling, data organization and data interpretation technologies. There is a need for newer and efficient data modeling and DW architecting techniques to meet the influx of RFID data sources into DW/BI analysis system. This will also necessitate newer semantic-oriented database technologies and the appropriate data modeling techniques, to handle these large and constantly varying RFID data with a pertinent need for spatial (geographical) tracking of the RFID data across the supply chain of any business domain.

The third crucial impact is the data standardization of the RFID data, so that all the entities in the supply chain can automatically share data, thus enabling a tremendous increase in automation at many levels of the supply chain environment. It is here that the BI/DW technologies are far more matured and evolved compared to the OLTP systems and hence will play a crucial role in the data standardization processes at both syntax and semantic levels.

The fourth impact is the event-based approach to data and information analysis that the BI/DW will have to provide. This is because auto ID/RFID enables machine-to-machine communication, which is automatic, event-driven, and which necessitates that data is captured and processed in real time. This will have a big impact on the way BI/DW processes are designed, which means the BI/DW architectures will have to be flexible, agile, and efficient and event oriented.

4.4.1 Active data warehousing for RFID data

An active data warehouse presents an extension of the enterprise data warehousing capabilities. The foundation of ADW architecture is the detailed transaction history. Responding to near-time business events as they occur, completing complex analysis upon demand, and alerting people or systems to take action leverage the analytical capabilities offered by this infrastructure. What makes this different from the traditional use of data warehousing technology for business intelligence is that an active data warehouse is a closed loop system. Events are analyzed as they occur, and intelligent decisions are promptly initiated. Closed loop systems allow an organization to automatically respond to opportunities with agility, often without the need for human intervention. As business analytics become more instrumental in strategic decision-making, the Active Data Warehousing technology is maturing. This technology is engaged in integrating advanced decision support with day-to-day, even minute-to-minute decision-making that increases quality that encourages customer loyalty and thus secures an organization's bottom line. It may involve components like:

- A well-architect dimensional data model for the destination data mart
- A streamlined ETL process
- An aggressive sizing strategy
- A framework and architecture for expected reporting patterns

Active Data Warehousing extends the support from the traditional data warehouse by:

- Allowing access by customers, partners and suppliers at the same time
- Integrating multi-subject, cross-channel information
- Allowing fully detailed ad-hoc reporting and machine modelling

However, the task of accumulating the data from tags in RFID environment is similar as with analogous task in data warehouse, but still there are several differences in traditional data warehousing and RFID data warehousing. In traditional data warehouse, the data is not queried at the its source, The crux is on storing it into central warehouse, from there it will be indexed and queried, where as In RFID environment data generated by the tag reader is more likely to be used at the same place as of its origin which requires efficient transformation (cleaning, filtering, joining) before storing it into the warehouse.

4.5 Challenges in managing RFID Data

Large volume of RFID Data: RFID systems will have an unprecedented ability to produce great volumes of raw data in relatively short span of time. Adopters of RFID Technology must ensure their IT systems are dimensioned accordingly.

Requirement of Integration: The low level RFID observation need to be transformed and aggregated in semantically meaningful data suitable for corresponding application level. Enterprise with geographically distributed facilities networked to a central IT facility will be faced with the problem of managing raw RFID data while at the same time aggregating it into the central IT facility. Having large quantities of data flowing across network could place a burden on the enterprise IT infrastructure.

Data ownership and partner Data Integration: In retail supply chains or other applications in which data would need to be shared between different companies, questions might arise pertaining to the ownership of data. This could hinder integration of RFID systems between the companies.

Product Information Maintenance: In some application, retail supply chains for instances, central IT databases might continually need to be accessed to retrieve product information. In large-scale implementations, when high volumes of tags are processed, this could put extra burden on IT infrastructure.

Limited Communication Bandwidth: RFID system rely on the availability of unlicensed frequency bands, such as UHF is typically required in supply chain applications because of its increased read range, but European radio regulations permit the use of 865.0 MHz and 868.0 MHz by RFID readers. Another constraint is the bandwidth available per channel that limits data transmission rate between readers and tags. It restricts the number of tags that can typically be identified.

5. Role of RFID middleware

Radio Frequency Identification (RFID) holds the promise to automatically and inexpensively identifying items as they move through the supply chain. Tag and reader Physics solves the problem of being able to capture RFID Data. The Widespread adoption of RFID requires not only low cost tags and readers, but also the appropriate networking infrastructure. As already we have discussed the amount of information that would be generated by RFID tags is on the verge of exploding. RFID observation contains redundant, missed and unreliable data because of the various parallel transponders and to uncover various operational benefits of RFID, there must be something which can process the incoming data and intelligently integrate it into your application, as it is not a feasible solution to link existing software application directly to the RFID readers. The Reason Behind it is:

1. Inappropriate Incoming Data: Not all the incoming data is valuable. Duplicate reads and excess information must be filtered out so as not to bog down the network and end up with unstructured and confusing information within application.
2. Disparity between the Readers: Not all the readers speak same language, Building custom integration logic to each brand of reader will quickly eat up your RFID deployment teams time and budget.
3. Data Dissemination: Different RFID information needs to be passed off to different application and data stores.

Thus it requires cleaning and filtering of the incoming data before installing it into application. In this scenario RFID middleware plays a key role to achieve the maximum benefit of RFID technology. RFID middleware, simply put, is a software layer residing between the RFID hardware and the existing back-end system or application software. It extracts data from the RFID interrogators (readers), filters it, aggregates it and routes it to

enterprise applications such as a warehouse management system (WMS), enterprise resource planning (ERP) software or a manufacturing execution system (MES). Many RFID middleware focused on various features like reader integration and coordination, EPC track and trace tools, baseline filtering capabilities, but these are just a subset of many features the complete RFID middleware platforms must provide.

5.1 Additional consideration for RFID middleware

Reader and Device Management: There are no standard, consistent tools to manage readers, check their health, perform software upgrades, and turn them on or off when necessary. RFID Middleware needs to allow users to configure, deploy and issue commands directly to readers through a common interface for example, users should be able to tell a reader when to turn off if needed.

Data Management: RFID Middleware captures EPC data from readers, it must be able to intelligently filter and route the data to the appropriate destinations. Many of the commercially available offerings take the middleware-as-a-router approach, whereas other packages support business rules, business logic, and business processes to facilitate actions and decision-making leveraging RFID data. Middleware should include both low level logic (like filtering out duplicate reads) and more complex algorithms comprehensive algorithms (content based algorithm), comprehensive solution also offer tools for aggregating and managing EPC data in either a federated (multiple repositories of data) or central data source.

Application Integration: RFID middleware solution need to provide the messaging, routing and connectivity features required to reliably integrate RFID data into existing SCM, ERP, WMS or CRM systems ideally through a service Oriented Architecture.

A service oriented Architecture is essentially a collection of services. These services Communicate with each other. The communication may involve either simple data exchange or two or more services coordinating same activity, such as order placement or shipment.

Partner Integration: Some of the most promising benefits of RFID will come from sharing RFID data with partners to improve collaborative processes like demand forecasting and Vendor managed inventory. This means that RFID middleware must provide B2B integration features like profile management, support for B2B transport protocol integration with partners data such as EDI, web based system AS2 or eventually a well engineered system specifically for EPC data.

Integration with other Auto id technologies: A complete RFID middleware offerings should be able to transform data from all types of Auto Identification and Data Capture (AIDC) input technologies, including RFID, barcode, GPS, satellite and sensors and route it to any network application. This enhancement didn't dramatically affect the prices, as it is no longer a differentiating advantages but a requirement, which reflects customer's heterogeneous RFID environments.

Centralized system: Within domain of a Centralized system, RFID Middleware can enable system to capture and store hardware and software asset information. It must be able to create detailed audit trails (with logging and reporting) to easily identify failed polling and communication sessions. It must provide hands-free maintenance, remote control and

diagnostics. It must be capable enough to deploy, automate and manage anti-virus detection system.

5.2 Middleware's role within RFID solutions

The simplistic, but effective, definition of the role that RFID Middleware supports can be summed up in three primary functions:

1. Data collection and business logic at the edge of the network
2. Centralized system and device management
3. Enabling of mobile, remote and distributed systems with flexible enterprise integration.

Data collection and business logic at the edge of the network includes following(s):

*   Buffering I/O activity
*   EPC handling
*   Event data management – cleansing, filtering, massaging data, etc.
*   Event recognition – rules and exception based
*   Support read/write devices
*   Task management

Centralized system and device management includes following(s):

*   Capture and store hardware and software asset information
*   Create detailed audit trails (with logging and reporting) to easily identify failed polling or communication sessions
*   Provide hands-free maintenance, remote control, and diagnostics
*   Deploy, automate, and manage anti-virus detection systems

Enabling of mobile, remote and distributed systems with flexible enterprise integration includes following(s):

*   Interoperability – common standards and technologies are an immediate requirement
*   Manageability – remote configuration, management, and diagnosis of issues
*   Scalability – suitable architectures to handle the high-volume of data in real time
*   Reliability – robust systems that allow the continual flow of data
*   Security – who has access to data and/or devices and who can make changes

6. Conclusion

In this chapter, we have described the basic format of the RFID data, temporal and spatial characteristics of the data. Further, we have described the problem occurred because of the parallel transponders which generates duplicate data, noisy and inaccurate data. In order to remove these inconsistencies we have discussed various filtering techniques proposed by various authors. Yu-ju-tu and Selwyn Piramuthu has proposed a mean to reduce the false positive/negative through a variation of triangulation. For triangulation purpose they consider the concept of two readers to interrogate a single tag sliding window-based algorithm is no doubt an efficient techniques but it is surrounded with various disadvantages. We have presented a scenario where raw tag data occur less than the threshold value and noise occurred more than threshold, in that case the proposed technique assume noise as correct entry and discard the real raw tag data. We have proposed dynamic updation to the threshold value and examination of EPC header.

