International Journal of
Electronic Commerce Studies
Vol.1, No.1 , pp.51-60, 2010

Reliable Delegation Scheme for RFID Systems

Narn-Yih Lee
Southern Taiwan University, Taiwan
Email: nylee@mail.stut.edu.tw

Zong-Jhih Lin
Email: m9490227@webmail.stut.edu.tw

ABSTRACT

Radio Frequency Identification (RFID) systems are an automatic and contactless technology. However, RFID systems also introduce new privacy and security risks. Many papers have tried to propose various RFID authentication mechanisms to solve the RFID privacy issues. In 2005, Molnar et al. first presented the property of delegation. In 2007, Fouladgar and Afifi proposed a simple delegation scheme for RFID systems. The scheme utilizes a counter to control delegation time, but it cannot do so accurately. In this paper, we aim to use the timestamp to control delegation time and enhance the security of RFID systems.

Keywords: Cryptography, Delegation, RFID, Timestamp, Security

1. INTRODUCTION

Radio Frequency Identification (RFID) is an automatic identification technology. In 2006, Juels [1] indicated that RFID has two advantages compared with barcode technology. First, each RFID tag has a unique identity (ID), while a barcode only exhibits the type of product. The unique ID can help to search for related information regarding the products, such as manufacture date or expiration date. It gives customers better support for the products. Second, RFID is an automatic system which can identify products without line-of-sight contact. Due to the above advantages, the RFID system has become an important and popular technology in 21st century.

RFID has brought much convenience to our life. For example, RFID can help customers quickly finish payment procedures. RFID also can help staffs gather inventory information and can make tracking goods as simple as possible. More and more related RFID researches and applications have been proposed in recent literature [2-6]. However, RFID systems introduce new privacy and security risks. Molnar and Wagner [7] pointed out that RFID in libraries may reveal information regarding readers' habits. Knospe and Pohl [8] indicated that passive tags are powered by the incoming signal from the reader, and transmit their identities without further security mechanisms. Attackers can utilize these identities to identify tags. In [9], Choi et al. showed that consumers need some security mechanisms to resist possible privacy abuses. Therefore, how to ensure privacy safeguards in RFID use becomes very important.

In 2005, Molnar et al. [10] proposed a new delegation scheme (MSW) that allows the backend system to delegate the ability of identifying tags to RFID readers. In 2007,

Fouladgar and Afifi [11] further proposed a Simple Delegation Scheme (SiDeS). Although both MSW and SiDeS use counters to control delegated time, it may not be very accurate. In this paper, we try to utilize the timestamp to fix the problem.

1.1 Security Requirements

The following details the security features that the RFID authentication protocol should achieve the following security features and resist some attacks.

- User Privacy: Privacy involves both anonymity and untraceability. Anonymity means that secret information should not be leaked from the tags. Untraceability means that adversaries cannot use information that tags send out to trace those tags.
- Unlinkability: Messages sent by the tag are not linkable. Thus, an adversary cannot distinguish that two messages are sent by the same tag or different tags.
- Substantive Privacy: When a tag is compromised, leaked information from the tag cannot help the adversaries to compromise other tags.
- Forward Privacy: Assume that a tag is compromised, and the secret keys are revealed. Forward privacy ensures that the messages transmitted previously will remain secure.
- Data Integrity: A DoS attack, power interruption, or message hijacking etc. may cause data loss. Therefore, the protocol must incorporate data recovery to avoid any failure.
- Delegation: The backend system can authorize others to identify tags.
- Replay attack: Through this attack, a third party can obtain some information through the eavesdropping method. Then, the third party transmits the information to the RFID reader to achieve the purpose of attacking later.
- Man-in-the-middle attack: This attack occurs when an adversary locates between a legal tag and a reader. He uses an illegal reader to obtain the communicated data transmitted by the tag. After obtaining the information, he can impersonate the legal tag to cheat any legal reader.
- Denial of Service attack: DoS attack attempts to disrupt the backend system and prevent the system from providing services to authorized users.
- Forgery attack: Using this attack, an adversary uses some method of forgery to bypass the authentication mechanism and gain access to restricted data.

1.2 Our Contributions

This paper attempts to use the timestamp to control the delegated time. The times-tamp obviously has advantages over the counter to provide more accurate authorization. Besides, the proposed protocol can satisfy the mentioned security requirements, and use pre-computation to speed up tag identification. The next section presents the proposed protocol. Section 3 analyzes the security of the proposed protocol. The final section provides concluding remarks.

