The enhancing of RFID privacy and security with mutual authentication mechanism

Yuan-shaing Lo[#1], Henry Ker- Chang Chang[#2]

Graduate Institute of Information Management, Chang Gung University
Tao-Yuan, Taiwan 333, ROC

[1]doublelys@gmail.com

[2]changher@mail.cgu.edu.tw

Abstract— **In recent years, the deployment of the RFID system has become increasingly sophisticated and has resulted to many applications. However, the existence of some RFID privacy and security issues still need to be resolved. In this article, we propose a secure RFID system based on reduced cost and resource constraints, there is still effective against a variety of attacks and threats of mutual authentication of the protocol. The RFID systems can ensure that the information in the transmission or exchange, which can be more secure to protect privacy and confidentiality. For future development, researchers not only continued to improve the RFID system components performance but also enhancing the security and privacy protection mechanism.**

Keywords— **FRID, Mutual authentication, privacy, security.**

1. INTRODUCTION

In recent years, radio frequency identification (RFID) technology has been maturing and many applications can already be found from a wide range of developments [2]. The RFID has identification and contactless features and its management brings a lot of commercial advantage. Thus, all industries want to use the RFID system that can bring about more developments and applications. In 2003, the market leader of Wal-Mart in the USA divided the deadline of their demands for 100 major suppliers of goods so that all of them will use the RFID tags to improve the supply chain management performance for Wal-Mart. This initiative will depend on the RFID for the supply chain management. ABI research [1] reports that there will be an increase in the global market value for RFID to almost 12,000 millions by 2011 in global market. Hence, the prosperous development of RFID can lead to many more applications and production. In the near future, there will be more opportunities for the use of direct and indirect contact with life using the RFID technology. What we understand is that RFID will use the existing wireless networks to integrate the establishment of the ubiquitous network environment and provide more convenience for life.

Although the RFID contactless and identifiable features can effectively improve management performance, there are still a several of RFID security or privacy issues that need to be resolved. In the RFID systems, the tag is through the RFID readers and issued by the radio frequency signal when the tag receives the signals for collection and accumulation of energy, and then sends a specific message to release the information in response to the readers. However, we are unable to confirm the data message security service, i.e., it cannot guarantee the information received, or that the message is correct. In other words, the security of the communication environment is not guaranteed. We must have more security and protection on the privacy of a secret mutual authentication protocol in order to effectively fight a variety of attacks and threats. It is very difficult for the tags to be provided with a normal encryption algorithm, such as a public key cryptography of RSA or DES etc., the complexity of computing calculations is very large [17].

Moreover, previous studies have shown that the communication channel between readers and tags is insecure and hence, the requirement for protection is easily noticed. In short, under an insecure environment of communications and an insecure connection among the reader, the database and tag have to be protected [7]. In this article, we propose a secure RFID system based on reduced cost and resource constraints, but still effective against a variety of attacks and threats on the mutual verification of the protocol. The RFID systems can ensure that the information during the transmission or exchange can be made more secure in order to protect privacy and confidentiality.

In our approach, we conformed to the low-cost tag considerations and an enhanced security and protection based on defense mechanisms against attackers such as counterfeiting, eavesdropping, the man-in-middle attack, replay attack, or DoS attack. In order to prevent from the illegal readers or fake tags, we provide a method consisting of the following:

1. Mutual authentication.
2. Protect data privacy.
3. Protect location privacy.
4. Application of low cost tag.
5. Lower database loading

2. Related Works

There had many papers of RFID technology published before. The following sections would be introduced to the RFID system component, characteristics of RFID technology, how applications of RFID in life and RFID security requirements.

2.1. Components

The RFID system has three main components: the reader, the tag, the database. The tag and the reader communication are through radio frequency [11, 13, 15].

2.1.1. The Database

The database stores some information of product such as name, amount, date or so on, the information content of the object or subject can be found. Only the tags have been proved, the query of a database can be exhibited. Therefore, the RFID system can be widely used in a variety of areas, the provisions of goods or staffs identification can be understood.

2.1.2. The Tag

The tag can be attached to objects belonging to the mainly constituted by the antenna and microchip that can store information, easy operation and sends a message. The main sub-types of tags to distinguish into active tag and passive tag of two types.

The active tag includes a battery to connect with reader directly. The communication range in active tag is very large. On the other hand, passive tag has not battery and power supply was supported by the reader. The communication of range is very narrow to the passive tag.