We have also explained some challenges in data warehouse, best practices and key differences between traditional data warehousing and RFID active data warehousing. Then

we concluded the chapter with some discussion on the role of RFID middleware in data warehousing. Further, researcher may like to read the event driven and message base middleware design approach (Yulian Fei et al, 2008).

7. References

EPCglobal(2005), Tag data standards Version 1.3 standard specification" , *Auto-ID Lab*, USA

Fusheng wang and Peiya Liu(2005), Temporal Management of RFID Data, *Proceedings of the 31st VLDB Conference Trondheim,Norway*

J. Rao, S. Doraiswamy, H. Thakkar and L.S. Colby(2006), A Deferred Cleansing Method for RFID Data Analytics, *in Proceedings of the 32nd VLDB Conference,* pp. 175-186

Khan, M Ayoub et al(2009),A Survey of RFID Tags, *IJRTE* , Vol. 1, No. 4, pp. 68-71

Khan, M Ayoub, Ojha Sanjay(2009), SHA –256 based n-Bit EPC generator for RFID Tracking Simulator, In proceeding of IEEE IACC, Patiala, Punjab

M. Mealling(2003), Auto-ID Object Name Service (ONS) 1.0, *Auto–ID Lab*, MIT, USA

M. Mealling(2000), The naming authority pointer (NAPTR) DNS resource record, IETF Network Working Group Request for Comments, No 2915

M. Palmer(2004),Seven principles of effective RFID data management, http://www.progress.com/realtime/docs/articles/7principles_rfid_mg mnt.pdf,

N. Khoussainova et al(2007), Probabilistic RFID Data Management, *UW CSE Technical Report* UW-CSE-07-03-01

Oleksandr Mylyy(2006), RFID Data Management, Aggregation and Filtering, *Hasso lattner Institute at the university of Potsdam*, Germany

R. Derakhshan, M. Orlowska, and X. Li (2007), RFID data management: Challenges and opportunities, *Proc. IEEE International Conference on RFID 2007*, pp.175–182

Auto-ID Technical report(2002), *860MHz–930MHz EPC Class I, Generation 2 RFID Tag & Logical Communication Interface Specification*, Auto-ID Centre

Venkat Krishnamurthy et al(2004), Managing RFID Data , *Proceedings of the 30th VLDB conference, Toronto*, Canada

Y. Bai et al (2006),Efficiently filtering RFID data streams, Proc. CleanDB Workshop, pp.50–57

Yulian Fei, Gonglian Jin, Ruqi Wu(2008), Research on Data Processing in RFID Middleware Based on Event-Driven, IEEE International Conference on e-Business Engineering, pp.578-581

Yu-Ju-Tu and Selwyn Piramuthu(2008),A Reducing False Reads in RFID-Embedded Supply Chains, Journal of Theoretical and Applied Electronic Commerce Research ISSN 0718–1876 Electronic version Vol. 3 Issue 2 pp. 60-70

Hector Gonzale , jiawei Han , Diagoe Klabzan(2006), Warehousing and Anaylysing Massive RFID Datasets, *ICDE* 2006

Yu-Ju-Tu et al(2008), A décision support model for filtering RFID Data,*IEEE ADCOM*

Yijian Bai, Fusheng Wang, Peiya liu, Carlo Zaniolo, Shaorong Liu,(2005) , RFID Data Processing with Data stream Query Language , Siemens Corporate Research

Data Storage in RFID Systems

Dirk Henrici, Aneta Kabzeva, Tino Fleuren and Paul Müller
University of Kaiserslautern
Germany

1. Introduction

One of the advantages of the RFID technology over the still more widespread optical barcodes is the comparatively large data storage capacity. Conventional 1-dimensional barcodes can store just few bytes of data. For instance, the EAN13-code used at the point of sale in Europe stores 13 numerical digits identifying country, product manufacturer, and product type. There is no means for identifying each item uniquely. More complex 2-dimensional barcodes or larger 1-dimensional barcodes extend the amount of data that can be stored. This comes at the cost of a larger printing area as long as the readability shall not decrease.

While the amount of data that can be stored using optical barcodes is therewith limited by the available area, RFID transponders offer a more comprehensive data storage capacity. Already comparatively simple tags can store a serial number capable of identifying objects globally uniquely. RFID transponders can thus serve as a means of unique identification for different kinds of objects like clothes, foods, or documents. Transponders that are more expensive can store an even larger amount of data. For instance, additional data describing the tagged objects, a documentation of the objects' history, or even data putting the object in the context of other objects can be stored.

The question arises how to make use of the additional capabilities. What data should be stored directly on the RFID transponders and what data should be stored in databases in the backend of a system? The design decision influences many characteristics of the overall RFID system. Thus, data storage considerations are an important part in planning the architecture of such a system.

This book chapter discusses different design possibilities for data storage in RFID systems and their impact on the quality factors of the resulting system. As will be shown, many characteristics of the systems are influenced. The design decision on the data storage in an RFID system is therewith of great importance. The decision should thus be taken with care considering all relevant aspects.

Note that this book chapter relates only to RFID transponders used exclusively as data storage units. Transponders with processors, cryptographic hardware, or sensors require partially separate inspection and are out of scope.

2. Fundamentals

As already stated above, barcodes usually have only a very limited data storage capacity. For example, the International Standard Book Number (ISBN code) comprises 10 or 13

numerical digits. Such a small amount of data is not enough to uniquely identify an item and to hold all the relevant information describing the item. The same problem exists in other numbering schemes like the European Article Number (EAN) or the Universal Product Code (UPC). These codes identify the product manufacturer and the type of a product at the point of sale. However, they cannot hold a globally unique serial number or additional data like price, ingredients, or best before date.

To cope with the pressing storage limitations, one stores all required data in databases. The data on the barcode is then taken as an index to the object's data in the database. Since the database resides on a server and the data is stored on harddisks, there are only few limitations upon the data that can be stored there. Therewith, the amount of data stored on the barcode poses no limit as long as it is capable to provide an index to the data in the database.
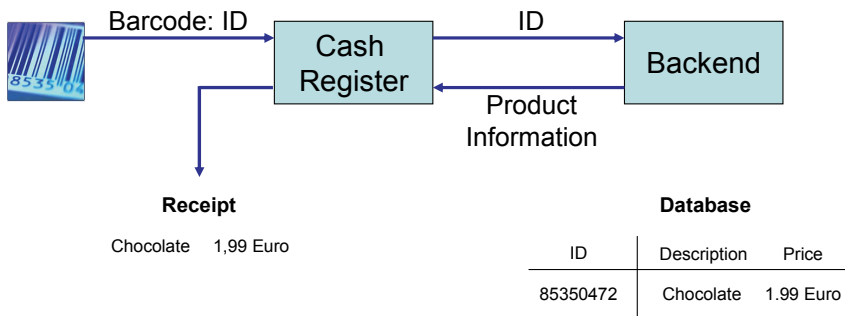

Fig. 1. Barcode system example

An example of a barcode system and the data storage in databases is depicted in Fig. 1. In the pictured supermarket scenario, the barcode ID identifies only the manufacturer and the product. A backend database contains additional product data that can be accessed using the identifier as an index. In the example, an item description of the product and the price of the product are stored in the database. In practice, the database is also used for additional purposes like keeping an inventory of the products in the store. The procedure at checkout is as follows: After the barcode is scanned on the cash register, the scanned barcode data is transferred to the backend of the system. The backend database retrieves the database record associated with the given barcode ID. The relevant data is transferred back to the cash register. Therewith the cash register has all data needed for calculating the total price and for printing the customer's receipt.

There are basically two possible data storage locations in a product identification system: directly on a barcode/transponder or within a backend database. In barcode systems, one usually has no choice: As the storage capacity of barcodes is so limited, one can only store an identifier and has to keep all other relevant data in a database. In RFID systems, there often is such a choice (cf. Fig. 2): One can store data either directly on the transponder, in a backend database, or even redundant at both locations.

Regarding the application spectrum, the storage location is practically unimportant. Remember the cash desk example: Whether the product price is read from the barcode or retrieved from the database does not matter eventually. The cash desk gets the required data, and that is what is relevant for the application. However, the different storage
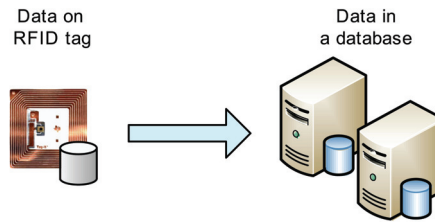
Fig. 2. Data can be stored on the RFID transponder or in a backend database

locations affect quality characteristics of the overall system differently. Such characteristics are e.g. costs, speed, flexibility, and security of the resulting system.

Usually, there are a number of data fields that shall be stored for each item in the auto-id system. For each data field, one must decide where to store it: on the transponder, in the backend database, or even at both locations. In the following subchapter, different possibilities for the realization of data storage in RFID systems, e.g. the separation of data between the transponder and the backend of the system will be presented. Afterwards their impact on different quality criteria will be discussed. Finally, an evaluation of the separate approaches based on these criteria and recommendations for their use in practice will be provided.