2. The Proposed Protocol

2.1 RFID model and Notations

The proposed RFID system includes four entities: tags, readers, backend system, and mobile devices. The illustration is shown in Figure 1.

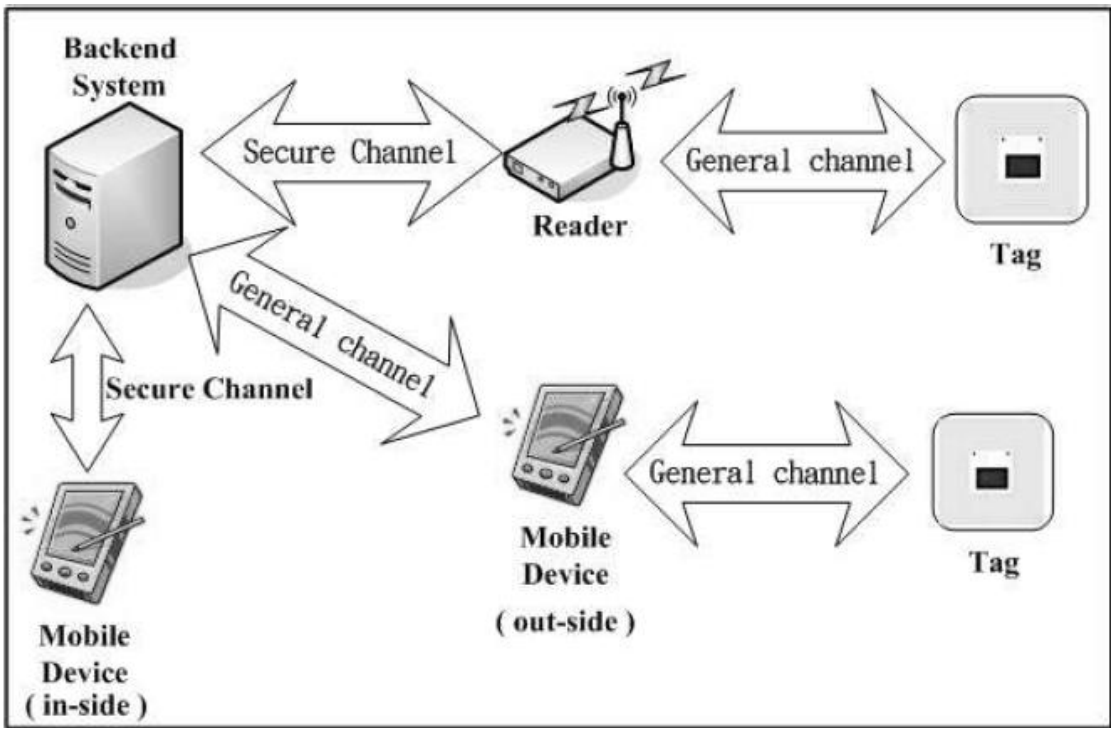

Figure 1. RFID system model

- Tag: It is a wireless transponder; its energy comes from the signal of the reader. When the tag receives the incoming signal, it will broadcast a response to the nearest reader.
- Reader: It is a transceiver; it broadcasts signals to the tags, and receives the response signals. The reader can send information via a secure channel to communicate with the backend system.
- Backend system: It is a trusted entity. We can assume that this system cannot be compromised. This system is responsible for identifying tags, and it can also go through a secure channel to communicate with the reader. The backend system can transmit information to mobile devices via a secure channel in a local location, and can transmit message to mobile devices through general channel in an out-side location.
- Mobile device: It is similar to notebooks, PDAs, and mobile phones. It acts as a reader, and it has sufficient capacity to store information from the backend system to identify tags.

2.2 Initial phase

We use the notations as summarized in the Table 1 through out the paper. The proposed protocol uses the Lamport hash chain [12] to prove the identity of the reader. Before deploying the tags, the backend system will compute a long hash chain, S_0, S_1,…, S_{top}, with a random seed a.

$S_{top} = a$,

$S_x = H(S_{x+1}) = H^{top-x}(a)$, where $x = 0, 1, \ldots, top - 1$

For example, $S_1 = H(S_2) = H^9(S_{10})$

Each tag share a unique key K_i with the backend system, and know the value S_0 and T_0 through a secure channel.

