A Novel Authentication Protocol suitable to EPC Class 1 Generation 2 RFID system

Junsong Zhang[1], Wendong Wang[1], Jian Ma[1, 2], Xiong Li[1]
*1, Corresponding author *State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications Beijing, China*
2, Wuxi SensingNet Industrialization Research Institute, Wuxi, China
zhangjs2002@sohu.com

Abstract

RFID, capable of non-contact automatic identification using the small, low-cost RFID tags, is taking the place of barcodes to become electronic tags of the new generation. EPCglobal Class-1 Generation-2 specification (Gen2 in brief) has been approved as ISO18000-6C for global use, but the identity of tag (TID) is delivered in plaintext which makes insecurity. Several solutions have been proposed based on Cyclic Redundancy Check (CRC). Due to the bad properties of the CRC function used in the protocol; the claimed security objectives are not met. In this paper, we propose a novel authentication protocol based on Gen2 for low-cost RFID tags which use the Pseudo-Random Number Generator (PRNG in brief) function instead of the CRC function. The advantages of the novel authentication is that the proposed protocol could withstand de-synchronization attack, disclosure attack and cloning attack, furthermore, it also could provide anonymity and mutual authentication.

Keywords: *RFID, EPCglobal Class-1 Generation-2, Privacy, Security*

1. Introduction

Radio frequency identification (RFID), a rapid growing technology for automated identification of objects and people, consists of three elements: a tag, a reader, and a database [1]. The reader accesses the information contained within the tag via radio transmission, and delivers the information to the database as an index, then the reader can retrieve the corresponding record from the database. There are three kinds of RFID tags: passive tags, semi-passive tags and active tags. In this paper, we focus on the passive tags due to their low cost and promising future. However, with no built-in power supply, it induces electricity by radio wave transmitted from the reader to send back the information kept inside. So, it comes with shorter transmission range.

EPCglobal class-1 generation-2 (Gen2 in brief) [2] was approved as international standard ISO18000-6C in July 2006. It is widely believed that Gen2 tags will be the mainstream during the developing of RFID applications. Since the limited computation and memory capacity, A Gen2 tag only supports Pseudo-Random Number Generator (PRNG) and simple Cyclic Redundancy Code (CRC) computation, but cannot support conventional cryptographic functions, such as one-way hashing, symmetric encryption, or public key algorithms. That makes the designing of the security protocol for Gen2 become even more challenging.

In the past few years, researchers have proposed some authentication protocols for Gen2 [3] [4], but these solutions more or less exist the security problems. Chien and Chen (2007) [1] proposed a mutual authentication protocol conforming to Gen2. However, Due to the bad properties of the CRC function used in the protocol, it has serious problems. In this paper we will demonstrate the weaknesses of this protocol, and then we propose a new authentication protocol which can resist the problems existed in Chien and Chen's protocol.

The remainder of this paper is organized as follows. Section 2 gives an overview of the related works. Section 3 reviews Chien and Chen's scheme [1] and discusses their security weaknesses. Section 4 presents a new authentication scheme to resist these security pitfalls. Section 5 analyzes the security and evaluates its performance. Finally, Section 6 states the conclusions.

2. Related works

The key features of RFID systems include a lack of contact between the readers and the Tags. Moreover, the Tags have the ability of storage and processing. These properties mean that RFID tags have many possible applications. However, the technology also poses many threats to the user, some research papers have pointed out that RFID may be vulnerable to the threats as follows [1][4][5][10]:

Replay attack: The adversary could intercept the transmitted information between the tag and the reader, and then resend the information illegitimately to deceive a legitimate device and pass the authentication.

Denial of Service (DoS) attack: Some authentication protocols use the same key between the database and tag to perform the authentication process, once the information pass from the tag to the database, the database will query the records in the database to match the information. So, the attackers can intercept the transmitted information and cause the tag and the database unable to update their keys synchronously thus fails the following authentications and accesses.

Track Attack: The adversary could masquerade as the reader and send a special message to the tag, which causes the tag tracked down by the fixed value.

