International Journal of Enhanced Research in Management & Computer Applications, ISSN: 2319-7471
Vol. 4 Issue 6, June-2015, pp: (21-28), Impact Factor: 1.296, Available online at: www.erpublications.com

A Secure Mobile RFID System Design

Soonhwa Sung, Jaecheol Ryou

Dept. of Computer science and Engineering College of Engineering Software Research Center (SOREC)
Chungnam National University, Yuseong-gu, Daejeon, 305-764, South Korea

Abstract: Mobile RFID is a new application that provides a valuable service to users with mobile communication. Current RFID authentication schemes are not viable to use in mobile RFID environment. Since unlike in regular RFID environments, whereas the communication channel between the server and the reader is assumed to be secure, the communication channel between the server and reader in the mobile RFID system is not assumed to be secure. Thus, it need to study a new communication system that provides a secure privacy of mobile RFID devices. Therefore, this paper proposes a mobile RFID authentication system to provide a privacy mechanism updating confidential information in order to protect many security and privacy threats for mobile RFID devices.

Keywords: Mobile RFID, Privacy, Authentication Protocol, Process Domain, Node Domain, Network Domain.

Introduction

Radio Frequency Identification (RFID) has been widely used in many applications and is an automatic identification technology that allows remote interrogation of the ID data on RFID tags using radio frequency in accordance with wireless communication between tagged objects and RFID readers[1- 9].

Privacy preserving authentication in RFID systems is an important problem. In secure RFID systems, a reader will accept the tag’s information only after it authenticates a tag. The tag may be attached to a pharmaceutical product that carries patient information, a passport that carries a personal identification, or a commercial product that carries information about manufactured date, expiring date, ingredients, etc.

Ordinary RFID is believed that the communication channel between the reader and the database is safe. However, in the mobile RFID system, the communication channel between the reader and the database is using wireless channel, and it is not assumed to be safe. The insecure channel is vulnerable to various threats such as eavesdropping, business espionage, and tag masquerading. For this reason, the mobile RFID system has security and privacy problems are difficult and more challenging than those of order RFID system.

Recently, some authentication protocol [10-13] were proposed for secure mobile RFID systems. The proposed protocols either need additional devices, or require complex encryption and decryption calculations. They have a common inherent problem that parties in their protocol must be to share one or more secret key.

Almost all of the existing mobile RFID authentication protocol is followed traditional challenge-response mechanism. The mobile reader is sending a random challenge to the tag, then the tag is replying with its authentication message which be generated by its secret value and other random numbers. An adversary can transmit intended or meaningless requests to acquire the location key and identification information from the tag.

The adversary can anticipate the response message of the tag and can use it to perform location tracking. The tag information can be obtained by sending some intended requests.

Several schemes [14-16] has been proposed, which use only ultra-light weight, such as the random number generator, pseudo random number generator, cyclic redundancy check and exclusive-or operation, to resist the latent attacks. However, these schemes still suffer from security weakness because the schemes apply only ultra-light weight operations.

The rest of this paper is organized as follows: related work is presented in section 2, authentication system for mobile RFID device is presented in section 3, analysis is detailed in section 4, and section 5 concludes the paper.

This work was supported by the National Research Foundation of Korea(NRF) and the Center for Women In Science, Engineering and Technology(WISET) Grant funded by the Korean Government(Program for Returners into R&D by the Ministry of Science, ICT & Future Planning(MSIP)). This work was partly supported by the ICT R&D program of MSIP/IITP, Republic of Korea. [13-912-06-003, Development of Mobile S/W Security Testing Tools for Detecting New Vulnerabilities of Android]