Table 1. Notations

Backend system	RFID system's backend system
Reader	RFID system's reader
RFID Tag	System's tags
$H(.)$	One-way hash function
$H^i(x)$	$H_i=H(H_{i-1}(x))$ *for* $i>1$
$H_k().$	Message authentication code with key *k*.
ID_r	Reader's identity
T_x	Timestamp in time interval *x*
T_t	The last timestamp
S_x	System's secret key in time interval *x*
K_{temp_i}	Tag's temporary key
PRNG	Random number generator

2.3 Identification phase

The proposed protocol is shown in Figure 2.

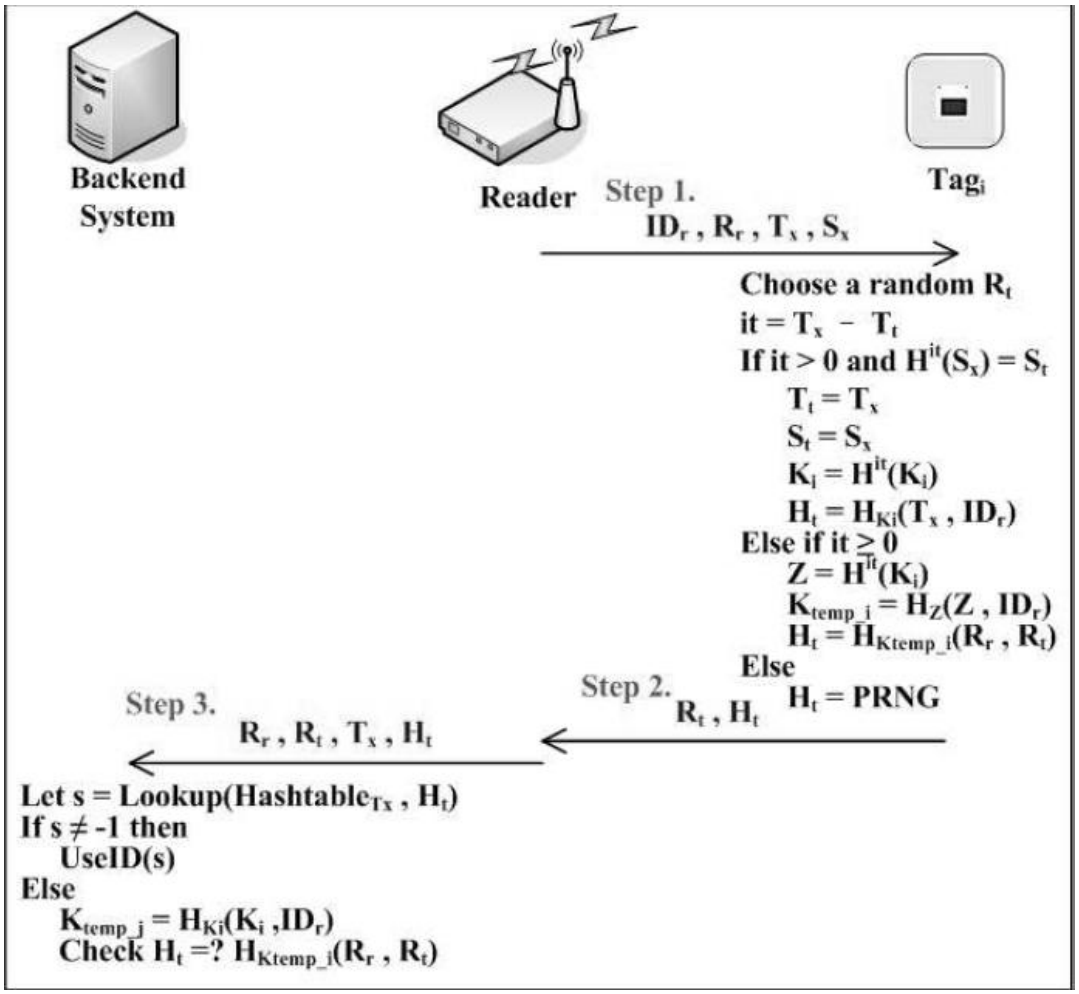

Figure 2. Identification phase

Step 1. Reader → Tag : ID_r,R_r, T_x, S_x

The reader chooses a random value R_r, and sends ID_r,R_r, T_x, S_x to the tag, where ID_r is the reader's identity. (The backend system lets all readers keep the same ID_r.) T_x is the timestamp, S_x is the system key.