2.1.3. The Reader

The RFID reader is a device that is used to interrogate an RFID tag. The reader has a specific radio frequency signal through an antenna which will have its own frequency signal media. In the RFID system, the reader does to receive a reply message of the tag, and send a message to the database.

2.2. Security Requirements

RFID systems are vulnerable to threats and attacks. Some security requirements are described in this section.

2.2.1. Anonymity

In the RFID system process of transmission, identifier is specially noticed vulnerably. In addition, the attacker can expose to the use of fake ID in the system. In the past, some researchers had proposed to use effectiveness the scheme to protect the anonymity of the ID issues [3, 8]. Therefore, the RFID system must have the ID anonymity.

2.2.2. Individual location privacy

RFID tags may be subjective to monitoring by the threat. If the tag has sent the same message, attacker will be able to grasp a specific tag with the owner. As long as the search for specific information, attacker will track or monitor [3, 9]. Contactless connection in RFID system is not being aware of their surveillance and tracking. This belongs to the individual location privacy.

2.2.3. Forward Secrecy

In order to reduce the cost of tags and limited resources, the attacker may have the opportunity to compromise and get on the tag of data. Even if an attacker can compromise to obtain relevant information on the tag, forward security can ensure that an attacker can not track the tag of information in the past [3, 12]. In other words, the attacker gets the moment information, but the attacker can not find that in the past or the future data. So, this concept is very important for RFID.

2.2.4. Against Replay Attack

The attacker wants to collect or intercept messages, then resend to the receiver at an appropriate time. Replay attack for some information has happened between the tags and readers. The attacker may try to get the message between tags and the readers [10, 14, 16]. When the attack replays the message later on, the receiver can not really understand which one is the true one. Therefore, for fixed information on the transmission would cause several security issues.

2.2.5. Against Man in the Middle Attack

It means is because of interruption communication both sides messages transmission, and the modify message or compile new message resent to the receiver. Therefore, different with replay attack mode, and does directly change the messages. Attacker can hold and modified the all messages to communicate with tags and readers [2, 5].

2.2.6. Against Denial-of-Service attack

An attacker can divide the secret data shared between the tag and the server by simply dropping or sending a forged message [3, 10]. Using information stored in database, an attacker can update the tags to secret private key. The attacker can send the forged messages to tag illegally. DoS attack can update the secret private key method and can cause a lot of problems.

2.3. The Review of Previous Researches

Duc *et al.* [6] proposed simple cryptography operations of the scheme, and conform to Gen2 tag standards. This scheme is based on the tag and the server of symmetric and synchronization session key. Therefore, it prevents cloned tags and fake readers to read the malicious and illegal access.

However, this scheme cannot effectively protect the privacy and security of the tag, because the tag is symmetry between the servers of the key. In the final step, the reader sent at the same time "end session" to the tag and the server. If one of the "end session" command is intercepted, then both session key will be out of asynchronous. Therefore, the tag and the server would not be authenticated with each other. DoS attack was successful. Hence, if the attacker compromises tag and acquire tag value (EPC, PIN, key), and prior to rely on eavesdropped and acquire values are M_1, C, r, and M_2, the attacker can trace back all past communications. Therefore, the forward secrecy has leaks and risk.

Chien *et al.* [4] proposed enhancing security and conform to the EPC Class 1 Gen2 standards, and can resist the replay attack and DoS attack. Because the challenge and response change of the random number N_1 and N_2 per session, and the keys would be updated after each successful authentication. Even if compromise of the tag would out of hand tracing of the previous communications form the tag.

However, this protocol is found in several weaknesses. Chien *et al.* proposed the keys updated after each successful authentication in the protocol. The server updated access key P and authentication key K, but the adversary prevents the tag from getting its information M_2, it will not update keys of K and P. At this time, if the adversary want to use the updated key of k_{new} and operate the authentication process in step2, the database replaces tag in key K_{x_i} after the authentication. Afterward the tag and the database are unable to operate the mutual authentication process. Besides, the adversary can use a simple operation of counterfeit tags of the message in step2.

Indeed, let $X=N_1\oplus N_1'$, $Y=N_2\oplus N_2'$ and $Z=CRC(0000 \,||\, X \,||\, Y)$, computes $M_1'=M_1\oplus Z =[CRC(EPC \,||\, N_1 \,||\, N_2)\oplus K_{x\_i}]\oplus CRC(0000 \,||\, X \,||\, Y)$,so $M_1'=CRC(EPC \,||\, N_1' \,||\, N_2')\oplus K_{x\_i}$.