Forward secrecy: If the data kept in the tag is compromised by adversary later on, the tag's past communications can be identified and traced from the historical communication records.

Many RFID security mechanisms for location privacy protection have been proposed in recent years. By the method used, those mechanisms can be categorized into the following two types: pseudonym and shared secret update.

Pseudonym: The aim of this method is to prevent the tag from being traced. A series of pseudonyms are pre-shared by the database and the tag. For each tag reading, the tag sends a new pseudonym to the reader. However, this method needs large memory space to store the pseudonyms and the pseudonyms need to be updated when they are all used.

Shared secret update: At the end of each tag reading, the database and the tag update the shared secret synchronously. So, at each tag reading, the tag and the database share the different key. However, if the information transmitted through the air is intercepted, modified, lost, or replayed by the adversary, the database and the tag will be unable to update their shared secret synchronously.

Gen2 is one of the most important standards proposed by EPCglobal. Some companies like Philips and Texas Instruments have undergone the production of Gen2 RFID chips. Wal-Mart also has phased in Gen2 while phasing out Gen1 since 2006[6]. However, restrained by its cost and resource, Gen2 is incapable of supporting complex operations like symmetric encryption, public encryption, and hash function. It only supports some simple operations. The supporting operations are as follows:

• *PRNG*：Pseudo Random Number Generator.

• *CRC* (Cyclic Redundancy Code): To produce checksum code to verify the integrity of the transmitted information.

• *XOR*：Exclusive OR.

Nowadays, many scholars have proposed a number of security solutions on the Gen2. Although Gen2 does not support traditional encryption algorithm, we still have the potential to improve their safety. Juel (2005) proposed a protocol which is free from being cloned and spoofed [13], but it can not solve the eavesdropping and privacy issues.

Since the communication between the tag and reader is open and insecure, Karthikeyan and Nesterenko [14] had proposed a protocol using simple *XOR* and matrix operations to protect the information from being identified. Nevertheless, the transmitted information is vulnerable to tampering, which makes it suffer from DoS attacks, replay attacks and man-in-the-middle-attack. Duc et al [4] developed a simple authentication protocol by using *CRC* function, *XOR* operations and a random number to protect the information transmitted in the channel. However, if attackers can intercept the "End Session" at the final communication step, the backend server will not update the old key in its database. Therefore, the keys between database and tag are out of asynchronous which incurs DoS attacks. Furthermore, the adversary could intercept the transmitted information M_1 and M_2, and *XOR* these two values to eliminate the protection of key K_i that causes the failure of forward secrecy.

Chien and Chen (2007) [1] then improved the scheme invented by Duc et al. [4] and Karthikeyan et al. [14] to provide stronger privacy and security properties. However, their scheme still has space for improvement in terms of performance efficiency and data security.

3. Security analysis of Chien and Chen's scheme

3.1. Review of Chien and Chen's protocol

In this section, we briefly review Chien and Chen's authentication scheme. The notations used in this paper are listed as follows:

EPC Electronic product code, each Tag has the unique EPC number.

$DATA$ The corresponding record for the tag kept in the database

K_i The authentication key stored in the tag for the database to authenticate the tag at the $(i+1)th$ authentication phase

P_i The access key stored in the tag for the tag to authenticate the database at the $(i+1)th$ authentication phase

K_{old} The old authentication key kept in the database

K_{new} The new authentication key kept in the database

P_{old} The old access key stored in the database

P_{new} The new access key stored in the database

x The value kept as either new or old to show which key in the record of the database is found matched with the one of the tag

$A \rightarrow B$ A forward a message to B

N_A The random number generated by device A

$A \oplus B$ Message A is XORed with message B

$CRC(A)$ To produce the checksum code of A

$PRNG(A)$ To produce Pseudo Random Number based on the seed A.

The information kept within respective devices:

The Tag kept K_i, P_i, EPC, and the Database kept $K_{old}, P_{old}, K_{new}, P_{new}, EPC, DATA$

We illustrate the normal operation procedure of Chien and Chen's scheme as in Figure 1. The interactions between the tag, the reader and the database are described as follows.