Step 2. Reader ← Tag : R_t,H_t

Once the tag receives ID_r,R_r, T_x, S_x, it will compute $i = T_x - T_t$. If $i > 0$ and $H^i(S_x) = S_t$, the tag will update data, compute $T_t = T_x$, $S_t = S_x$, $K_i = H^i(K_i)$, and send $H_t = H_{Ki}(T_x, ID_r)$ to the reader. Otherwise, the tag will compute $Z = H^i(K_i)$, and use Z and ID_r to compute $K_{temp\_i} = H_Z(Z, ID_r)$. Finally, the tag computes $H_t = H_{Ktemp\_i}(R_r,R_t)$ and sends H_t to the reader.

Step 3. System → Reader : R_r ,R_t, T_x,H_t

When the reader receives R_t and H_t, it will pass R_r,R_t,T_x,H_t to the backend system. The backend system will search the look-up table (See Table 2) to find the same T_x in the rows. If the same H_t is found in the row, it means that the backend system identified the tag successfully. If the backend system cannot find the same H_t in the rows, it will use one tag's key to compute $K_{temp\_i} = H_{Ki}(K_i, ID_r)$ for each time, where K_i is the tag's key at the time interval T_x. Finally, the backend system will compute $H'_t = H_{Ktemp\_i}(R_r,R_t)$ until $H'_t = H_t$. If $H'_t = Ht$, it means that the backend system identified the tag successfully.

Table 2. Look-up table in the backend system

	K_1	K_2	…	K_n
$T_x = 1$,$K_i = H(K_i)$	$H_{1,1}$	$H_{1,2}$	…	$H_{1,n}$
$T_x = 2$,$K_i = H^2(K_i)$	$H_{2,1}$	$H_{2,2}$	…	$H_{2,n}$
…	…	…	…	…
$T_x = m$,$K_i = H^m(K_i)$	$H_{m,1}$	$H_{m,2}$	…	$H_{m,n}$

$H_{a,b} = H_{Kb}(T_x, ID_r)$, where $T_x = a$, $a = 1, 2,...m$, $b = 1, 2,...n$

2.4 Delegation phase

The proposed protocol allows the backend system to delegate mobile devices to identify RFID tags. When the backend system wants to delegate a mobile device, it will compute a delegation table (see Table 3) and send it to the mobile devices via a secure channel. The delegation table includes delegation time T_x, H_t, and K_{temp_i}, but not the tag key.

Table 3. Delegation table

	Tag_1	Tag_2	…	Tag_n
$T_x = 1$	$H_{1,1}$	$H_{1,2}$	…	$H_{1,n}$
$T_x = 2$	$H_{2,1}$	$H_{2,2}$	…	$H_{2,n}$
…	…	…	…	…
$T_x = m$	$H_{m,1}$	$H_{m,2}$	…	$H_{m,n}$

$K_{temp\_i} = H_{Ki}(K_i, ID_r)$,$H_{a,b} = H_{Kb}(T_x, ID_r)$,
where $T_x = a$, $a = 1, 2, ,...m$, $b = 1, 2, ,...n$

The tag identification phase is showed in Figure 3.