3. Data storage possibilities in RFID systems

The following subsections describe different possibilities of separating data storage between transponders and backend database. The different data separation possibilities are grouped into general classes. Subsection 3.1 provides an abstract description of each class. Practical examples for their application in different use cases are the content of subsection 3.2.

3.1 Technical design possibilities

In the following, general classes for the different data separation possibilities between transponder and backend are introduced. Each paragraph describes one class and is headed by a description of the data that is stored directly on an RFID transponder. All other needed data is stored in the backend of the system.

Tag with identifier and voluminous data

This class is sometimes called "data-on-tag". It intends to keep all data relevant to an object directly on the transponder and to avoid the necessity of data storage in a backend database. In this approach, all relevant product data is stored directly on the RFID transponder. The object marked with the transponder can also be identified via a globally unique identifier, e.g. the tag serial number or an identifier assigned by the application.

Tag with identifier and few additional data

In this class, a unique identifier of an object is stored directly on the RFID tag. This identifier is structured, and it comprises several parts like manufacturer and product type. Referenced by this identifier, additional data stored in the backend can be accessed. In addition to the unique identifier, a few other data fields are stored directly on the RFID chip. Normally these fields are important to the lifecycle of the tagged object.

Tag with multi-structured identifier

This scenario stores only data needed for the unique identification of the tagged object directly on the tag. All other data is stored in the backend of the system. The data identifying the object and acting as an index to data in backend databases has a defined structure. The data word subdivides into multiple parts. Each part has a particular meaning. As an example, the Electronic Product Code (EPC), which is the designated successor of the EAN code and UPC code, provides separate data word parts for the manufacturer of the product, the product type, and a serial number. Thus, the data word has a three-part structure. Each part of the structure has an interpretable meaning. The composition of these parts provides the worldwide unique identification of each product item.

Tag with minimal structured identifier having application relation

Similarly to the previous class, only identification data is stored directly on the RFID tag. Like in the previously presented class, all data describing the object is kept in databases. The difference between the two approaches is in the structure of the identifier. The structure of the data word is reduced to a technically essential minimum. The concrete structure of the data depends on the specific application context.

Identifiers having minimal structure comprise two parts. The first part specifies who is in charge of the tag. The second one provides the uniqueness of the identifier. Content of the first part could be the manufacturer of the product for example. The structure is required to provide scalability of the resulting system. This way, data can be partitioned amongst different databases: The first part of the identifier selects the database; the second part provides an index within the selected database. Within a closed system, no structure at all is required.

Tag with minimal structured identifier without application relation

This scenario is very similar to the one described before. However, the single parts of the identifier permit no inference on the application or the object qualities. The identifier again consists of two parts. The first part specifies the management organisation. It does not necessarily have any reference to the tagged object. Thus, the first part identifies neither the manufacturer of the product nor its owner or proprietary. Like in the previously presented approach, the second part is a serial number identifying the object uniquely within the management organisation. Again, the structure of the identifier provides scalability to the system. However, in this class, the components of the identifier do not reveal information about the respective tagged object.

Tag with unstructured identifier

In this scenario, the RFID tag stores only a serial number as identifier. The identifier is seemingly random and has no meaning. In a closed system, such an unstructured identifier is enough to reference arbitrary additional data stored in a backend database.

The unstructured identifier approach is only successfully applicable in closed systems. The application of tags with unstructured identifiers in a cross-organisational or even in a global RFID system is not sensible since the reader of the transponder will not be able to identify the organisation it has to contact to obtain further information regarding the tagged object. Consequently, the scalability of the system is strongly restricted. Pseudonymization infrastructures offer a theoretical solution to the problem. However, due to some drawbacks this solution is not practically interesting (see Henrici 2008).

Tag with changing identifier

Tags with a static identifier can be used for the identification of objects and therewith for the construction of traceability profiles. Such functionality is often desired, for example in logistics. However, for people carrying tagged objects, the functionality can violate privacy since indirectly people can be recognized and pursued. With a changing identifier that is still usable to identify the object in the legitimate backend, it is possible to allow only authorized individuals to recognize and pursue tagged objects and thus provide privacy protection. Possible implementations of this approach are still a field of research in RFID security (see Henrici 2008). Yet, a secure implementation requires RFID transponders that offer additional functionality than just data storage. Since such transponders are out of the scope of this chapter, changing identifiers will not be considered further.

	Identifier and voluminous data	Identifier and few additional data	Multi-structured identifier	Minimal identifier with application relation	Minimal identifier without application relation
Manufacturer identifier	X	X	X	X	
Product model identifier	X	X	X		
Unique serial number	X	X	X	X	
Date of manufacture	X	X			
Best before date	X	X			
Manufacturer in plaintext	X				
Product model in plaintext	X				
Ingredients list	X				
Recommended retail price	X				
Instructions for use	X				
Management organisation identifier					X
Unique number within the management organisation					X

Fig. 3. Practical example: Supermarket product

3.2 Practical examples

In the following, a set of practical examples illustrates how the presented classes of different separation of data between transponders and backend behave within different areas of application. All of the examples relate to inter-organisational or even global RFID systems. In closed systems, transponders with an unstructured identifier would also be an interesting option.

For each example, a table shows which data will be stored directly on the RFID transponder. All other data relevant within the separate scenarios are found in a backend database; the data can be retrieved using the identifier read from the transponder as an index.

The total amount of data stored for a specific object is always the same. In the different approaches, the data is just distributed differently between the transponder and the backend database. A redundant storage of data both on the transponder and in the database is also

possible. However, in the scope of the considerations in this chapter only the information stored directly on the transponder is of interest. Whether this information is only stored only on the transponder or whether it is also available in the backend database is insignificant. Redundancy can be an interesting feature in some use cases though.

	Identifier and voluminous data	Identifier and few additional data	Multi-structured identifier	Minimal identifier with application relation	Minimal identifier without application relation
ISBN	X				
Author in plaintext	X				
Title in plaintext	X				
Key words in plaintext	X				
Library: Identifier	X	X	X	X	
Library: media number	X	X	X	X	
Library: loan status	X	X			
Library: safety	X	X			
Volume number	X	X			
Market price	X				
Blurb	X				
Management organisation identifier					X
Unique number within the management organisation					X

Fig. 4. Practical example: Library book

The following example scenarios are presented:
- a supermarket product (cf. Fig. 3),
- a library book (cf. Fig. 4),
- a medicine (cf. Fig. 5),
- a bus ticket (cf. Fig. 6).

4. Discussion of the different technical design possibilities

The previous section showed different possibilities to separate the required object data between the transponder and the backend. This section discusses the advantages and disadvantages that each technical design possibility has in practice. Different quality characteristics of the resulting RFID system are taken into consideration: Speed of reading and error rate, flexibility, security, privacy, and costs.

All application functionalities can be realized using an arbitrary one of the different possibilities. The application has all data available. Whether the data source is a transponder or a backend database does not make any difference regarding the functionality of the applications. However, some people argue that the data-on-tag approach has advantages for mobile applications where there is no network connection available between reader and backend. Due to the increasing ubiquitous availability of wireless and mobile networking

	Identifier and voluminous data	Identifier and few additional data	Multi-structured identifier	Minimal identifier with application relation	Minimal identifier without application relation
Manufacturer	X				
Pharma Zentral Nummer (PZN)	X	X	X	X	
Charge number	X	X	X		
Unique serial number	X	X	X	X	
Best before date	X	X			
Prescription	X	X			
Active ingredient in plaintext	X				
Active ingredient strength	X				
Dosage form	X				
Package size	X				
Name in plaintext	X				
Package insert	X				
Storage remark	X				
Management organisation identifier					X
Unique number within the management organisation					X

Fig. 5. Practical example: Medicine

	Identifier and voluminous data	Identifier and few additional data	Multi-structured identifier	Minimal identifier with application relation	Minimal identifier without application relation
Bus company	X	X	X	X	
Ticket type	X	X	X		
Ticket number	X	X	X	X	
Balance	X	X			
Issue date	X	X			
Validity	X	X			
Previous rides	X				
Forwarding conditions	X				
Management organisation identifier					X
Unique number within the management organisation					X

Fig. 6. Practical example: Bus ticket

and the fact that a network connection is often also required for related functionality and accessing other applications, the argument ceases importance. Moreover, other aspects like the quality characteristics presented in the following, become more important over time since business demands and user expectations increase.

4.1 Speed of reading and error rate

A high speed of reading is of great interest for many different kinds of applications. For example, on a conveyer belt as many transponders as possible are to be scanned per time unit in order to raise the throughput of the belt. When using mobile reading devices, a high reading speed is important, too, especially when bulk reading is performed. For example, supermarket consumers dislike waiting at the cash register because reading of the RFID tags is taking long. When the reading device sends out its request, a lot of tags are queried at the same time. A good anti-collision mechanism is needed but also a low time for reading a tag. It must thus be possible to read a transponder at a high speed.

Another important requirement is a low error rate. Transponders shall be detected with a high probability and their data have to be read correctly – even in disadvantageous environments. This is a very important aspect for maintaining a high data quality which is required to make the RFID technology capable of serving today's sophisticated business demands.

For both the reading speed as well as the error rate, the decisive factor is the wireless connection between transponders and reading devices. The data transfer rate and the bit error rate (BER) determine the quality of the connection. These parameters depend on the applied transmission method (e.g. frequencies, data coding) and on environmental influences.