Related Works

The mobile RFID-based applications lately become a new issue for research and development due to advantages of RFID technology and mobile smart device. However, a mobile RFID system is encountering all kinds of security and privacy threats because the communication between a reader and a database is insecure.
[17] scheme was also proposed to get rid of some security issues which are nothing but an extra device added approach. [18] scheme introduced a prototype named "watchdog tag" and [19] scheme proposed two protocols to provide low-cost RFID systems that require good operational and security properties. The first protocol of [19], in spite of very restricted functionality, resolves not only security properties, but also operational properties, the second protocol of [19] resolves the replay attack in the cost of a random number generator in tags. Moreover, these schemes have significantly reduced the amount of tag transmissions which is the most energy consuming task. [20]scheme proposed a low-cost RFID mutual authentication protocol based on the method of Hash-based Message Authentication Code (HMAC) under the assumption that hash function is secure, the property that the new protocol can achieve mutual authentication between reader and tag. [21]scheme proposed a one-way hash based low-cost authentication protocol with forward security and analyzed its efficiency, but the computation load was not taken into consideration. [22]scheme improved two lightweight RFID authentication protocols to pursue stronger anonymity property and security feature. [23] analyzed and improved lightweight RFID protocol using substring. [24]scheme proposed an effective and secured certificate mechanism using mobile devices as RFID readers together with the credit cards containing RFID tags . The result shows it can improve the existing RFID security issue under the premise of safety, efficiency and compatibility. [25]scheme proposed ultra-lightweight RFID authentication. However, the schemes did not have a mechanism to verify updated secret key between the tag and the server.

Meanwhile, a mobile phone embedded RFID reader modules will be situated anywhere and operated using many RFID tags in various RFID application systems. It is difficult to secure the privacy of a mobile RFID-enabled device without an authentication system with a novel communication protocol. Therefore, It is necessary for a new authentication system to protect against privacy threats to mobile RFID readers.

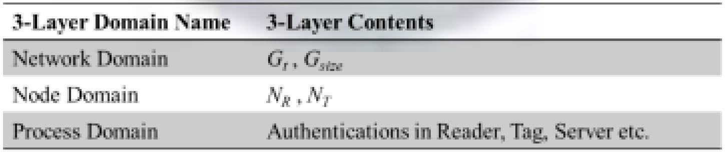
Authentication System for Mobile RFID Device

Currently, RFID authentication research cannot be used in mobile RFID environment and the authentication results in computing load to low cost tag. Therefore, to provide sufficient protection to the information privacy, this paper proposes three-layer mobile RFID authentication system for privacy protection.

A. Layer-based Mobile RFID Module

Mobile RFID system has network, process and node domain as shown in Fig.1. The mechanism constitutes functional layers for an efficient identification and each layer supports mobile RFID authentication module.
Table1 shows Three-layer of network: Network domain has group tag G_t and group tag size G_{size}. Node domain contains reader node N_R and tag node N_T. Process domain includes the authentication of reader, tag and server etc.

Table 1. Notation



3-Layer Domain Name	3-Layer Contents
Network Domain	G_t , G_{size}
Node Domain	N_R , N_T
Process Domain	Authentications in Reader, Tag, Server etc.

Network domain constitutes a group tag G_t and group tag size G_{size}. G_t denotes a group classification compliant with a purpose of tag use and G_{size} denotes the number of tag in a group. If some G_t are same purpose, G_{size} starts query by size. Network domain provides quick and correct response from the tag query by connecting the groups from a purpose of tag use.
Node domain constitutes N_R and N_T to verify updated secret keys. N_R acts to manage shared secret keys between a reader and a server and N_T acts to manage shared secret keys between a tag and a server. After setting up $ID_{deadline}$, node domain informs N_R about K_i secret key shared between a reader and a server. Similarly, it informs N_T about K_i secret key shared between a tag and a server. In addition, it verify forward secrecy for the updated secret keys of N_R and N_T.
Process domain as a core mobile RFID authentication system proceeds authentication protocol in a reader, a tag and a server.

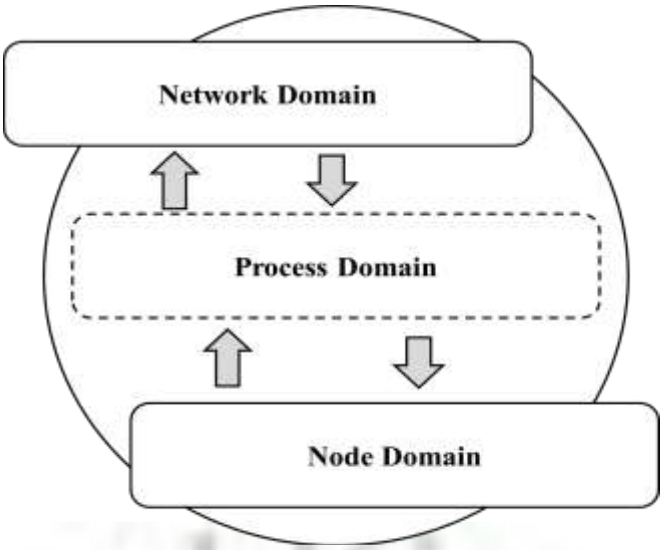


Fig. 1. Three-layer based a Mobile RFID Mechanism

In Fig.1, after process domain interacts with network domain, it can completely verify a mobile RFID system by means of node domain.