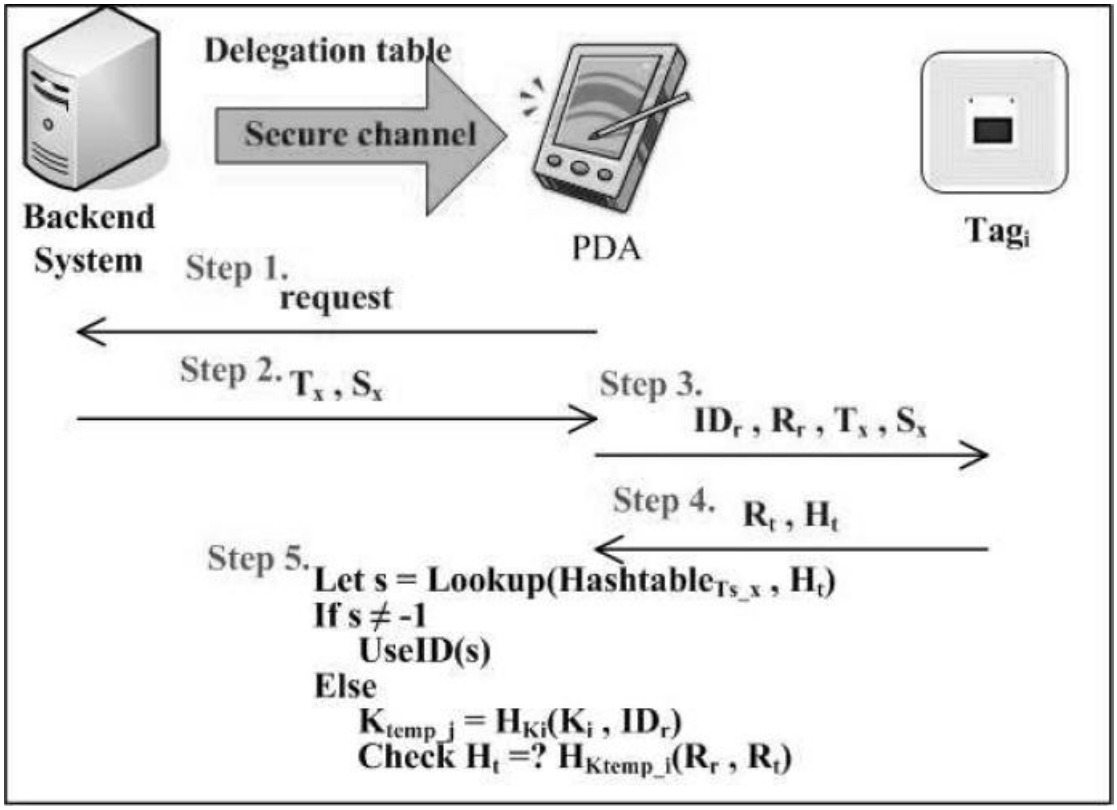

Figure 3. Tag identification phase

Step 1. Backend system ← PDA : Request

First, the PDA will send a request to the backend system.

Step 2. Backend system → PDA : T_x, S_x

Once the backend system receives the request, it will confirm the identity. If it is legal, it will send the timestamp T_x and the system key S_x to the PDA, where x is the x-th time interval.

Step 3. PDA → Tag : ID_r,R_r, T_x, S_x

When PDA receives T_x and S_x, it will choose a random value R_r, and sends ID_r,R_r, T_x, S_x to the tag, where ID_r is PDA's identity.

Step 4. PDA ← Tag : R_t,H_t

Once the tag receives ID_r,R_r, T_x, S_x, it will compute $i = T_x - T_t$. If $i > 0$ and $H^i(S_x) = S_t$, the tag lets $T_t = T_x$, $S_t = S_x$,$K_i = H^{it}(K_i)$, and sends $H_t = H_{Ki}(T_x, ID_r)$ to the PDA. Otherwise, if $i \leq 0$, the tag will compute $Z = H^i(K_i)$, and use Z and ID_r to compute $K_{temp\_i} = (Z, ID_r)$. Finally, the tag computes $H_t = H_{Ktemp\_i}(R_r,R_t)$ and sends H_t to the PDA.

Step 5. PDA identifies the tag

When the PDA receives R_t and H_t, it will pass R_r,R_t, T_x,H_t to the backend system. The backend system will search the delegation table (See Table 3) to find the same T_x in the rows. If the same H_t is found in the row, it means that the PDA identified the tag successfully. If the PDA cannot find the same H_t in the row, it will use all tags' temporary key K_{temp_i} to compute $H'_t = H_{Ktemp\_i}(R_r,R_t)$ until $H'_t = H_t$. If $H'_t = H_t$, it means that the PDA identified the tag successfully.

3. Security analysis

We analyze the security of the proposed protocol as follows:

- User privacy: In the proposed protocol, the tag generates a new response R_t and H_t for every reader query, where $H_t = H_{Ki}(T_x, ID_r)$ or $H_t = H_{Ktemp\_i}(R_r,R_t)$. The adversary cannot identify or track the tag by using the response of the tag, because R_r and R_t are random numbers, and the value of T_x will change all the time.
- Unlinkability: In the proposed protocol, the tag will generate a new response for the reader's query. An adversary is unable to distinguish whether the messages are from the same tag or not.
- Substantive privacy: When a tag is compromised, an adversary cannot use K_i to compromise other tags. That is because that all tags' secret keys K_i are different in the proposed protocol.
- Forward privacy: When a tag is compromised, it is useless for the adversary to obtain the previous information of the tag. since the tag's key will change in each time interval, where $K_i = H^i(K_i)$.
- Data integrity: Once an adversary breaks the communication between the tag and the reader, the proposed protocol can still identify the tag.
- Delegation: The proposed protocol can authorize mobile devices to identify tags.
- Resist replay attack: The adversary cannot generate a legal S_x. Hence, he only can obtain $H_t = H_{Ktemp\_i}(R_r,R_t)$. When a legal reader wants to query a tag, the reader will send a random number R_r to the tag. R_r cannot be controlled by the adversary and the tag must reply according to the random number R_r. Thus, the adversary cannot use the legal tag's response to cheat the legal reader.
- Resist man-in-the-middle attack: The adversary inserts an illegal reader between a legal tag and a legal reader to eavesdrop the communication. Those transmitted messages are unable to be distinguished without the correct K_i. Since the adversary cannot obtain the secret key K_i, he cannot impersonate a legal tag to cheat a legal reader.
- Resist Denial of Service attack: Assume that an adversary tries to break the backend system; he interrupts the signal that the mobile device generates. Although the mobile device cannot connect to the backend system, it still can identify tags. Therefore, the proposed protocol can resist a DoS attack.
- Resist forgery attack: The proposed protocol does not leak any secret information during the communication between the reader and the tag. As a result, adversaries cannot cheat the legal reader to impersonate a legal tag.