The data transfer takes longer if the transmission rate is low. Further, for a given bit error rate on the communication channel, it is more likely that an error occurs if a greater amount of data is transferred. Conclusively, the amount of data to be transmitted should be minimized to avoid transmission errors and to achieve a high-speed of reading. In order to optimize the speed of reading and to reduce the error rate, it is advantageous to store only the data that is absolutely necessary directly on the transponder, i.e. only an identifier. Other data should therewith be kept in the backend where high bandwidths and reliable transmission channels can be provided easily.

The part of the data that is stored in a backend database needs to be retrieved from the server. Thus the reading device needs a network connection to be able to communicate with the backend. However, in current IT infrastructures such a network connection is nearly always available since it is required for other purposes as well.

4.2 Flexibility

In times of rapidly changing business requirements, companies have to adjust to new situations quickly. Therefore, flexibility is a key factor for a company's success on the market. The most flexible RFID solutions with respect to data storage are the ones that store only identifiers on the transponders and as much product data as possible in the backend.

A first advantage of exclusively storing identifiers on the transponder and of keeping all other data in backend databases is the system's compatibility with already existing barcode systems. Today, barcode systems are the most prominent solutions for auto identification. RFID transponders are expected to supplement and in many scenarios to replace the

barcodes in the future. In many years to come, both technologies will continue to complement each other and RFID tags will only be used to identify expensive products. The reason for this is that barcodes are extremely cheap, they are simple, and they do not provide that many privacy issues as RFID. In contrast, RFID transponders provide a more comfortable handling and can offer better protection against forgery. Systems that use barcodes and RFID transponder simultaneously can be easily implemented if barcodes and RFID tags are considered as different kinds of data storage while keeping the same kinds of data. This means that the data should have the same structure. In order to minimize the size of the barcodes printed on the objects, the amount of data should be minimal, i.e. just an identifier.

A second advantage of storing just identifiers on the transponders is transponder reuse and cooperation between different companies within the supply chain. When barcodes or transponders store globally unique identifiers, they can be used in a global business scenario. Several worldwide companies are involved in such a scenario. All these companies want to use the same transponders rather than to attach their own transponder to the objects. However, it may be possible that each company needs to store additional data or data that is not intended for other companies. The storage capacity of the transponders limits the additional data that each company can store directly on the transponders. Therefore, if data is stored directly on transponders, it needs to be ensured that the transponders have enough memory and that each company has the rights to access the information they need. If a company is cooperating with many others within the supply chain which is the standard scenario today, the coordination becomes very difficult if not infeasible. Just storing globally unique identifiers on the transponders is a much more practicable way to make transponder uses across companies and cooperation possible. Each company can operate a backend database, and the identifiers stored on the transponders act as an index to data stored in the backend. This way, cross-company RFID systems are comparatively easy to implement.

Systems using multiple auto-id technologies are easy to implement if data is stored in databases. For instance, barcode identifiers and identifiers on RFID transponders can reference the same data in the backend so that the different identification technologies can interoperate within the same auto-id system. Using this procedure, compatibility with existing barcode systems can be preserved. This is important in many application scenarios like the point-of-sale.

Another advantage of storing data in the backend instead of on the transponders is that in many application scenarios it is useful to be able to alter data without the transponders being in the range of a reading device. Data stored in a backend database can be accessed and altered at any time, independently from the location of the tagged object.

When an RFID transponder is read, always the current data is retrieved from the database. This results in huge advantages in certain situations - particularly when the transponders are located outside of the administrative influence. A system relying on backend databases is also more flexible because data stored in the backend can be kept up to date much easier than data stored on the RFID tag. For example, it should be avoided to store a package insert of a medicament directly on a transponder, because in the backend always the latest package insert can be made available. This is the only way to ensure that e.g. the latest information on side effects is available. This example also shows that data that is valid for many objects needs to be altered just once instead of requiring the update of all copies.

Data storage in the backend is more flexible than data storage on transponders if evolvement of applications is considered. Over time, business demands change and increase and thus new versions of applications are implemented. Updating the design often requires changing the structure of the data to be stored. Adding or deleting data fields in a database in the backend is much simpler than in the memory of numerous transponders. When changing the data structure on some transponders, others would still use the obsolete versions. This would require a version management since readers are required to handle different versions of data formats on the transponders. This increases the complexity of the whole RFID system considerably. In contrast, data structures in backend databases can be changed at an arbitrary time. The changes become valid at once, and the old data structures are no longer in use anywhere in the system. Storing data in the backend and not on transponders thus makes evolvement of applications a comparatively easy task and the implemented RFID system therewith future proof.

4.3 Security (in general)

The connection between the reading device and the transponder is wireless, using the air as transmission medium. Thus communication is public: Transmitted data can easily be intercepted. In theory, it is possible to apply cryptographic protocols to secure the transmission, but this requires the use of RFID transponders that have more functionality than just data storage and that are thus more expensive. Such tags are more powerful than cheap ones and offer functionality like cryptographic algorithms and more memory. Such functionality is considered in (Henrici 2008) and other literature. However, in this chapter we exclude these types of transponders from our discussion because in many scenarios, like in the retail trade, only cheap chips can be used. The transponders that we address in this chapter are thus able to store data (encrypted or in clear), but they are not capable of executing cryptographic operations on their own.

Storing unencrypted data on transponders exposes it to the public because attackers can intercept or retrieve the data unnoticed. As long as the transponders remain within closed and controlled areas such as a factory building, this threat can be neglected. Unfortunately, most transponders leave such closed areas during their lifecycle. Therefore, it makes sense to store as much data in the backend as possible because in this case data does not have to be transferred over an unsecured communication channel. Further, access to the data in the backend can be restricted effectively and flexibly. Arbitrary access controls to backend databases can be implemented so that every requestor for data gets just the data he is entitled to access. Such fine granular and flexible access controls cannot be implemented on transponders.

However, storing data on transponders is useful in applications where centralized data storage should be avoided. For instance, the electronic passports in many countries (e.g. Germany) currently store biometric data on transponders but do not store copies in central databases to secure the data. For such security sensitive applications, data can be stored encrypted on transponders to prevent unauthorized access. Encrypting data has the disadvantage that a key management is required. Depending on the application, such a key management becomes very sophisticated.

Another special case in which some data fields should be stored on the transponders is when there is a requirement that data shall be written exactly once and then never be allowed to be altered afterwards, not even by the transponder issuer himself. Such

"unalterable data" could be required e.g. for the protection of consumers. It is impossible to guarantee that data in the backend cannot be modified since at least the database operator can change the data. The storage of data in the backend must be avoided in these special cases.

On the other hand there is data that needs to be altered at some time of the lifecycle of an object. Low-cost RFID transponders cannot implement a stronger protection than a key/password that is transmitted in plaintext as authorization. The capability of an effective and flexible protection is thus very restricted. Such problems or even vulnerabilities are not present when having read only identifiers on transponders and storing and altering data in the backend. State-of-the-art computing power can be used in the backend for implementing flexible access control and encryption operations.

4.4 Data security and privacy

As described in the previous subsection, data stored on the transponder can be eavesdropped during communication or the attacker can use his own reading device to access the stored data. To avoid these threats, it is reasonable to store as much data in the backend as possible. An effective and flexible access control can be implemented there, and data does not have to be transmitted over insecure communication channels.

From a data security perspective, when leaving the factory, the transponder should only contain the information that is needed by other companies that process these transponders. This is the only way to avoid possible threats posed by industrial espionage and to respect the principle of data security to store no more than the absolutely required data. If just an identifier is stored on a transponder, no action needs to be taken when the tagged object leaves the company's environment. Linked data can still be available in databases so that it is available in case the tagged object returns. In contrast, when data is stored directly on transponders, some data needs to be deleted when the tagged object leaves to adhere to data security. If no copy is stored elsewhere, the deleted data is no longer available for future use.

Law

Laws regarding data security and privacy are different amongst the countries (see EPIC 2004). In many democratic countries, there are laws regarding acquisition, processing, storage and deletion of personal information. Sometimes the laws cover data that may be related to personal information or that may be linked to persons, too. The matter is already quite complex if a single country is considered. Laws and regulations varying over the countries and economic areas make things even more sophisticated.

If an RFID system is implemented, the laws and regulations of all countries in which the system shall be operated needs to be considered. To avoid different functionality and procedures in different countries, it makes sense to try to find a common denominator that is acceptable in all countries. To be safe, storage of data directly on transponders should be avoided since data on transponders is difficult to secure and since adaptation to changing laws and regulations is difficult or infeasible if many transponders are already "in the wild".

Public Acceptance

RFID technology can only unfold its benefits in all areas of life if the public does not fear it and accepts it. In the media, many different scenarios are described that show the misuse of RFID technology and how it poses a threat. Some threats are real; other threats described in these scenarios do not show exclusive misuse of RFID technology but can be said about

other systems like barcodes, too. For example, products can be associated with persons when the attacker maps the product identifiers to the consumer in a supermarket. This could both be done with barcodes or RFID tags. So, one goal when designing a RFID system should be to avoid privacy threats and to thus earn the acceptance of the public.