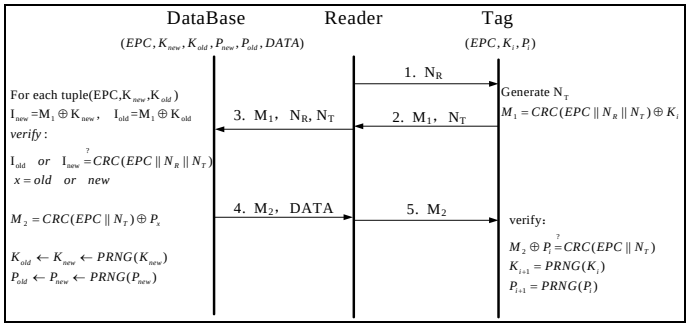

Figure 1. Chien and Chen's authentication protocol

1) Reader→Tag: The reader generates a random number N_R as a challenge and sends it to the tag.

2) Tag→Reader: When the tag receives N_R, it generates random number N_T, computes the response value M_1=CRC (EPC||N_T||N_R) ⊕K_i, and then forwards the two values back to the reader.

3) Reader→Database: Together with N_R generated in step 1, the reader forwards the received N_T and M_1 to the database.

4) Database→Reader: Upon receiving the incoming authentication request, the database iteratively retrieves key values (K_{new}, K_{old}, P_{new}, and P_{old}) from each tuple in backend server. Then, the database computes the $I_{new}=M_1 \oplus K_{new}$ and $I_{old}= M_1 \oplus K_{old}$, and checks whether I_{old} or I_{new} matches CRC(EPC||N_T||N_R) computed by the database itself. This process is iteratively repeated for each entry

until it finds a match. Then mark the value of x as old or new depend on which key (K_{old} or K_{new}) in the database is found matched.

If the database finds the matching entry, it computes $M_2 = CRC(EPC \| N_T) \oplus P_x$ and sends it together with DATA of the matching record to the reader, and updates the shared symmetric key value $P_{old} = P_{new}, K_{old} = K_{new}, K_{new} = PRNG(K_{new})$ and $P_{new} = PRNG(P_{new})$ through the PRNG function.

If the database does not have to carry out a successful match, then give up the connection.

5) Reader→Tag: Reader retrieves DATA and forwards M_2 to Tag. The tag then performs a XOR operation on M_2 and its own P_i, and verifies whether the $M_2 \oplus P_i$ and computed value CRC(EPC$\|$ N_T) are identical or not. If both values are the same, the tag updates the record kept inside by replacing K_{i+1} with PRNG(K_i), P_{i+1} with PRNG(P_i) for next access.

3.2. Weaknesses of Chien and Chen's protocol

After studying Chien and Chen's authentication protocol, we have identified several weaknesses of their protocol. The major problem about Chien and Chen's protocol is the use of the CRC function. Due to their linearity, CRC functions have some properties that, from the security point of view, can label as bad. For a detailed description of the problem, we give a theorem and a corollary about the CRC function:

Theorem 1. For any CRC (independent of its divider polynomial) and for any values a, b, c and d $\in$ $F_2[x]$, it holds that:

$$CRC(a \| b) \oplus CRC(c \| d) = CRC(a \oplus c \| b \oplus d) \quad (1)$$

Before we proof this theorem, we introduce the other properties about CRC function [17].

(1) $CRC(a \oplus b) = CRC(a) \oplus CRC(b)$

(2) $CRC(a \| b) = CRC(a << n) \oplus CRC(b)$

While a and b represent arbitrary values and n is the bit-length of b. And then, we could proof the theorem.

Proof. Without loss of generality, it is assumed that n is the bit-length of a, b, c and d.

