Journal of Computers Vol. 27, No. 4, 2016, pp. 121-129
doi:10.3966/199115592016122704010

An Enhanced ID-Updating Hash-Based RFID Authentication Protocol with Strong Privacy Protection

Jian Shen[1234], Shaohua Chang[24], Haowen Tan[24],
Sai Ji[24], and Jin Wang[24*]

[1] Jiangsu Technology & Engineering Center of Meteorological Sensor Network, Nanjing University of Information Science & Technology, Nanjing, China

[2] Jiangsu Engineering Center of Network Monitoring, Nanjing University of Information Science & Technology, Nanjing, China

[3] Jiangsu Collaborative Innovation Center on Atmospheric Environment and Equipment Technology, Nanjing University of Information Science & Technology, Nanjing, China

[4] School of Computer & Software, Nanjing University of Information Science & Technology, Nanjing, China, PRC
s_shenjian@126.com, casaha@126.com, tan_halloween@foxmail.com, jisai@nuist.edu.cn, wangjin@nuist.edu.cn

Received 13 May 2015; Revised 13 August 2015; Accepted 22 November 2015

Abstract. RFID authentication has raised many concerns about the security risks and privacy issues due to its lightweight authentication properties. Many research achievements in RFID focus on strengthening the entire RFID system and solving the security problems. Recently, a hash-based RFID security protocol with the intension of updating the identifier of the tag in both the reader side and the tag side itself was proposed. However, there exists inherent risk in the ID-updating procedure. In the scenario that the adversary blocks the legal messages continuously for several times, the backend processing system (BPS) cannot recognize the tag due to the de-synchronization of the identifier in last several sessions. Thus the tag will be invalid and cannot be reused again. In this paper, we propose an enhanced ID-updating hash-based RFID authentication protocol with strong privacy protection. In our protocol the ID-updating procedure is resistant to de-synchronization attack. Additionally, the possible feedbacks towards different cases of the tag are taken into consideration. Our proposed protocol is proved to be effective and secure in real applications. Above all, the de-synchronization attack towards the communication between the tag and reader can be prevented according to our design. The identifier of the RFID tag is assumed to be updated with cryptographic hash functions during every session. In this way the identifier can be synchronized in both the BPS side and the RFID tag side. The location privacy of the tag can be protected in our protocol.

Keywords: de-synchronization attack, ID updating, RFID

1 Introduction

Radio frequency identification (RFID) technology has been developed for several years in the expectation for supplant of barcodes [1]. The working process of RFID system is to identify the validity of the RFID tags attached to the goods. Unlike the barcode which needs to have line-of-sight contact with the checking machine, RFID tags can be authenticated in a relatively long distance with high scanning speed [2]. The basic RFID system consists of the backend processing system (BPS), the reader and RFID tag.

* Corresponding Author

The BPS, which also acts as the verifier, is assumed to have the full authority of the entire RFID system. The BPS is assumed to be trustworthy and reliable. The BPS possesses all the secrets of the reader and tags. Note that in some existing protocols the BPS cannot communicate with the RFID tag directly. The RFID tag is arranged to be in contact with the specific reader, which acts as a bridge to alleviate the burden of BPS. This is necessary for large-scale authentication with numbers of tags and tag groups [3]. In other word, the BPS functions as a database to offer necessary information to the trusted reader [4-6]. On the other hand, the BPS checks the validity of the generated proof from the reader as the verifier.

The RFID reader, performing as the necessary channel between the BPS and tags, takes the responsibility of acquiring and gathering information from the tag and verifying its validity. For different requirements in real applications, the reader is equipped to have enough computational power [1, 7]. We would like to emphasize that the communication channel between the BPS and the reader is semi-secure [8-9]. However, with no particular restrictions on its computation, the BPS is capable of using appropriate cryptographic techniques to ensure the safety of communication between the reader and the BPS. Thus in some occasions the BPS and the reader are assumed to be one entity, which means that in this occasion the communication channel between the BPS and the reader is totally secure.