Table 4. Comparisons of security properties

	MSW[10]	RIPP-FS[13]	SiDeS[11]	Ours
User privacy	O	O	O	O
Unlinkabilty	O	O	O	O
Substantive privacy	O	O	X	O
Forward security	X	O	X	O
Data integrity	O	O	O	O
Delegation	O	X	O	O
Resist forgery attack	X	O	X	O
Resist replay attack	X	O	X	O
Resist Man-in-the- Middle attack	X	O	X	O
Resist DoS attack	X	O	O	O

4. Conclusions

In this paper, we have utilized the timestamp to control delegation time for an RFID system. The proposed protocol can resist known attacks that include replay attack, man-in-the-middle attack, DoS attack, and forgery attack, and it can delegate mobile device to identify tags. That is, the mobile RFID reader can identify tags without the on-line help of the backend system. Finally, the comparisons among the literature [10-11] and our protocol are given.

Acknowledgements

This research was supported in part by the National Science Council of Republic of China under the contract numbers NSC96-2628-E-218-002-MY2.

References

[1] Juels, RFID Security and Privacy: A Research Survey. *IEEE Journal on Selected Areas in Communications*, 24(1), 381-394, 2006.

[2] A. Juels and R. Pappu, Squealing Euros: Privacy Protection in RFID-Enabled Banknotes. Lecture Note in Computer Science Financial Cryptography 2003, 103-121, 2003.

[3] K. Finkenzeller, RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification 2nd Edition.

[4] P. C. Liao, L. Liu, F. Kuo, M. H. Jin, Developing a Patient Safety Based RFID Information System-An Empirical Study in Taiwan. IEEE International Conferenceon Management of Innovation and Technology, 2, 585-589, 2006.

[5] S. L. Garfinkel, A. Juels, R. Pappu, RFID privacy: an overview of problems and proposed solutions. Security & Privacy Magazine, IEEE, 34-43, 2005.

[6] X. Gao, Z. Xiang, H. Wang, J. Shen, J. Huang, and S. Song, An approach to security and privacy of RFID system for supply chain. IEEE International Conferenceon E-Commerce Technology for Dynamic E-Business, 164-168, 2004.

[7] D. Molnar and D. Wagner, Privacy and security in library RFID: issues, practices, and architectures. ACM conference on Computer and communications security ,210-219, 2004.
[8] H. Knospe and H. Pohl, RFID Security. Information Security Technical Report, 9(4), 39-50, 2004.
[9] D. H. Choi, T. S. Kim, and H. W. Kim, Privacy protection for secure mobile RFID service. International Symposium on Wireless Pervasive Computing, 2006.
[10] D. Molnar, A. Soppera, and D. Wagner, A Scalable, Delegatable Pseudonym Protocol Enabling Ownership Transfer of RFID Tags. in Selected Areas in Cryptography,SAC2005, 276-290, 2005.
[11] S. Fouladgar and H. Afifi, A Simple Delegation Scheme for RFID Systems (SiDeS). IEEE International Conference on RFID, 1-6, 2007.
[12] N. M. Haller, The S/KEY one-time password system. Proceedings of the Symposium on Network and Distributed System Security, 151-157, 1994.
[13] M. Conti, R. D. Pietro, L. V. Mancini, and A. Spognardi, RIPP-FS: An RFID Identification. Privacy Preserving Protocol with Forward Secrecy. International Conference on Pervasive Computing and Communications workshops, PerComW, 229-234, 2006.