B. Mobile RFID System Authentication Phase

The proposed authentication module in Fig.2 circulates such as initialization, registration, tag authentication, secret key updating in a server, encryption, reader authentication, secret key updating in a tag and verification of updated secret key. The authentication phase supports lightweight authentication to be implemented on low-cost tags that ensure privacy protection.

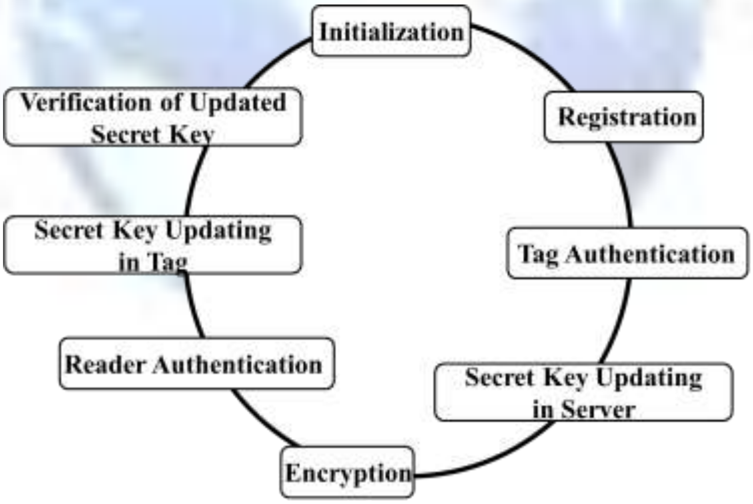
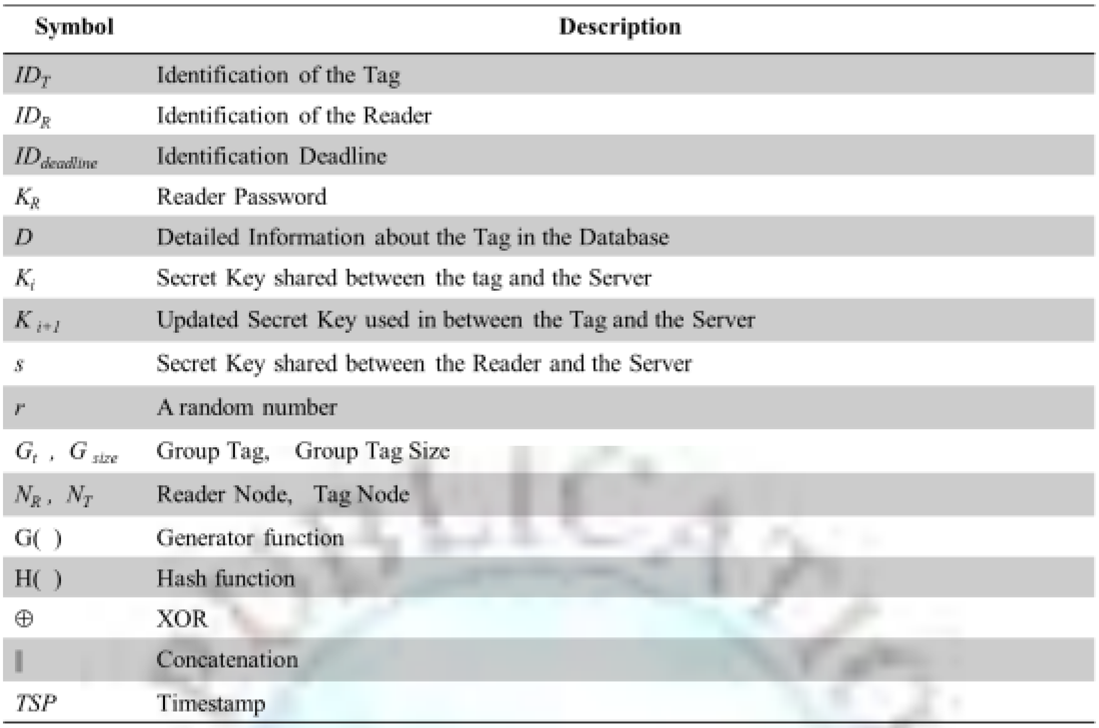