3. THE PROPOSED SCHEME

Due to cost reduction and other restraint, the RFID tags can not have the complexity of computing capabilities and are vulnerable to malicious attacks. This article would consider the tag issue of cost and privacy protection using a simple XOR operation to implement security protocol. For those malicious attacks, there is a mutual authentication protocol in the proposed mechanism which will be effective against a variety of attacks.

3.1. Assumptions

1. The RFID tags are passive tags, through the operation of external devices to provide energy.
2. The tag store data with the memory, and is able to operate some simple XOR operations and generate random variables.
3. Each the tag and the database use secret key, and stored in the database and tag. Another tag also stored a key communication and exchange of information on the use of the reader.

4. In the mobile environment, we can't confirm the database and reader for the secure channel.
5. Each tag each has owns different secret key K_{r1}, and the secret key does not update.

We would provide a new and simple computation complexity to the RFID system.

3.2. Parameters

TID: the identifier of the tag.
X (Meta-ID): hash of TID; it also be represented as X.
K_t: the secret key of the tag.
K_r: the reader of secret key Kri, i = 1, 2 each reader, database and tag has a different secret key. K_{ri} is the share key among the reader, the database and the tag.
K_{t_old}: the old authentication key of the tag, and stored in the database.
r: the random number value which is generated by pseudo random number generator (PRNG),ri, i = 1, 2.
ts: timestamp.
Δ_{ri}: difference of random number ri and timestamp values ts, Δ_{ri}, i=1, 2.
$\oplus$: exclusive-or operation (XOR).
$||$: concatenation.

3.3 The Proposed Scheme

In the section, the idea is originated to resist the insecure communications environment and protects the privacy. In the proposed scheme, we would describe the related dynamic confirmation approach. This scheme will protect security and privacy for low cost RFID tag. The proposed scheme is description steps as presented the Fig. 1. Then the scheme is as the following:

Step1. The reader chooses a random number r_1 and produces timestamp ts. The reader performs a XOR operation using the secret value K_{r1} with components $S=(r_1 \,||\, ts) \oplus K_{r1}$, and sends the tag.

Step2. The tag generates a random number r_2, and acquires r_1 and ts by performing a XOR operation with the secret values K_{r1} on the received values S. In the meantime, the tag produces Δr_1, the difference between the random number r_1 and the timestamp ts. The tag obtains the parameter which the reader sends, and starts to use these parameter values in replying to the reader. The tag calculates $y=r_2 \oplus K_t$, $a=(X \oplus y) \oplus \Delta r_1$ and CRC(a) separately to obtain the three values. Then it performs a concatenation operation with a, r_2 and. Finally, the tag performs a XOR operation using the secret value K_{r1} with components $m_1=(a \,||\, r_2) \oplus K_{r1}$ and $m_1'=(CRC(a)) \oplus K_{r1}$ are sends the tag.

Step3. The reader performs a XOR operation using the secret value Kr_1 whose components are m_1 and m_1'. Then the reader utilizes the secret values Kr_2 with the database to compute for $M_1=(a \,||\, r_2) \oplus K_{r2}$, $M_1'=CRC(a) \oplus K_{r2}$ and $S'=(r_1 \,||\, ts) \oplus K_{r2}$, and forwards them to the database.

Step4. The database performs a XOR calculation with K_{r2} to M_1, M_1', S', and obtains a random number r_1 and time stamp ts, which are created by the reader, and the tags operate values of a, r_2 and CRC(a). The database produces Δr_1, the difference between random number r_1 and timestamp ts. The database performs a XOR calculation with Δr_1 to $(X \oplus y)=a \oplus \Delta r_1$, and which to find database of every tag of a secret key K_t (or K_{t_old}) components of $y=r_2 \oplus K_t$ (or K_{t_old}). Hence, the database is obtain X' performs a XOR operation using value of y components are $X'=[X \oplus y] \oplus y$. The database verification X' in the database are equal and the calculation for $CRC((X' \oplus y) \oplus r_2) \underset{=}{?} CRC(a)$ based on parameter values received by the reader are compared. If X' in the database are equal and $CRC((X' \oplus y) \oplus r_2)=CRC(a)$, then the data is considered to originate from a legitimate tag.