On the one hand, $CRC(a \| b) \oplus CRC(c \| d) = CRC(a << n) \oplus CRC(b) \oplus CRC(c << n) \oplus CRC(d)$,

On the other hand, $CRC(a \oplus c \| b \oplus d) = CRC((a \oplus c) << n) \oplus CRC(b \oplus d)$

$= CRC(a << n) \oplus CRC(c << n) \oplus CRC(b) \oplus CRC(d)$

So, $CRC(a \| b) \oplus CRC(c \| d) = CRC(a \oplus c \| b \oplus d)$

Corollary 1. In particular, if in Equation (1) we have a = c, then:

$$CRC(a \| b) \oplus CRC(a \| d) = CRC(a \oplus a \| b \oplus d) = CRC(b \oplus d) \quad (2)$$

According to the above theorem, we can say that Chien and Chen's protocol does not guarantee the non-impersonation of legitimate tags. In order to accomplish this attack, the attackers only need to listen to the information between the reader and the legitimate tag.

1) Reader → Tag : N_R

2) Tag → Reader : $M_1 = CRC(EPC \| N_T \| N_R) \oplus K_i, N_T$

At this point, the attacker isolates the legitimate tag, so he has the following message: M_1, N_R, and N_T, with this information, the adversary should be able to rebuild message when queried by the reader. Although the adversary does not know the secret information stored in the tag (EPC, K_i, P_i), message M_1' could be easily calculate as described below. We know from the Corollary 1, we get:

$$M_1 \oplus M_1^{'} = CRC(EPC \| N_R \| N_T) \oplus CRC(EPC \| N_R^{'} \| N_T^{'}) = CRC(N_R \oplus N_R^{'} \| N_T \oplus N_T^{'})$$

So, message M_1' can be obtained easily by doing an XOR between M_1' and the even though he does not has the value of EPC. Therefore, the identity of a legitimate tag could be easily impersonated.

Although the author claims that the proposed protocol can resistance DoS attack, In case that if the message M_2 is intercepted, tampered or missing up to twice, the database will have no matching old authentication key and access key to complete the mutual authentication that incurs DoS attacks. For example, in the first round of the authentication, the authentication key and access key in the tag should be able to match the new authentication key and access key in the database just right. But if the message M_2 intercepted which leaves the tag unable to update the keys, at the second access, the

authentication key and access key in the tag will just have to match the old authentication key and access key in the database. In this access if the message M_2 intercepted again, the tag will unable to update the keys keep inside for the second time. While at that moment, the old authentication key and access key in the database has been renewed. As a result the database possesses no matching keys to proceed with the authentication any longer.

In addition to the above presented security weaknesses, Chien and Chen's protocol does not guarantee the location privacy of the tags too. We assume that an adversary act as a reader to communicate with the tag, the tag will response the message $M_1 = CRC(EPC \| N_R \| N_T) \oplus K_i$ to the reader, since the adversary does not know the keys of the tag, the adversary could not authentication with the Tag and the keys stored in the tag unchanged. At this point, the adversary could send another challenge to the tag, the tag will response a message $M_1^{'} = CRC(EPC \| N_R^{'} \| N_T^{'}) \oplus K_i$ again, at this moment, the attacker can verify if answers arise from the same tag by means of Equation (2):

$$M_1 \oplus M_1^{'} = CRC(EPC \| N_R \| N_T) \oplus K_i \oplus CRC(EPC \| N_R^{'} \| N_T^{'}) \oplus K_i = CRC(N_R \oplus N_R^{'} \| N_T \oplus N_T^{'})$$

Because the adversary knows the rand number N_R, N_R', N_T and N_T', the attacker will able to carry out track attack.

4. Our proposed protocol

In this section we introduce a new derived mutual authentication scheme to achieve RFID system requirements for data security and privacy protection. Our scheme is designed to accommodate the EPC Gen2 standard. As previous proposed schemes, we assume that the communication channels between the reader and the tag are insecurity while the communication channels between the readers and the backend server are secure. Due to the fact that, in practical applications, the reader usually has more computing power and the connection between the reader and database is often wired. So, we believe that this assumption is reasonable. There are two phases in the proposed protocol: System Initialization phase and Normal Authentication Operation phase.