Initialization
Registration
Tag Authentication
Secret Key Updating in Server
Encryption
Reader Authentication
Secret Key Updating in Tag
Verification of Updated Secret Key

Figure 2. Mobile RFID System Authentication Phase

C. Mobile RFID Authentication Protocol

Table 2 shows the notations for the proposed authentication protocol.

Table 2. Notation



Symbol	Description
ID_T	Identification of the Tag
ID_R	Identification of the Reader
$ID_{deadline}$	Identification Deadline
K_R	Reader Password
D	Detailed Information about the Tag in the Database
K_i	Secret Key shared between the tag and the Server
K_{i+1}	Updated Secret Key used in between the Tag and the Server
s	Secret Key shared between the Reader and the Server
r	A random number
G_t , G_{size}	Group Tag, Group Tag Size
N_R , N_T	Reader Node, Tag Node
G( )	Generator function
H( )	Hash function
$\oplus$	XOR
$\|$	Concatenation
TSP	Timestamp

The mobile RFID reader must be registered and authenticated by the server. After the server has authenticated the reader, it sends ID_R and K_R to the reader. Fig.3 explains the mobile RFID authentication protocol as follows.

Initialization Phase:

1. The reader generates and stores a random number r through the use of a G( ) within the reader
2. The tag confirms its use purpose by sending a query to G_t of network domain.

Registration Phase:

3. The reader sends H (ID_R) and H ($ID_T \oplus K_i$) to the server.
4. After receiving the purpose message of tag use from G_t of network domain, the tag sends H ($ID_T \oplus K_i$) to the reader.

Tag Authentication Phase:

5. The server checks whether H ($ID_T \oplus K_i$) matches with the stored hash value of the tags. If it matches, the tag is authenticated else failed.

Update Secret Key in the Server Phase:

6. The server updates K_i to K_{i+1} where K_{i+1} =G(K_i)
7. The server sends K_{i+1} and s to N_R of node domain

Encryption Phase:

8. The server computes H ($ID_T \oplus K_i$) $\oplus K_{i+1}$.
9. The tag sends E_{KR} [D‖ H($ID_T \oplus K_i$) $\oplus K_{i+1}$] with K_R to the reader.
10. After decrypting it, the reader takes D and sends H ($ID_T \oplus K_i$) $\oplus K_{i+1} \oplus r \oplus TSP$ to the tag.

Reader Authentication Phase:

11. The tag verifies the reader by r and TSP, then it computes K_{i+1} of the updated secret key between the tag and the server using H $(ID_T \oplus K_i)$ with r.

Update Secret Key in the Tag Phase:

12. The tag updates K_i to K_{i+1}.
13. The tag sends K_{i+1} to N_T of node domain

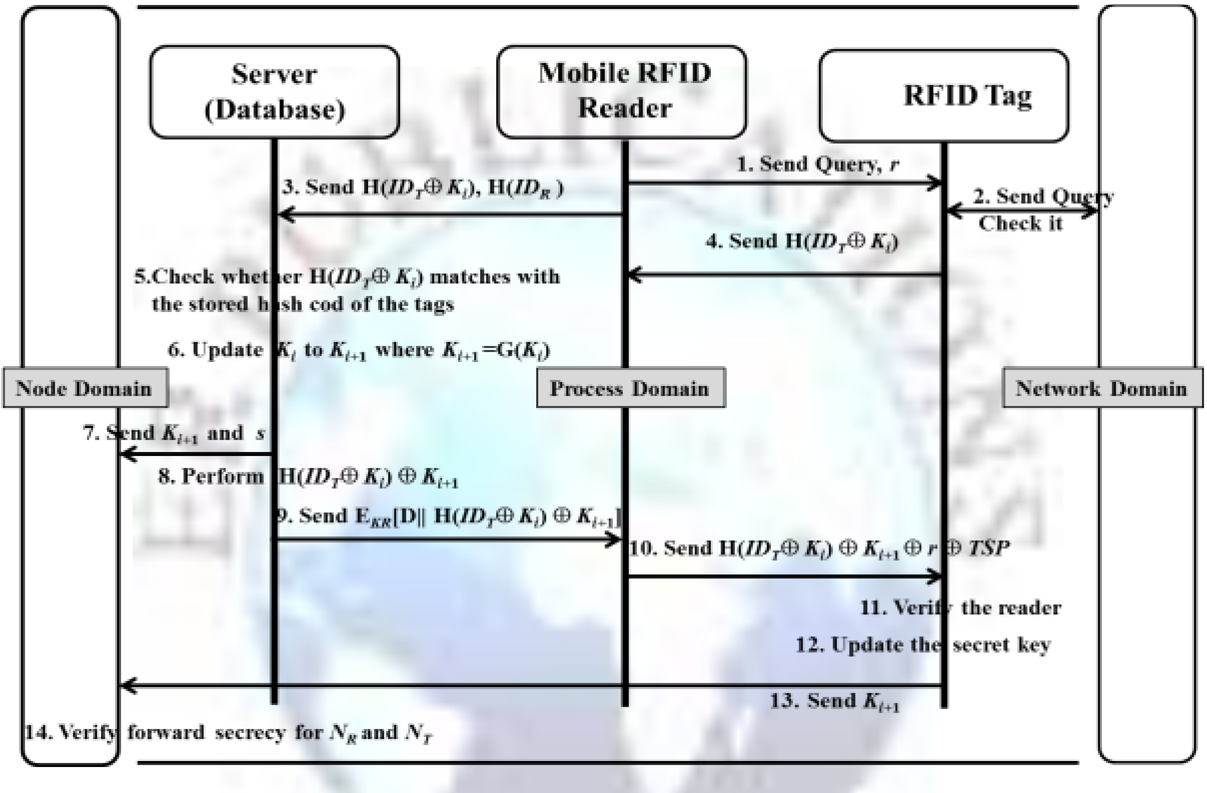

Server (Database)
Mobile RFID Reader
RFID Tag
1. Send Query, r
2. Send Query Check it
3. Send H($ID_T \oplus K_i$), H(ID_R)
4. Send H($ID_T \oplus K_i$)
5.Check whether H($ID_T \oplus K_i$) matches with the stored hash cod of the tags
6. Update K_i to K_{i+1} where K_{i+1}=G(K_i)
Node Domain
Process Domain
Network Domain
7. Send K_{i+1} and s
8. Perform H($ID_T \oplus K_i$) $\oplus K_{i+1}$
9. Send E_{KR}[D‖ H($ID_T \oplus K_i$) $\oplus K_{i+1}$]
10. Send H($ID_T \oplus K_i$) $\oplus K_{i+1} \oplus r \oplus TSP$
11. Verify the reader
12. Update the secret key
13. Send K_{i+1}
14. Verify forward secrecy for N_R and N_T

Figure 3. Mobile RFID Authentication Protocol

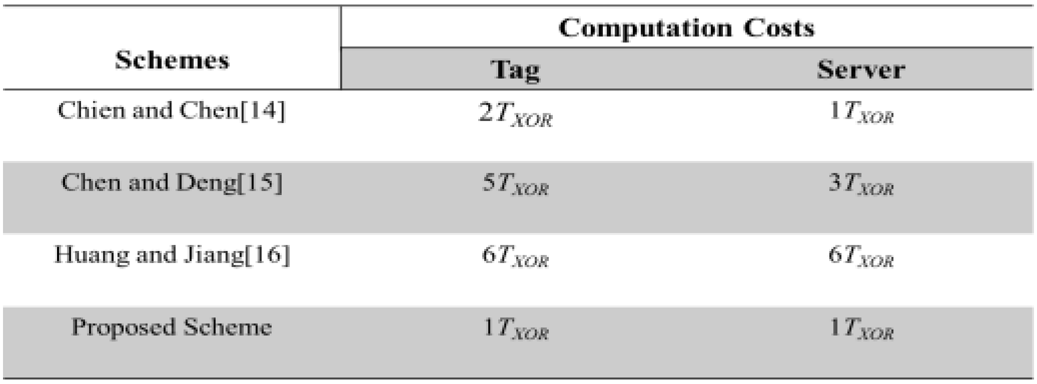
Verification for Update Secret Key Phase:

14. Node domain verifies that the updated secret keys of N_R and N_T are carried out within $ID_{deadline}$.
Updating mechanism for confidential information conforms to node domain. The server which stores old and new values of the tag secrecy communicates with node domain and node domain manages the updated secret keys. Using forward secrecy, the node domain verifies the updated secret keys of N_R and N_T within $ID_{deadline}$.