Data stored on a transponder can be read unnoticed; eavesdropping on the read operations is possible. Depending on the frequency, the range of a reading device can be a few centimeters up to a few meters for passive transponders. However it must be assumed that the usual range can be exceeded with specialized technology, for example by using a higher field strength. By applying technical tricks, 10 cm can easily become 50 cm (Kfir & Wool, 2005). Other scientific publications also report of even higher range extensions (Sarma et al., 2003). Note that the usual read range is only that short because passive transponders are powered by the electromagnetic field of the reading device. Passive eavesdropping is possible from much greater distances.
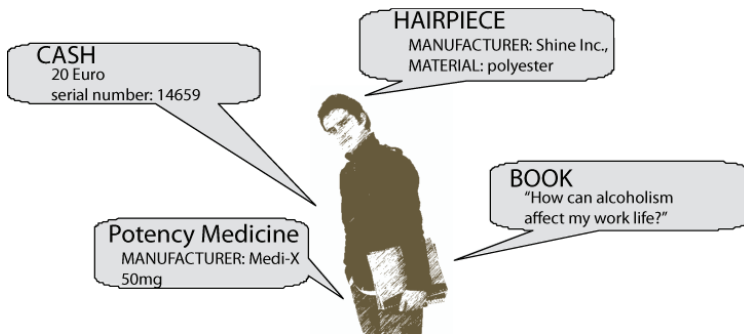

Fig. 7. Example for the violation of privacy

An example for the violation of privacy can best describe the impact of storing too many data directly on the transponder. Imagine, you could read all transponders that the person in Fig. 7 is carrying. A lot of confidential information could be retrieved, such as the health status or embarrassing details of the person's life. RFID transponders might be used for detection and prevention of banknote forgery, so a pickpocket would know if someone carried enough money worth a theft.

The privacy problem in this example originates from a combination of harmless pieces of information. Together the pieces provide a lot of personal information. The pieces of information are:

- A link between persons and objects: We see that the person carries objects.
- A link between objects and RFID transponders: The transponders are attached to the objects.
- A link between RFID transponders and stored data: The transponders store data that have a meaning.

A single piece of information is relatively harmless, e.g. the RFID transponders contain no personal data. Nevertheless, several pieces can be assembled to form a detailed image, thus undermining privacy. The data on the transponders can be linked to the person and conclusions can be drawn.

To solve this problem completely, the data on the transponders must not reveal any information that would be interesting for an attacker when linked to the person carrying it. Thus, from the perspective of data privacy, it is recommended to store as little data as

possible directly on the transponders and to take away any interpretable meaning of the data.

Even the listing of manufacturers, product key and serial numbers is too much information, as we learn from the example. Nevertheless, current plans for the point-of-sale are to equip all products with an RFID transponder that contains at least the manufacturer, product type, and serial number in the form of a multiply structured identifier. The reason is that the developers used what is the standard in barcode systems (manufacturer and product type) and transferred these concepts to the new RFID systems by just adding a serial number.

Sometimes it is argued that the identifiers used in barcode systems are just plain numbers that have no meaning to an attacker as they cannot map the numbers to the manufacturer or the product. However, this argument is misleading: firstly, the mapping between identifiers and brand and product type is known to every enterprise resource planning system in the point-of-sale so that it cannot be kept secret; on the other hand, an attacker can easily create tables with the mappings by hand. For example, for the well-known EAN-system, an official database is freely accessible (GEPIR, 2009). Additionally, there are a number of community-driven databases (see EAN-DB, 2009). It is probable that such databases will be available for the EPC (Electronic Product Code) in the near future, too.

For privacy reasons, RFID transponders should thus contain only minimally structured identifiers that preferably have no interpretable meaning. This means that a minimally structured identifier composed of an identifier of a management unit and a unique serial number provided by this unit is the best choice. Ideally, the management unit has no reference to the object whatsoever. The management unit should be neither the manufacturer nor the owner or the proprietor of this object because such information can provide clues to the nature of the product.

In the previous subsection 4.3 a special case was discussed: data that may not be altered or data that should not be stored in a central location. To hide such data, it should be stored on the transponder in an encrypted form. The necessary key to decrypt the information can be stored in the backend where it can be secured by the necessary access controls and other measures. Alternatively, the key can be printed on the object. This is done in electronic passports: the data of the holder's photograph can be decrypted using data that is printed on the passport. This protects the data from being accessed unnoticed by the passport holder.

Location Privacy

Another privacy issue arises when a person is constantly carrying objects with RFID transponders attached to them. Example objects are watches, eyewear, and footwear. Then the so-called "location privacy" is threatened: When a reading device detects a transponder several times, it is possible to conclude that it is most likely carried by the same person. This information can be used to create a movement profile or to capture consumer habits.

A related problem would occur if tire manufacturers would equip tires with transponders. Petrol stations for example could create movements profiles unnoticed by the consumers and log where and how often a consumer fills up his car and thus derive itineraries and habits. This scenario is not fictional: several years ago, a tire manufacturer has announced the equipment of their tires with RFID transponders. Consumer protests resulted in a boycott and a negative corporate image; so the plan was abandoned.

The creation of such movement profiles is made possible by using transponders that store data that is unequivocal and unchanging. This can be for example a simple identifier or arbitrary other fixed data. Even encrypted data can be misused when it does not change as

the attacker can conclude that it is the same transponder and thus the same object every time he reads the same data pattern.

Just storing unstructured identifiers that change regularly is one solution to this problem. This way, outsiders cannot determine that they are dealing with the same object. Transponders with additional functionality are required for such solutions, but these are out of scope of this chapter.

4.5 Costs

The costs of RFID systems are an important issue as far as productivity and efficiency of business processes are concerned. This includes the prices of the transponders as well as the costs of the infrastructure, i.e. the reading device and the backend systems. Operating and maintaining a system leads to additional costs.

In the previous subsections, we discussed some of the factors that have impact on the costs as well, for example, time wasted by a system that reads the transponders at a low speed. This subsection addresses the direct costs that have to be considered.

In some scenarios, the number of objects is very high. Thus transponders are needed in large quantities, especially if the transponders cannot be reused. Therefore, the unit price is a major factor of the expenses. The capabilities of the transponders determine their unit price; these include the amount of available memory, hardware circuits to compute complex algorithms or protocols, etc. The number of transponders that are manufactured also affects the unit price (small batch series versus mass production).

Consequently, transponders of the same type should be used that have only a minimal set of functionality. This enables mass production. Further, transponders that only store a globally unique identifier should be used. Then only comparatively cheap transponders with a small amount of memory are required. The structure of the stored identifier, i.e. the parts in which it is divided, may differ from scenario to scenario, but the structure does not affect the price.

The prices of the reading device are one part of the infrastructure costs. In all application scenarios, reading devices will be needed, regardless of whether data is stored directly on transponders or the backend. Additional expenses for the infrastructure encompass cost of installation, maintenance and operation of the backend system and the communication network.

If all data is stored on the transponders, a mobile reading device can read the data immediately. In this case, no communication with a backend system is necessary, and therefore the costs of the backend can be reduced. This may be considerable amount because it includes the communication system as well as the backend databases.

However, in practice, the infrastructure is very often required for other purposes as well and sometimes even already available. For example, it is often desired to transfer the data to an enterprise resource planning system where the data is further processed and statistics are derived. Therefore, there will be no extra expenses for the installation, maintenance and operation of a backend system in these cases. Then it is irrelevant regarding infrastructure costs whether data is stored on the transponder or in the backend system.

5. Conclusion

Increasing maturity of RFID technology and falling prices for transponders result in a broad acceptance and usage of RFID systems over the years. RFID technology will also be used in areas where the technology is now too unreliable or too expensive.

Enterprises and service providers have to consider different options when designing the RFID systems. This chapter discussed the question whether the architect of an RFID system should decide to store data directly on the transponder or preferably in backend systems. First, the technical design possibilities were listed and illustrated by practical examples. In the next step, the effects on quality characteristics have been shown considering the different design options.

	Identifier and voluminous data	Identifier and few additional data	Multi-structured identifier	Minimal identifier with application relation	Minimal identifier without application relation	Structureless minimal identifier	Changing identifier
Read and error rate				X	**X**	**X**	**X**
Flexibility				(X)	X	X	**X**
Security					(X)	X	**X**
Data protection / Privacy protection							**X**
Costs				(X)	**X**	**X**	**X**

Fig. 8. Summary

Fig. 8 highlights the impact of the choice of the technical design regarding data storage on the prospective system. Plain crosses or crosses printed in brackets denote cases where the criterion is satisfied; crosses printed in bold indicate an optimal solution with respect to the criteria in question. The figure provides only the general trend and omits details and special cases.

The figure shows that the optimal solution for the protection of privacy is the one with changing identifiers. Due to the higher cost of this solution compared to other solutions, this variant will only be applied if it is required by obligation of law which cannot be expected in the near future.

The most meaningful solution is the one to only store a minimal identifier without a reference to the application context on the transponders, and all other data remains in the backend. This version enables high-speed reading so that a large number of transponders can be read in a short time. The flexibility of the backend data storage solution is advantageous in many fields of application. Modifications to existing applications are carried out relatively easily. No useful data is transmitted via an insecure communications channel. Establishing an effective access control, encryption, and other precautions in the backend is relatively simple, flexible, and cost-effective. Therewith, privacy of individuals and enterprises can be protected. The solution to only store minimal identifiers is also very desirable from a cost perspective.

Thus it is recommended for decision makers and developers to develop RFID systems in such a way that only a minimal amount of data is stored directly on transponders, i.e. a minimal identifier which has no reference to the application context. All other data can be held flexibly in backend systems. Only in special cases another approach makes more sense.