4.1. System Initialization

The manufacturer generates random values for K_0 and P_0 respectively, and performs to store these various values in the tag's memory. We take K_0 and P_0 as the initial value of the secret information. And then the corresponding record in the database is $(K_{old} = K_{new} = K_0, P_{old} = P_{new} = P_0)$.

4.2. Second-order headings

The authentication phase is depicted in Figure 2. And the detailed steps of the authentication phase are described as follows.

1)Reader→Tag: The reader generates random number N_R as a challenge and forwards it to the tag.

2)Tag→Reader: When the tag receives the challenge N_R, it generates random number N_T, computes the response values $M_1 = PRNG(K_i \oplus N_R \oplus N_T), D = N_T \oplus K_i$, and then the Tag forwards the two values back to the reader.

3)Reader→Database: Together with N_R generated in step 1, the reader sends the received M_1 and D to the database.

4)Database→Reader: Upon receiving the incoming authentication request, the database iteratively retrieves key values $(K_{new}, K_{old}, P_{new}, P_{old})$ from each tuple in backend server. Then, the database computes the values $I_{new} = D \oplus K_{new}$ and $I_{old} = D \oplus K_{old}$, then checks whether $M_1 = PRNG(K_{new} \oplus N_R \oplus I_{new})$ or $M_1 = PRNG(K_{new} \oplus N_R \oplus I_{old})$. This process is iteratively repeated for each entry until it finds a match. Then mark the value of x as old or new depend on which key (K_{old} or K_{new}) in the database is matched.

If the database finds the matching entry and x = new, then the Database calculates $M_2 = PRNG(EPC \oplus N_T) \oplus P_{new}$, and sends it together with the field DATA of the matching record to

the reader, then the database updates the shared symmetric key value $P_{old} = P_{new}, K_{old} = K_{new}$, $K_{new} = PRNG(K_{new})$ and $P_{new} = PRNG(P_{new})$ through the PRNG function.

If the database finds the matching entry and x = old, then the Database calculates $M_2 = PRNG(EPC \oplus N_T) \oplus P_{old}$, and sends it together with the field DATA of the matching record to the reader ,while the database save the shared symmetric key value $K_{old}, K_{new}, P_{old}$, and P_{new} directly.

If the database does not have to carry out a successful match, then the Database gives up the connection.

5)Reader→Tag: Reader retrieves DATA and forwards M_2 to Tag. The tag then performs a XOR operation on M_2 and its own P_i, and verifies whether the value $M_2 \oplus P_i$ and the computed value $PRNG(EPC \oplus N_T)$ are identical or not. If both values are the same, the tag updates the record kept inside by replacing K_{i+1} with PRNG (K_i), P_{i+1} with PRNG(P_i) for the next access.

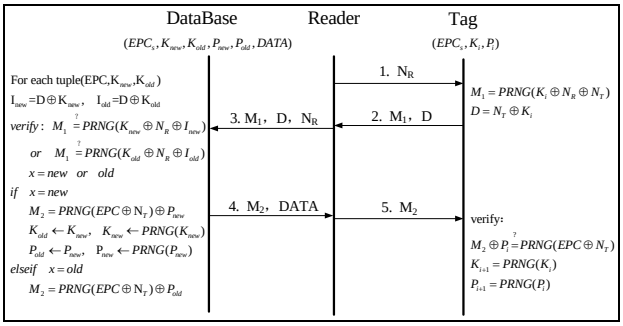

Figure 2. Our proposed protocol

On the Database side, if the value of variable x is old, it means that the Tag and the Database have lost synchronization, and the value of variable P_i stored in the Tag is not update. Therefore, the Database side does not need to be updated the value of variable P_i again in this scenario. We only need to use P_{old} calculate M_2 and deliver it to the Tag. On the contrary, in Chien and Chen's scheme, regardless of the value of variable x is old or new, they all still do the following operations: $P_{old} = P_{new}, K_{old} = K_{new}, K_{new} = PRNG(K_{new})$ and $P_{new} = PRNG(P_{new})$. If the Database and the Tag lost synchronization twice, they will not communicate with each other anymore. In our scheme, this situation would not arise.