Analysis

In this section, the computation cost and security strength of the proposed method is analyzed.
Table 3 compares the proposed scheme with the related schemes in terms of the computation cost during the authentication phase. In Table 3, T_{XOR} is the execution time and the computation cost for the proposed scheme has lower computation-cost operation than other schemes.

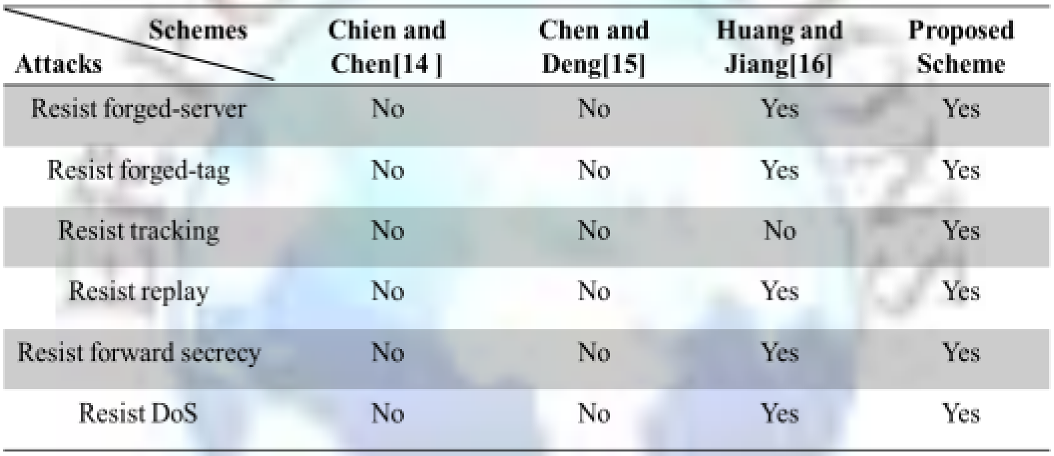
Table 3. Notation



Schemes	Computation Costs	
	Tag	Server
Chien and Chen[14]	$2T_{XOR}$	$1T_{XOR}$
Chen and Deng[15]	$5T_{XOR}$	$3T_{XOR}$
Huang and Jiang[16]	$6T_{XOR}$	$6T_{XOR}$
Proposed Scheme	$1T_{XOR}$	$1T_{XOR}$

Table 4 shows the comparisons of schemes in terms of what attacks they can resist. Huang and Jiang's scheme cannot resist the tracking attack. Chien and Chen's scheme and Chen and Deng's scheme suffer from all the attacks. However, the proposed scheme can resist all the attacks.

Table 4. Security Comparisons



Schemes / Attacks	Chien and Chen[14]	Chen and Deng[15]	Huang and Jiang[16]	Proposed Scheme
Resist forged-server	No	No	Yes	Yes
Resist forged-tag	No	No	Yes	Yes
Resist tracking	No	No	No	Yes
Resist replay	No	No	Yes	Yes
Resist forward secrecy	No	No	Yes	Yes
Resist DoS	No	No	Yes	Yes

The security of the proposed scheme against relevant attacks is analyzed as follows:

1) **Replay Attack**
The attackers can obtain outputs of the tag and transmit the eavesdropped messages to the reader. However, he cannot impersonate the legitimate tag because the outputs are different on every session due to random number *r* and *TSP*

2) **Forward Security**
The forward security means that even if the adversary obtains a current secret key, he still cannot derive the keys used for past time periods. To ensure this, verification for update secret key scheme which involves key deployment is used. For each valid session, a tag uses the current key K_i for generation and verification of authentication tags. At the end of each valid session, K_i is updated by generator function G ( ) and previous K_i is deleted. After a server sends K_{i+1}=G (K_i) to N_R, N_R confirms and manages that the current key K_i updates for forward security within identification deadline $ID_{deadline}$ at the end session. Similarly, N_T confirms and manages it. Therefore, even if the adversary obtains the current secret key, he cannot induce any previous keys due to the protection of updated secret key from node domain.