6. References

EAN-DB. 2009. *Community-driven EAN databases*
        Open EAN/GTIN Database, http://openean.kaufkauf.net/
        EAN search « EAN-Suche », http://www.ean-suche.de/
        Codecheck, http://www.codecheck.info/
EPIC and Privacy International. (2004). Privacy & Human Rights 2004: An International
        Survey of Privacy Laws and Developments; Powell's Books
GEPIR – The yellow pages of GS1 – Die gelben Seiten von GS1. (2009).
        http://www.gepir.de/v31_client/
Henrici, D. (2008). *RFID Security and Privacy -- Concepts, Protocols, and Architectures*, Springer-
        Verlag, Heidelberg
Kfir, Z. & Wool, A. (2005). *Picking virtual pockets using relay attacks on contactless smartcard
        systems*, IEEE Conference on Security and Privacy for Emerging Areas in
        Communication Networks - SecureComm
Sarma, S. E.; Weiß, S. A. & Engels, D. W. (2003). *Radio-Frequency Identification: Security Risks
        and Challenges*, Cryptobytes, RSA Laboratories Vol. 6, No. 1, pp. 2-9

An Efficient Approach for Data Transmission in RFID Middleware

Hongying LIU[1], Satoshi GOTO[2] and Junhuai LI[3]
[1,2]Graduate School of Information, Production and Systems, Waseda University,
[3]Computer Science & Engineering School, Xi'An University of Technology,
[1,2]Japan
[3]China

1. Introduction

RFID projects have been deployed in many enterprises profoundly. From the perspective of architecture, a RFID application system includes three parts: hardware, software and middleware. The hardware consists of RFID readers, tags and antennas. Software refers to the enterprise management information system which has been operated for a long time. Middleware is the most time-consuming part. How to import data from RFID reader to management information system? Who is responsible for this task? Whether or not adopt off-the-shelf RFID components? All the above issues should be carefully considered.

RFID middleware is system software that collects a large volume of raw data from heterogeneous RFID devices, filters them and summarizes them into meaningful information, delivers this information to applications and makes them interoperate with legacy systems. The implementation of RFID middleware in enterprises can provide flexible configuration. Parameters of related components can be set. And then only the required information is imported to the system. When extra RFID readers are added to the system, there is no need to develop program again. The RFID middleware will take care of all these changes.

However, the performance of RFID middleware is not satisfactory. In particular, when Web Service is used to bridge the difference of diversified platforms, the efficiency of data transmission is decreased. A Web Service is a software system identified by a URI, whose public interfaces and bindings are defined and described using XML. Web Services allow access to software components through standard web technologies, regardless of platforms, implementation languages, etc. This technology has impacted RFID-based applications in a profound way. For the mobile client system, Web Services enable the integration of various applications in a distributed environment from the resource-limited terminals. Though its performance optimization poses challenges for researchers.

Several methods and strategies have been proposed to improve it. In our paper, we design a Context-Store and apply it to the exchange process of SOAP messages between mobile terminal and server. A SOAP message which includes three sections: SOAP Envelop, SOAP Header and SOAP Body, are separated into 2 groups, one is the static part, and the other is the dynamic part. The main idea of our approach is to store the static part while only transmit the dynamic part through network. Then on the receiver side, we can assemble and obtain the whole message.

Under the experiment of a mobile client server system, RFID data is transmitted between the J2ME platform on PDA and the Microsoft Windows Server 2003 operating system on server. SOAP messages in different lengths are tested. Compared with the general method and compressing method, our Context-Store approach has the least average response time. It is efficient. Finally, the prototype system, which is implemented and applied to production lines in a manufactory, is described in details. Processing data collected from RFID tags attached to the product on production line is packed into SOAP messages and sent to application server by Wireless LAN. After confirmation, the PDA client can access application server to update processing data continuously.

2. Background

Radio Frequency Identification (RFID) is a kind of Auto-Recognition technology that allows RFID reader to read data from RFID tags via radio signals from a distance and without line of sight. With significant technology advantages over bar code identification systems, RFID has been gradually adopted and deployed in a wide range of applications, such as access control, item tracking, highway tolls, production line auto-management, supply chain management and so on. A typical RFID system consists of tags (transponders), readers, antennas embedded both in tags and readers.
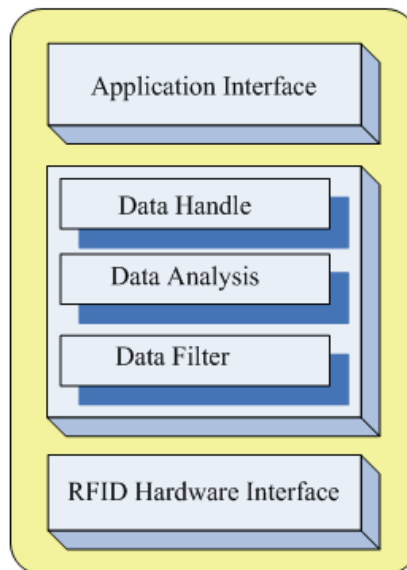
Fig. 1. Typical structure of RFID middleware

RFID middleware is system software that collects a large volume of raw data from heterogeneous RFID devices, filters them and summarizes them into meaningful information, delivers this information to applications and makes them interoperate with legacy systems (Taesu Cheong & Youngil Kim, 2005). Therefore the basic functions of RFID middleware are supporting the independency of the multi-protocol of heterogeneous readers and playing the role of a broker for data exchange.

A typical RFID middleware has such abstract structure as shown in Fig. 1. The Hardware Interface directly communicates with RFID readers and other terminal devices. The middle layer is responsible for data management and data transmission, such as filtering data, analyzing data and handle data. The Application Interface provides friendly access interface for upper layer applications including various enterprise and its partners. For instance, we can invoke Web Services in this Interface to accomplish broader applications. A number of works on RFID middleware has been published (Christian Floerkemeier & Matthias Lampe, 2005; Young-Il Kim et al., 2006).

A Web Service is a software system identified by a URI(Universal Resource Identifier), whose public interfaces and bindings are defined and described using XML (World Wide Web Consortium, 2008). Web Services allow access to software components through standard Web technologies, regardless of platforms, implementation languages, etc. This technology has impacted RFID-based applications in a profound way. Especially for the mobile client system, Web Services enable the integration of diversifying applications in a distributed environment from the resource-limited terminals. It transmits business data on Web by virtue of HTTP (Hypertext Transfer Protocol, a universal protocol used on Web) and SOAP (Simple Object Access Protocol). The transmission process is illustrated in Fig.2. The client creates a SOAP message embedded in a HTTP POST (a request method used in HTTP) request according to the WSDL (Web Services Description Language), and then sends to server through network. The Web Service request processor on the server will deal with this message. It parses the SOAP message, invokes corresponding Web Services, and then creates response message. The server sends back this SOAP response message to client by HTTP.

SOAP (World Wide Web Consortium, 2007) is a lightweight and simple protocol which is based on XML. It is designed to transmit structured and solidified information, and can be used together with many protocols and formats on the Internet, such as HTTP, SMTP (Simple Message Transfer Protocol) and MIME protocol (Multipurpose Internet Mail Extension) etc.
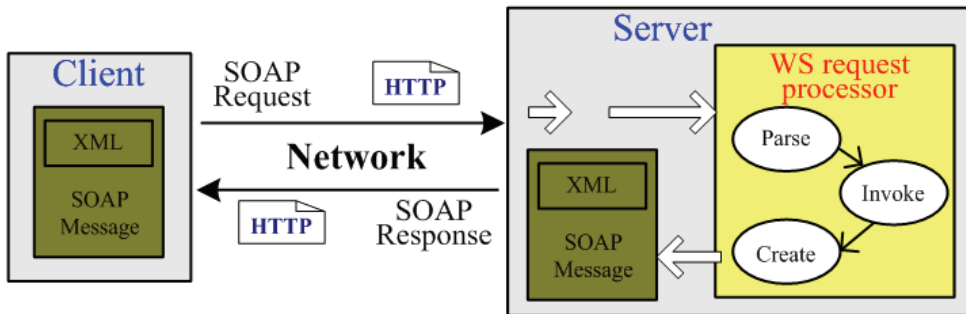

Fig. 2. Data transmission process with Web Services

For the application of Web Services-based RFID either within an enterprise or between different enterprises, several meaningful attempts have been done. Generally, when the technique of Web Services is applied to RFID system within an enterprise, the main purpose is to deal with the information in enterprise network, and make advantage of the processing capability of RFID middleware system. Clemens Kerer et al (Clemens Kerer et al., 2004) design a so-called "Presence Manager Service" to manage the list of people attending the conference. This application tries to combine Web Services with RFID devices and send the

data collected from RFID reader to organizer of the conference. It is a unique application of which functions are not complex and the data involved is in a small scale. So it is not appropriate to apply this method to large scale systems, such as supply chains in logistics. When Web Services is used to assist the information exchange between different enterprises, its characteristic of supporting real-time data share and mutual interchange of B to B is revealed. Both the information on RFID tags and the processing status are provided to users. Niranjan and Aura Ganz (Niranjan & Aura Ganz, 2004) propose a framework for a multimedia information transmission system in which diverse wireless networks and devices communicate. The client components which include lap-top, PDAs, are connected to smart objects through Web Services in dynamic environment. Each network provides its own resources to other networks by Web Services. B S Prabhu et al (B S Prabhu et al., 2006) introduce a framework for RFID middle ware. The task of this middle ware is to serve the information exchange between enterprises. Each enterprise communicates with others through Web Services across the boundaries.