5. Performance and security analysis of proposed protocol

Due to the bad linear properties of the CRC functions, Chien and Chen's authentication protocol cannot achieve the security objectives they claimed. In this paper, we develop a new protocol which uses the PRNG function to instead of CRC function. The PRNG function which we used is generated by linear congruential method [2]. The following is the formula:

$R_{i+1} = (a * R_i + b) \bmod N$.

Where a, b, and N is the parameters of PRNG function, R_0 is the seed of this function. The PRNG-generated random sequence determined by the seed, that is, different random seeds will produce different sequences, while the same seed will produce two identical sequences. The pseudo-random number which generated by Gen2 RFID tags has the following properties [2].

1) Probability of a single RN16: The probability that any RN16 drawn from the RNG has value RN16=j, for any j, shall be bounded by 0.8/216 < P (RN16 = j) < 1.25/216.

2) Probability of simultaneously identical sequences: For a Tag population of up to 10,000 Tags, the probability that any two or more Tags simultaneously generate the same sequence of RN16s shall be less than 0.1%, regardless of when the Tags are energized.

3) Probability of predicting an RN16: An RN16 drawn from a Tag's RNG shall not be predictable with a probability greater than 0.025% if the outcomes of prior draws from the RNG, performed under identical conditions, are known.

So we can take advantage of PRNG function in the RFID systems very well. The performance of the Tags and the Reader will be good too.

In the last part of this section, we will analyze the proposed mutual authentication scheme and compare it with previous works based on the following security criterions.

5.1. Data security

Data security in RFID systems tends to focus on the data secrecy of messages transmitting between tags and readers. In our proposed protocol data security is achieved by only transmitting bit-scrambled (XORed) or transformed (PRNG function generated) data message such as M_1, D, and M_2. So, the adversary could not to get the secret values kept in the tag or the database. Although N_R is transmitted in plain text format, it is a random-generated one-time-valid number and performs meaningful computation to generate M_1. Even though the number can be modified or eavesdropped, the security of the meaningful data M_1 and D will not be compromised, since the random number N_T is not transmitted in the air ever.

5.2. Replay attack

When the tag and databases interact with each other, the random numbers N_T and N_R will being generated. These numbers are used to protect the transmitted information to keep from replay attacks, since the attackers do not know the value of the random numbers in advance. So, the attackers can not insert the old message in the new round of sessions.

5.3. Track attack

In each access, we use different random numbers N_T and N_R to compute the transmitted messages M_1 and D, so, the malicious attackers cannot easily trace a specific tag since there are no consistent clues revealed in each tag's response. Furthermore, we use PRNG function to instead of CRC function. The PRNG function has such good properties that the adversary can not to use M_1 and M_2 to calculate a fixed number to trace the tag any more.

5.4. DoS attack

In Chien and Chen's protocol, we could see that the database keeps the old values of tag's authentication key and access key (K_{old} and P_{old}) just once then they are renewed. But in case that M_2 is intercepted, tampered or missing up to twice, the database will have no matching old authentication key and access key to complete the mutual authentication. In our scheme, we design a checking mechanism. If the matching record in the database is found by matching up by the old secret, which means an asynchronous update occurs. In this case, the values of (K_{old}, P_{old}, K_{new}, and P_{new}) will be kept the same instead of being replaced by the new values. This is a design highlight of our scheme.

5.5. Forward security

In the proposed scheme, after each successful access, the keys kept in the tag will be updated using the PRNG function. The attacker could not use the key which is being used to recover the previous key. So even if the tag is compromised, there is no way to trace the past communications between the Tag and the Database.

6. Conclusion

The application of RFID has gradually merged into our everyday lives. As it gains on its popularity, security and privacy issues gain more and more concerns. Currently, Gen2 is the mostly applied new standard for passive tags. In this paper we have conducted a thorough analysis on the Gen2 conforming

protocol proposed by Chien and Chen, and then present a new mutual authentication scheme for RFID systems. Our scheme improves the data security and privacy protection for RFID systems from the previous authentication schemes and is compatible with the Gen2 standard. Furthermore, our scheme can defend against the serious replay attack and DoS attack, at the same time the scheme provides excellent privacy protection such as anonymity and forward secrecy.