3) **Privacy Attack**
An attacker in privacy attack wants to know the query and information of a tag. In initialization and registration phase of paragraph 3.3, the query and information of a tag is protected. In addition, an attacker cannot know the query and information of a tag because the tag sends E_{KR} [D|| H($ID_T \oplus K_i$) $\oplus K_{i+1}$] with a reader password K_R to the reader in encryption phase.

4) **Tag Cloning**
Tag cloning means that the data on a valid tag is scanned and copied by a malicious RFID reader and the copied data is embedded onto a fake tag. After tag authentication and updating secret key in the server, the encryption and reader authentication by *r* and *TSP* are carried out. These mean that the tag cannot respond true values unless the tag first authenticates the reader. Moreover, they prevent a malicious reader from scanning and copying the data on a valid tag.

5) Eavesdropping

The information of proposed methods has been encoded by hash function which makes the adversary not to get the true value because of the one-way characteristic. The attackers cannot know the detailed content of the information even if they spy on the outputs. In encryption phase, the tag sends its detail in encrypted form with a reader password K_R to the reader, so the attackers cannot know the real information.

6) Denial of Service Attack

The proposed scheme needs synchronization of secret key shared between the server and the tag. In tag authentication phase, after the server checks whether H $(ID_T \oplus K_i)$ matches with the stored hash value of the tags, it updates K_i to K_{i+1}. If the adversary performs this attack on the flow the proposed protocol, he can prevent the tag from taking confirmation. This breaks the synchronization between the tag and the server because the server refreshes the tag secrecy but the tag does not. However, in the proposed protocol, the server makes itself synchronize with the tag at the situation because it stores old and new values of the tag secrecy.

Acknowledgment

The authors appreciate Prof. Cheong Youn and Eunbae Kong for their helpful research supporting.

Conclusion

The mobile RFID applications are becoming a new issue of their research and development because of the advantages of RFID technology and mobile smart devices. However, the mobile RFID system encounters various problems of security and privacy because the communication channel between the server and the reader in the mobile RFID system is not secure. If the security problems is not solved, the use of mobile RFID applications will be greatly reduced as well as the mobile RFID applications are threatened.

Therefore, the proposed scheme solves the problem of security and privacy from the unsecure communication channel between the server and the reader because of the encryption using hash functions satisfying the characteristics of the mobile RFID system such as low computation load. To discourage fraud of valid mobile reader, the updating mechanism for secret information can provide the privacy of a mobile RFID system using authentication of the tag and the reader. In addition, the proposed system verifies the updated secret key from the server, so its security is stronger than previous mobile RFID system.

As a result, the proposed system demonstrates its superiority to other related schemes in terms of computation cost and security.

References

[1]. T. Kriplean, E. Welbourne, N. Khoussainova, V. Rastogi, M. Balazinska, G. Borriello, T. Kohno, and D. Suciu, "Physical Access Control for Captured RFID Data", *IEEE Pervasive Computing*, 2007.

[2]. Y. Liu, L.Chen, J. Pei, Q. Chen, and Y. Zhao, "Mining Frequent Trajectory Patterns for Activity Monitoring Using Radio Frequency Tag Arrays", *Proc. of IEEE PerCom*, 2007.

[3]. Y. Li and X. Ding, "Protecting RFID Communication in Supply Chains", *Proc. of ASIACCS*, 2007.

[4]. B. Sheng, C. Tan, Q. Li, and W. Mao, "Finding Popular Categories for RFID Tags", *Proc. of ACM Mobihoc*, 2008.

[5]. Chiu C. Tan, Bo Sheng, and Qun Li, "How to Monitor for Missing RFID Tags", *Proc. of IEEE ICDCS*, 2008.

[6]. C. Wang, H. Wu, and N. F. Tzeng, "RFID-based 3-D Positioning Schemes", *Proc. of IEEE INFOCOM*, 2007.

[7]. C. H. Lee and C. W. Chung, "Efficient Storage Scheme and Query Processing for Supply Chain Management Using RFID", *Proc. ACM SIGMOD*, 2008.