Though these Web Services-based performance improvement poses challenges for researchers. There are some achievements both from industrial and academic institutes. V Prabakar et al. focused on the manageability of Web services in RFID application (V Prabakar et al., 2006; Han Chen et al., 2005). K.Devaram and D.Andresen suggested to cache SOAP messages in client side to enhance the performance (K Devaram & D Andresen, 2003) Seshasayee B and Noah Mendelsohn et al encoded the SOAP message by binary codes (Noah Mendelsohn et al., 2004; Seshasayee B et al., 2004). Mike Nikitas compressed SOAP messages (Mike Nikitas, 2003). However the above methods cause some negative effects. The binary encoding loses the advantage of readability of the XML-based SOAP messages. The compressing method produces extra compressing and decompressing time costs and loses the access transparency.

In this paper, we design and realize a Context-Store approach to improve the Web Services performance in RFID middleware. Both the experiments and the application example show its efficiency. The remainder of this paper is organized as follows. Section 3 presents our framework. Section 4 describes the realization of our approach in detail. Section 5 shows the experiments. Section 6 outlines the application in manufactory. Section 7 draws conclusions and suggests future research.

3. Framework design

According to the research work (Julio Fernandez et al., 2005; Toyotaro Suzumura et al., 2005), the major factor affects the performance of Web Services is the cost of SOAP message transmission. So the purpose of our approach is to reduce the message length transmitted in network. The main idea is to store the static part while only transmit the dynamic part through network. Then on the receiver side, we can assemble and obtain the whole message. SOAP message (World Wide Web Consortium, 2007) is a sort of XML document. It comprises 3 sections: SOAP Envelop, SOAP Header and SOAP Body. In the following discussion, we divide it into 2 parts, the static part which contains the SOAP Envelop, fixed SOAP Header (assessing Web Services not for the first time) and Tag information such as "<? xml version="1.0"enconding="utf-8"?>", and the dynamic part which contains SOAP Body and dynamic SOAP Header (accessing Web Services for the first time).

The framework of the system is shown in Fig. 3. This framework includes mobile terminals which are capable of collecting data from RFID tags, Context-Store, Web Services server and transmission channels such as network and so on. The mobile terminal sends requests by SOAP messages. The Web Services server responses. Context-Store is a kind of file storage
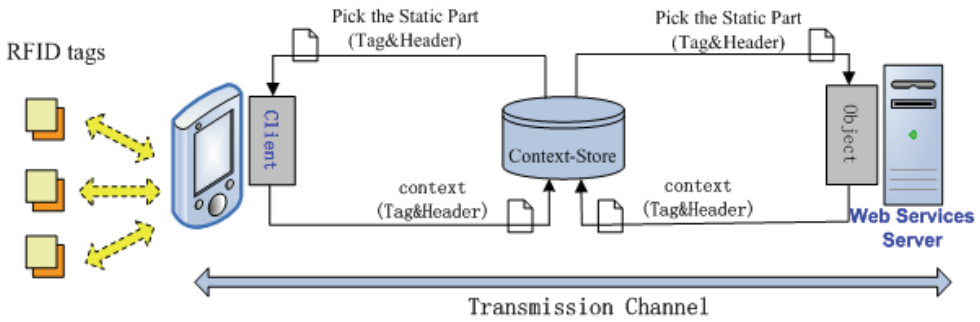
Fig. 3. System framework

structure, which can be accessed by client and server. It stores the context information such as SOAP Envelop, fixed SOAP Header and tag information. To choose a suitable structure as Context-Store is up to the specific application environment. For example, considering the limited resources on mobile terminal, we adopt a simple text file structure. The static part of SOAP message stores in Context-Store, while the dynamic part is transmitted through network. Then after assemble, we can obtain the whole message from the mobile client side or the Web Services server side.

4. Approach description

4.1 Context-Store construction
The main idea of our approach is to reduce the lengths of SOAP messages transmitted through network to enhance the performance of Web Services.

Fig. 4. A Context-Store template

The mobile terminal communicates with the Context-Store in the following steps:
Step 1.   Create a context with ID;
Step 2.   Store a specific context matched to the ID;
Step 3.   Pick the context from Context-Store;
The server communicates with the Context-Store in the following steps:
Step 1.   Store the context information which access the Web Services for the first time;
Step 2.   Pick the context from Context-Store;
We construct a template for the Context-Store in Fig. 4 to initiate communication process between mobile client and server in which we set the ID as "00". Because of the fast speed of assess ordinary text file, in our realization, we construct TXT files as Context-Store to store

context information in both mobile client and server side. They are symmetrically nominated as Client_Context_Store and Server_Context_Store respectively.

4.2 SOAP expansion on mobile client

On the mobile terminal client side, we expand the communication process by the following algorithm, and it is illustrated in Fig. 5.

```
If request
{
    Serialize a message;
    Construct SOAP message;
    Access Client_Context_Store;
    Compare the ID with ID in SOAP message;
    If matched
  {
       The arbitration module disassembles SOAP;
    Send SOAP Body and ID to server;
    }
    Else
     Send a whole SOAP;
}
Else
{
    Pick the context from Context-Store;
    Deserialize SOAP message;
    Assemble SOAP message;
}
```
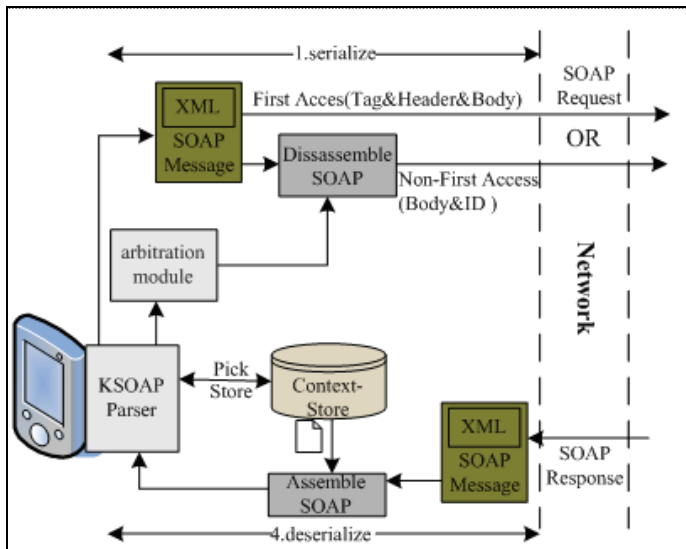

Fig. 5. Algorithm on mobile client

4.3 SOAP expansion on Web Services server

On the Web Services server side, we expand the communication process by the following algorithm, and it is illustrated in Fig. 6.

```
Receive a SOAP message;
Access Server_Context_Store;
Compare the ID with ID in SOAP message;
If matched
    The arbitration module assembles SOAP;
Else
{
     The arbitration module receives a whole message;
   Deserialize the SOAP message;
   Serialize the SOAP message;
   Send Soap Body;
}
```
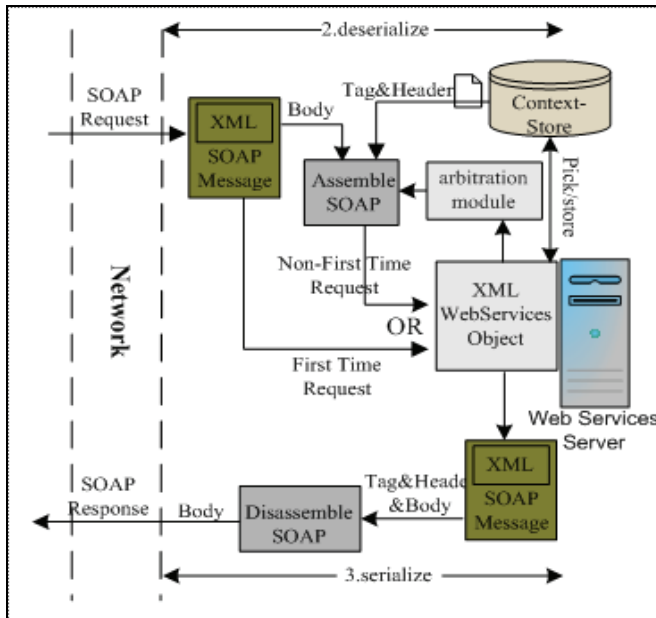

Fig. 6. Algorithm on Web Services server

5. Experiments

We construct the following environment to test our approach. The mobile client side adopts PDA, which installs J2ME and the Wireless Toolkit 2.5.2 development tool. The server side installs the Intel Pentium 4 CPU, 3.0GHz, 768MByte RAM, Bandwidth 100Mbps, and Microsoft Server 2003 operating system, and Dot Net SOAP Engine expansion system, IIS