7. Acknowledgement

The authors are grateful to the editor and anonymous reviewers for their valuable suggestions which improved the paper.

8. References

[1] Hung-Yu Chien, Che-Hao Chen, “Mutual Authentication Protocol for RFID Conforming to EPC Class 1 Generation 2 Standards”, Computer Standards & Interfaces 29(2), 254–259 (2007)
[2] EPCglobal, http://www.EPCglobalinc.org/
[3] Dirk Henrici, Paul Müller, “Hash-based Enhancement of Location Privacy for Radio Frequency Identification Devices using Varying Identifiers”, In: PerSec 2004. Workshop on Pervasive Computing and Communications Security at IEEE PerCom 2004, Orlando, Florida, USA PERCOMW (March 14-17, 2004)
[4] Nguyen Duc, Hyunrok Lee, Kwangjo Kim, “Enhancing Security of EPCglobal GEN-2 RFID Tag against Traceability and Cloning”, In The 2006 Symposium on Cryptography and Information Security, Hiroshima, Japan (January 17-20, 2006)
[5] Daewan Han, Daesung Kwon, “Vulnerability of an RFID authentication protocol conforming to EPC class 1 generation 2 standards”, Computer Standards and Interfaces, 31(4), 648–652.
[6] ABI Research (2007b). RFID markets stay strong: ABI Research expects 21% annual growth through 2012. http://www.businesswire.com/portal/site/google/ index.jsp?ndmViewId=news_view&newsId=20071116005050&newsLang=en Retrieved 10.03.09.
[7] Hung-Min Sun, Wei-Chih Ting, “A Gen2-Based RFID Authentication Protocol for Security and Privacy”, IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 8, NO. 8, 2009
[8] N. W. Lo, Kuo-Hui Yeh, “An efficient mutual authentication scheme for EPCglobal class-1 generation-2 RFID systems”, In Proceedings of international conference on embedded and ubiquitous computing (EUC’07) (pp. 43–56).
[9] Stephen A. Weis, Sanjay E. Sarma, Ronald L. Rivest, Daniel W. Engels, “Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems”, Security in Pervasive Computing, pp. 201–212 (2003)
[10] Selwyn Piramuthu, “RFID mutual authentication protocols. Decision Support Systems”, 50 (2011) 387–393
[11] Younghwa An, Soohyun Oh, “RFID System for User’s Privacy Protection”, In Asia-Pacific Conference on Communications, pp. 516–519 (2005)
[12] Alex X. Liu , LeRoy A. Bailey. “PAP: A privacy and authentication protocol for passive RFID tags”, Computer Communications 32 (2009) 1194–1199
[13] Sindhu Karthikeyan, Mikhail Nesterenko, “RFID security without extensive cryptography”, In Proceedings of the 3rd ACM workshop on security of ad hoc and sensor networks (SASN’05) (pp. 63–67).
[14] Pedro Peris-Lopez, Julio Cesar Hernandez-Castro, Juan M. Estevez-Tapiador, Arturo Ribagorda, “Cryptanalysis of a novel authentication protocol conforming to EPC-C1G2 standard”, Computer Standards and Interfaces, 31(2), 372–380.
[15] He Jialiang, Ouyang Dantong, Ye Yuxin, "An Efficient Lightweight RFID Authentication Protocol for Low-cost Tags", AISS, Vol. 3, No. 9, pp. 331 ~ 338, 2011
[16] Daewan Han, Daesung Kwon, “Vulnerability of an RFID authentication protocol conforming to EPC Class 1 Generation 2 Standards”, Computer Standards & Interfaces 31 (4) (2009) 648–652.
[17] Seonghun Ahn , Byoung Seob Park, "Design and Implementation of RFID Middleware System for Ubiquitous Learning Environment using Large Scale Data", IJACT, Vol. 1, No. 2, pp. 73 ~ 80, 2009