[8]. A. Nemmaluri, M. Corner, and P. Shenoy, "Sherlock: Automatically Locating Objects for Humans", *Proc. of ACM MobiSys*, 2008.

[9]. L. Ravindranath, V. Padmanabhan, and P. Agrawal, "Sixthsense: RFID-based Enterprise Intelligence", *Proc. of ACM MobiSys*, 2008.

[10]. S. Y. Kang et al., "A Study on Secure RFID Mutual Authentication Scheme in Pervasive Computing Environment", Computer Communications, 31(18):pp.4248-4254, 2008.

[11]. Cao. T, Zhang. Y., "Cryptanalysis and Improvement of a RFID Authentication Scheme", Journal of Computational Information Systems, 5(4):pp.1177-1183, 2009.

[12]. Kejia Wu, Enjian Bai and Wen Zhang, "A Hash-based Authentication Protocol for Secure Mobile RFID Systems", The 1st International Conference on Information Science and Engineering (ICISE2009), pp.2440-2443, 2009.

[13]. Ming Hour Yang, "Lightweight Authentication Protocol for Mobile RFID Networks", International Journal Security and Networks, 5(1):PP.53-62, 2010.

[14]. H. Y. Chien and C. H. Chen, "Mutual Authentication Protocol for RFID Confirming to EPC Class 1 Generation 2 Standards", Computer Standards and Interfaces, Vol.29, Issue 2, pp.254-259, 2007.

[15]. C. L. Chen and Y. Y. Deng, "Conformation of EPC Class 1 Generation 2 Standards RFID System with Mututal Authentication and Privacy Protection", Engineering Applications of Artificial Intelligence, Vol. 22, pp.1284-1291, 2009.

[16]. Y. C Huang and J. R Jiang, "An Ultralightweight Mutual Authentication Protocol for EPC C1G2 RFID Tags", In Proc. Of 2012 International Symposium on Parallel Architectures, Algorithms and Programming (PAAP'12), pp.133-140, Dec. 2012.

[17]. Zongwei Luo, Terry Chan, Jenny S. Li, "A Lightweight Mutual Authentication Protocol for RFID Networks", Proceedings of the IEEE International Conference on E-business Engineering, pp.620-625, Oct. 2005.

[18]. C. Floerkemeier, R. Schneider, M. Langheinrich, "Scanning with a Purpose-Supporting the Fair Information Principles in a RFID Protocols", Proceedings of the 2nd International Symposium on Ubiquitous Computing Systems, pp.1-9, 2004.

[19]. Yong Ki Lee and Ingrid Verbauwhede, "Secure and Low-cost RFID Authentication Protocols", Proceedings of the 2nd IEEE International Workshop on Adaptive Wireless Networks, Nov. 2005.

[20]. Shang-ping Wang, Qiao-mei Ma, Ya-ling Zhang and You-Sheng Li, "HMAC-Based RFID Authentication Protocol", Proceedings of the 2nd International Symposium on Information Engineering and Electronic Commerce, China, pp.1-4 2010.

[21]. He Lei, Lu Xin-mei, Jin Song-he and Cai Zeng-yu, "A One-Way Hash Based Low-cost Authentication Protocol with Forward Security in RFID System", Proceedings of the 2nd International Asia Conference on Informatics in Control, Automation and Robotics, China, pp.269-272, 2010.

[22]. K.H. Yeh and N. W. Lo, "Improvement of Two Lightweight RFID Authentication Protocols", Information Assurance and Security Letters 1, pp.6-11, 2010.

[23]. He Lei, Gan Yong, Cai Zeng-yu and Li Na-na, "An Improved Lightweight RFID Protocol Using Substring", Proceedings of the 5th International Conference on Wireless Communications, Networking and Mobile Computing, China, pp.1-4, 2010.

[24]. Allen Y. Chang, Dwen-Ren Tsai, Chang-Lung Tsai and Yong-Jiang Lin, "An Improved Certificate Mechanism for Transactions Using Radio Frequency Identification Enabled Mobile Phone", Proceedings of the 43rd Annual International Conference on Security Technology, Taiwan, pp.36-40, 2009.

[25]. H. M. Sun, W.C. Ting, and K.H. Wang, "On the Security of Chien's Ultra Lightweight RFID Authentication Protocol", IEEE Transactions on Dependable and Secure Computing, pp.315-317, 2011.