6.0. Under such configuration, the result of our experiment is shown in Fig.7. The result in an Internet mobile computing environment is indicated in Fig.8.
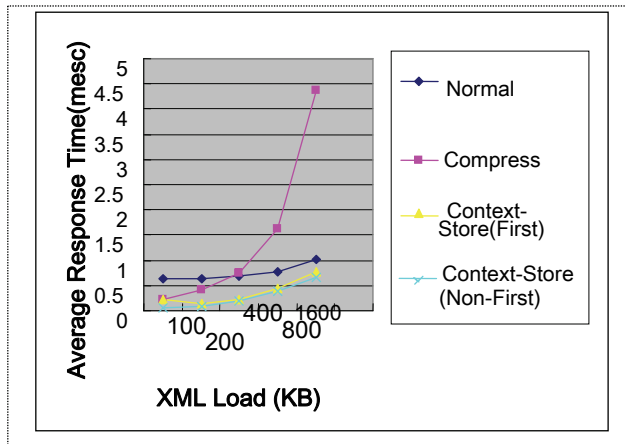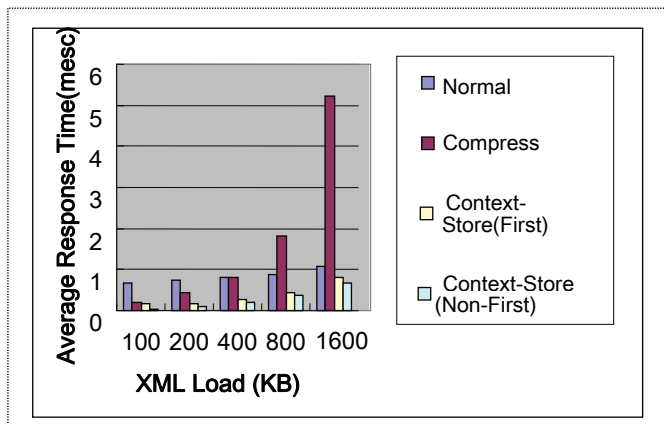

Fig. 7. Comparisons under Wireless LAN

Fig. 8. Comparisons under mobile computing environment

We packed several SOAP messages in the length of 100, 200, 400, 800, 1600 Kilo Bytes with the contents of Production ID, material, tested date and so on. Under the methods of normal SOAP transmission, Compressing and our Context-Store transmission, all the average response time increases as the length of the SOAP message augments. But apparently, our Context-Store approach has the least time cost compared with the other 2 methods. For the Compressing method, due to the plenty of time consumed by CPU and the limited processing ability, the performance becomes worse even though it cost less time in data transmission. For the Context-Store approach, owing to the only dynamic part of SOAP message transmission, the average response time reduces. In other words, our approach greatly enhances the performance of SOAP message transmission efficiency.

6. Application

Based on the above design and experiments, the prototype system has been implemented and applied to production lines in a manufactory, shown in Fig. 9. In the manufactory,
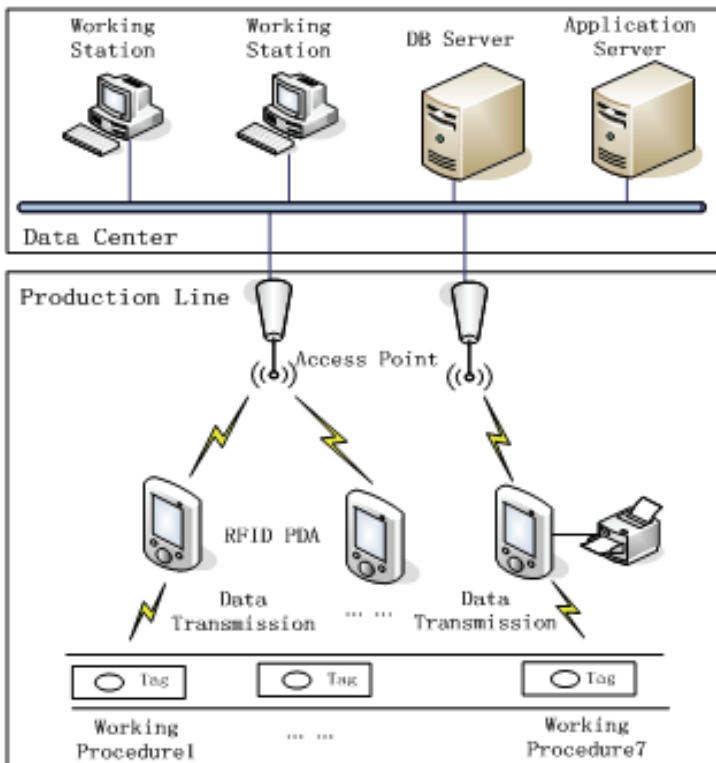

Fig. 9. Application example

considering the noisy surroundings, the limitations of temperature and humidity and the difficulty of network cabling, we choose PDA with RFID embedded communication module as readers rather than wired RFID readers. The PDA access LAN through Access Point (AP) at the frequency of 2.4GHz.While the embedded communication module exchanges data with tags at the frequency of 902 MHz which is also of free Industrial Scientific Medical (ISM) band. So there is no radio frequency interference. Other application softwares are deployed as follows: working station installs Microsoft Server 2003 operating system, Message Queue Component and Dot Net Framework2.0. The application server installs Internet Information Services 6.0 as WEB server.

In such application scene, workers read information of products with PDA in their hands from 1.0 meters away and record important process information into tags. Meanwhile, through WLAN, By virtue of Web Services, the PDA clients access application server to update process data. With our proposed approach, the performance of data exchange is improved and the production efficiency is increased.

7. Conclusion

In this paper, we introduce the widely applied RFID middlewares with the technique of Web Services. More importantly, we design and realize a Context-Store approach to improve the performance of data transmission between mobile client and Web Services server. The experiments show our approach greatly reduces the average response time of SOAP messages, thus achieve its original goal. What's more, the application example of the production lines in manufactory indicates an increase of the production efficiency. However, the symmetrical Context-Store in both mobile client and Web Service server may lead to data inconsistency. Our future work will focus on exploring a more effective storage structure or seek for a way of keeping data consistency.

8. Acknowledgments

9. References

B S Prabhu ; Xiaoyong Su & Harish Ramamurthy. (2006). WinRFID:A Middleware for the Enablement of Radio Frequency Identification (RFID) Based Applications. In: *Mobile, Wireless and Sensor Networks: Technology, Applications and Future Directions* . John Wiley, 2006.

Christian Floerkemeier & Matthias Lampe.(2005). RFID middleware design: addressing application requirements and RFID constraints, *Proceedings of 2005 joint conference on Smart objects and ambient intelligence: innovative context-aware services: usages and technologies*, page :219-224, ISBN:1-59593-304-2, Grenoble, France, 2005, ACM New York.

Clemens Kerer; Schahram Dustdar & Mehdi Jazayeri.(2004). Presence Aware Infrastructure Using Web Services and RFID Technologies. *Proceedings of the ECOOP Workshop*, 2004.

Han Chen; Paul B. Chou; Sastry Duri; Jeffery G. Elliott & Johnathan M. Reason. (2005). A Model-Driven Approach to RFID Application Programming and Infrastructure Management, *Proceedings of IEEE International Conference on e-Business Engineering* .

Julio Fernandez;Ana Fernandez & Jose Pazos. (2005). Optimizing web services performance using caching, *Proceedings of the International Conference on Next Generation Web Services Practices*, 6 pages, 2005.

K Devaram & D Andresen. (2003). SOAP Optimization via Parameterized Client-Side Caching, *Proceedings of the IASTED International Conference on Parallel and Distributed Computing and Systems*, page : 785-790. Marina Del Reg, CA, 2003.

Mike Nikitas. (2003). Improve XML Web Services' Performance by Compressing SOAP. URI: http://www.dotnetjunkies.com/Article/466   30   AE   2-1C79-4D5F-827E-6C2857FF1D23.dcik, 2003.

Niranjan & Aura Ganz. (2004). REALMS-RFID Enabled Animated Space. *Proceedings of International Conference on Communication and Computer Network* , MIT, MA.

Noah Mendelsohn; Mark Nottingham & Hervé Ruellan.(2004). XML-binary Optimized Packaging W3C Working Draft. URI: http://www.w3.org/TR/2004/WD-xop10-20040608/, 2004, 06.

Seshasayee B; Schwan K& Widener P. (2004). SOAP-binQ: High-Performance SOAP with Continuous Quality Management, *Proceedings of the 24th International Conference on Destributed Computing System*, page : 158-165.

Taesu Cheong & Youngil Kim. (2005). RFID Data Management and RFID Information Value Chain Support with RFID Middleware Platform Implementation , In: *On the Move to Meaningful Internet Systems 2005: CoopIS, DOA, and ODBASE, Editors: Agia Napa, Cyprus*, page : 557-575, Publisher : Springer Berlin, ISBN : 978-3-540-29736-9, Heidelberg Germany .

Toyotaro Suzumura;Toshiro Takase & Michiaki Tatsubori. (2005). Optimizing web services performance by differential deserialization, *Proceedings of the IEEE International Conference on Web Services*. page:185-192,2005.

V Prabakar; Dr. BV Kumar & SV Subrahmanya. (2006). Management of RFID-centric business networks using Web Services, *Proceedings of the Advanced International Conference on Telecommunications and International Conference on Internet and Web Applications and Services*, page 133.

World Wide Web Consortium. (2007). SOAP Version 1.2 Part 1: Messaging Framework (Second Edition), W3C Recommendation 27 April 2007. http://www.w3.org/TR/soap12-part1/ . Editors: Martin Gudgin, Marc Hadley & Noah Mendelsohn etc.

World Wide Web Consortium. (2008). Extensible Markup Language (XML) 1.0 (Fifth Edition) W3C Recommendation 26 November 2008. http://www.w3.org/TR/REC-xml/   Editors:Tim Bray, Jean Paoli & C. M. Sperberg-McQueen etc.

Young-II Kim; Joo-Sang Park &Tae-Su Cheong. (2005).Study of RFID middleware framework for ubiquitous computing environment, *Proceedings of 7th International Conference on Advanced Communication Technology*, page: 825-830, DOI: 10.1109/ICACT.2005.246078, Korea,July,2005, Seoul, Korea.