Step5. Since the verified X' exists in the database, it produces the Δr_2, the difference between random number r_2 and timestamp ts. The database performs a XOR operation using the secret value K_t and Δr_2, which are the components of $b=(X \oplus K_t) \oplus \Delta r_2$ and $vc=CRC(X \oplus \Delta r_2)$. Afterwards, it performs a XOR operation again using the secret value K_{r2}, which is a component of $m_2=(b \,||\, vc) \oplus K_{r2}$. Finally, the database delivers m_2 to the reader.

Step6. The reader performs XOR calculations with K_{r2} on $(b \,||\, vc) =m_2 \oplus Kr_2$, using $(b \,||\, vc)$ which the reader receives from the database. Afterwards the reader performs a XOR operation using the secret value K_{r1}, which is a component of $M_2= (b \,||\, vc) \oplus K_{r1}$, and then sends them to the tag.

Step7. The tag performs XOR calculations with K_{r1} on M_2, and it obtains values $(b \,||\, vc)$, which it receives from the reader. Moreover, the tag produces Δr_2, the difference between random number r_2 and timestamp ts. The tag performs XOR calculations with Δr_2 on $(X \oplus K_t)=b \oplus \Delta r_2$

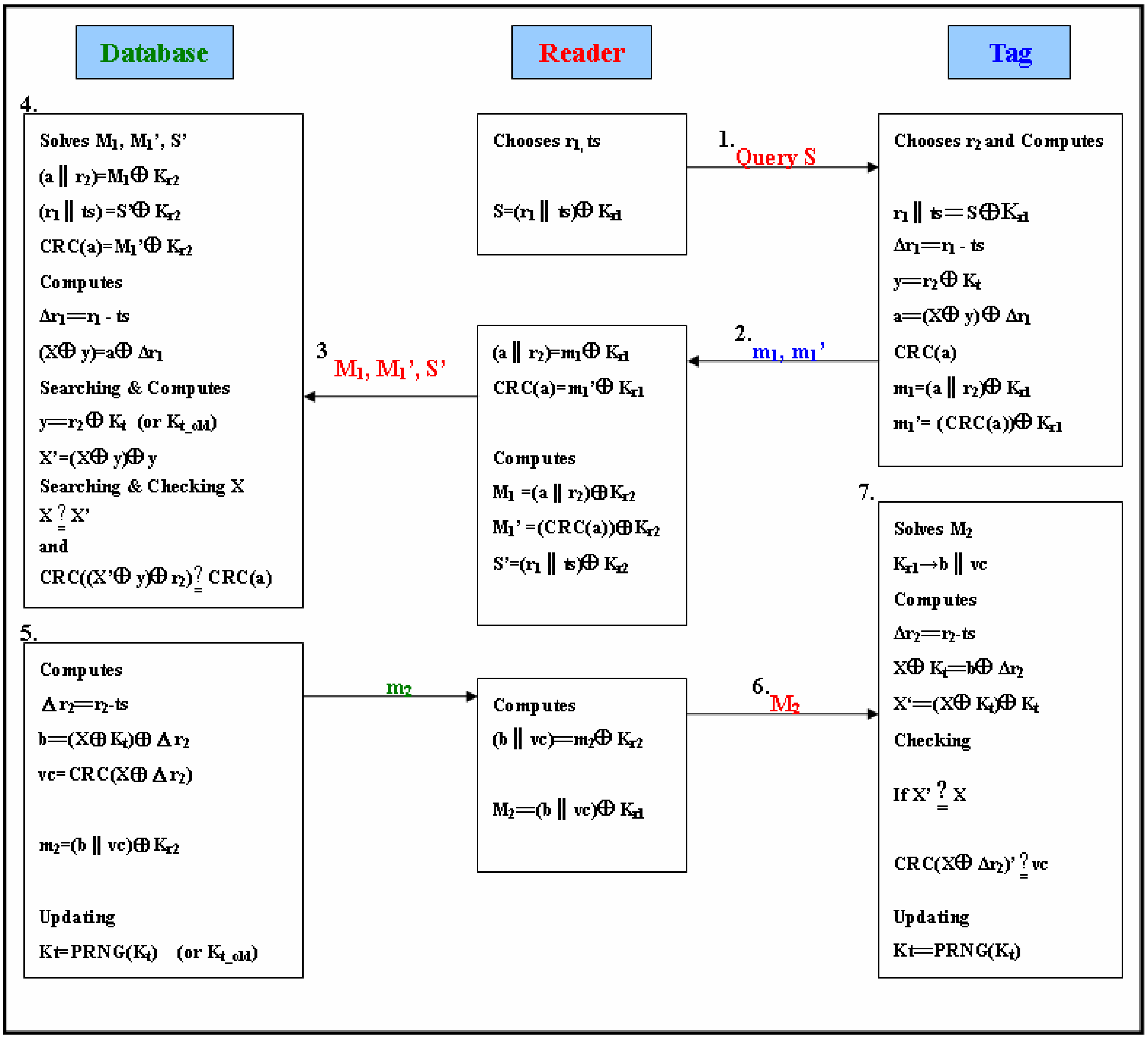

Fig.1 Diagram of the proposed protection scheme

and CRC function calculations $CRC(X \oplus \Delta r_2)$'. Then it obtains X' and performs XOR operation with K_t on $X'=(X \oplus K_t) \oplus K_t$. If the X' and tag's metaID X are equal, and $CRC(X \oplus \Delta r_2)'=vc$, then the representative is owned by the tag. Finally, the tag and the database are both updated using the secrets key K_t by PRNG.

4. SECURITY ANALYSIS

4.1. Against eavesdropping

Since the reader is between the tag and the information that is passed through the air, then malicious attackers cannot be prevented from eavesdropping. However, in our scheme the attacker cannot understand the information. Because the secret key K_{r1} (or $K_{r2)}$ to all transmitted information is encrypted. Therefore, the proposed scheme can against eavesdropping attacks.

4.2. Against spoofing

Since the tag has a MataID and a secret key, an attacker cannot access any information. In addition, when the readers and the tags transmit information, they must also use a secret key in order to communicate. Therefore, the use of counterfeit tags or theft of information is very difficult.

4.3. TID anonymity

In our scheme uses mataID, it is represented as X; mataID is hash of tag identity. The tag does not always use the real tag ID. Then we would calculate for the random values and mataID, step2 $a = (X \oplus y) \oplus \Delta r_1$ and step5 $b = (X \oplus K_t) \oplus \Delta r_2$, that it is computationally infeasible for any attacker to solve x. So that the values for every passing sessions are changing in order to make it difficult for an attacker to grasp.

In fact, in our methods used to protect the anonymity of repetitive.

4.4. Location privacy

If the tags send the fixed information or have predictable messages, the attacker can track the tags. In the proposed scheme, the tag changes the information for each legitimate reading session. Therefore, dynamic changes information in the tag is one of the advantages of the proposed scheme.

4.5. Forward secrecy

For each round, the readers and the tag will generate a random value. Thus, the mataID and the key must be calculated from random values. In addition, we will also be able to function and the CRC function of data transmission will be correct. Even if the tag has been compromised, the attacker cannot get past the transmission of information or other tag information.

4.6. Against replay attack

In our scheme, either the readers or their tag will have a random value. The transfer of all information is made only once. Indeed, each session the reader and tag will have a different random number r_1 and r_2. Therefore, every session will have to change the tag computing value $m1=(a \| r_2)\oplus K_{r1}$ and $y=r2\oplus K_t$. Hence the attacker sent the same message, the proposed scheme to against these attacks.

4.7. Against Man in the Middle Attack

In our scheme, all messages must be encrypted by K_{r1} or K_{r2}. In addition, our message and other parameters to combine must be able to calculate after the XOR operation. Even if the attacker calculates mataID X, the attacker is very difficult to presume real TID. If an attacker to modify the message, CRC function can be immediately found error. Therefore, the attacker to modify the message is very difficult in ours scheme.

4.8. Against DoS attack

The attackers attempt to use many schemes so that the communications between the tag and the database are blocked. Have asymmetric secret key is one of the ways. Thus, the database and the tag are asynchronous. However, the attacker has no way to update the tag use of secret key k_t. And since our database is maintained at a value of k_t, an obstruction can result from a malicious attack. In this case, we can still use the old k_t that is K_{t_old}, for computing.

5. CONCLUSIONS

The future RFID technology will be comprehensive and intermingled with daily life. As a result, it will be in line with low-cost elements as well as the protection of privacy and security issues will be taken into account. In this article, we have a RFID protocol in line with the future trend of strengthening the protection of privacy and security. We used a simpler calculation to reduce the burden on the tag without losing sight of the attacker who comes with a variety of threats. We considered not only the insecurity of communication channels between the database and the reader, but also the insecurity among the channels between the database and the reader. As a result, the future of RFID deployment will certainly be beneficial.

REFERENCES

[1] (2007)ABI Research, [Online], Available: http://www.abiresearch.com/home.jsp,.

[2] Chin-Ling Chen and Yong-Yuan Den "A practical RFID system: with mutual authentication and privacy protection," in *Proc. 2007 Taiwan Academic Network Conference (2007 TANET)*, 2007, pp.1-6.

[3] Yalin Chen, Jue-Sam Chou and Hung-Min Sun "A novel mutual authentication scheme based on quadratic residues for RFID systems," *Computer Networks*, Vol. 52, No. 12, pp. 2373-2380, August 2008.

[4] Hung-Yu Chien and Che-Hao Chen, "Mutual authentication protocol for RFID conforming to EPC class 1 generation 2 standards," *Computer Standards and Interfaces*, Vol. 29 , Issue 2, pp. 254-259, February 2007

[5] Tassos Dimitriou, "A lightweight RFID protocol to protect against traceability and cloning attacks," in *Proc. IEEE International Conference on Security and Privacy for Emerging Areas in Communication Networks,* 2005, pp. 59-66,

[6] Dang Nguyen Duc, Jaemin Park, Hyunrok Lee and Kwangjo Kim, "Enhancing security of EPCglobal gen-2 RFID tag against traceability and cloning," in *Proc. IEEE Symposium on Cryptography and Information Security Hiroshima* (SCIS), 2006, pp97-101.

[7] Soo-Young Kang, Deok-Gyu Lee and Im-Yeong Lee, "A study on secure RFID mutual authentication scheme in pervasive computing environment," *Computer Communications*, Vol. 31, Issue 18, pp.4248-4254, December 2008.

[8] Soo-Young Kang and Im-Yeong Lee, "A study on new low-cost RFID system with mutual authentication scheme in ubiquitous," in *Proc. 2008 International Conference on Multimedia and Ubiquitous Engineering*, 2008, pp. 527-530.

[9] Divyan M. Konidala and Kwangjo Kim, "Mobile, RFID security issues," in *Proc. The 2006 Symposium on Cryptography and Information Security*, 2006.

[10] William Knight, “RFID-another technology, another security mess?,” *Infosecurity Today*, Vol. 3, Issue 3, pp. 35-37, May-June 2006

[11] (2007)Spartan Solutions, Learn about RFID, [Online]. Available: http://www.spartan-solutions.com/learn_about_rfid/index.html, Spartan Solutions

[12] Katina Michael and Luke McCathie, “The pros and cons of RFID in supply chain management,” *in Proc. International Conference on Mobile Business (ICMB'05)*, 2005, pp. 623-629.

[13] E. W. T. Ngai, T. C. E. Cheng, S. Au and Kee-hung Lai, "Mobile commerce integrated with RFID technology in a container depot," *Decision Support Systems*, Vol. 43, Issue 1, pp. 62-76, Feb.2007

[14] T. Scott Saponas, Jonathan Lester, Carl Hartung, and Tadayoshi Kohno, “Devices that tell on you: the nike+ipod sportkit,” in *Proc. Technical report, Department of Computer Science and Engineering,* 2007.

[15] Masataka Suzukit, Kazukuni Kobarat and Hideki Imait, “Privacy enhanced and light weight RFID system without tag synchronization and exhaustive search,” in *Proc. IEEE International Conference on Systems, Man, and Cybernetics*, 2006, Vol. 2, pp. 1250 -1255.

[16] May Tajima, “Strategic value of RFID in supply chain management,” *Journal of Purchasing and Supply Management*, Vol. 13, Issue 4, pp. 261-273, December 2007

[17] Batbold Toiruul, KyungOh Lee, “An advanced mutual authentication algorithm using AES for RFID systems,” *Computer Science and Network Security*, Vol. 6, No. 9b, September 2006

[18] Yang Xiao, Xuemin Shen, Bo Sun and Lin Cai , “Security and privacy in RFID and applications in telemedicine,” *IEEE Transactions on Communications Magazine*, vol. 44, Issue 4, pp. 67-72, April 2006.