The RFID tag which can be divided into three varieties: active tag, passive tag, and semi-passive tag, is the most concerned RFID device that is vulnerable to security risks. Thanks to the recent technology progress, the cost of RFID tags has been dropped to a relatively low price. The wide promotion of RFID tags will come in a short time [2, 10]. At the same time, these low-cost tags have large probability to suffer from security attack and privacy leakage due to their limitation in computation power and storages. We assure that these security and privacy problems can be solved by adopting impeccable authentication protocols and secure strategies [1-2, 11]. That is what our researches focus on.

As a matter of fact, the communication channel between the reader and the tag is not secure. The transmitted information is vulnerable to eavesdropping as well as other kinds of attacks. For example, the RFID tag releases radio signals to the reader through the wireless channel. Thus the location of the RFID tag can be acquired by the malicious reader from eavesdropping only with small expenses. The tracing towards the tag can be possible in this occasion.

We would like to emphasize that in some protocols the BPS and the reader are considered as one entity, which is convenient in practical situation. In this situation, the BPS is designed to contact with the tag directly instead of using the reader as the bridge. However, when the number of the tags is very large, the collision between messages from different tags will affect the authentication process. The BPS has to communicate with large numbers of tags at the same time, giving relatively big burden to the RFID system. In this protocol we assume the model with just one RFID tag. Thus we also combine the BPS and the reader as one entity. We mainly concern about the synchronization problem that may occurs in the communication channel of BPS and tag. That is to say, we also consider the BPS and the reader as one entity so that we focus on solving the de-synchronization issue. When it comes to grouping authentication scenarios, then our protocol will need some modification and the idea we propose can still be effective and useful.

The concerns about the possible risks of RFID authentication have been raised in the past few years. Both the RFID system and the users of the RFID tags will be under extreme situations with the threats of information leakage. The regular authentication procedure of the RFID system may be interrupted by the adversary. The key information of the RFID tags may be detected and collected by the illegal entities. As a result, it is necessary to improve the security level of the RFID system with limited sources in RFID tags [1, 12]. In this paper we proposed an enhanced ID-updating hash-based RFID authentication protocol with strong privacy protection. Our protocol is resistant to de-synchronization attack and can provide strong privacy protection. Moreover, the identifier of the tag is designed to be updated after every session runs. In order to prevent communication blocks from the adversaries, both the BPS and the tag will check the state number ahead of time to ensure that the ID-updating of previous session is successful [13].

This paper is organized as follows. In the following section, the related original protocols are presented in brief, along with the weakness of the protocol proposed by D. Z. Sun and J. D. Zhong. The detailed scheme of our proposed protocol is described in Section 3. Next is the security analysis of the protocl in Section 4.

2 Related Work

2.1 Original RFID authentication protocols

Researches on RFID authentication has developed for many years. The RFID researching area focusing on wireless authentication towards RFID tags has been developing rapidly since 2004. In recent years, various kinds of RFID protocols have been proposed to apply with different situations. Many RFID protocols have far-reaching influence and are the base of the RFID protocols nowadays. We describe these protocols briefly below in this section.

In 2004, Juels [1, 3] proposed "Yoking proof" to solve the simultaneously scanning problem in the occasion of two tags. The main idea of yoking proof protocol is to generate a proof showing the existing of two tags at the same time. It is the first time that the researchers devote themselves to the authentication of low-cost RFID tags. Pseudo random number is adopted in yoking proof protocol in order for avoiding damaging through replay attack. However, Saito and Sakurai [2], pointed out that Yoking Proof is still vulnerable to replay attack. After that, they proposed "yoking proof using timestamp" to solve this problem. Piramuthu [5] claimed that Satio and Sakurai's proof still showed no resistance against replay attack. In 2008, "Reading order independent yoking proof" is presented [4].

In 2012, Sun and Zhong [14] proposed a hash-based RFID security protocol for strong privacy protection. As they claimed, their protocol provides strong privacy protection and manages to conduct key updating in every session run so that it is difficult for the adversary to damage the RFID system and acquire the privacy information of the tag [15-16]. The key updating section is the advancement in low-cost RFID tag authentication. The main idea of this protocol is to update the identifier by iterating the cryptographic functions.

H. Liu et al. proposed grouping-proofs-based authentication protocol [17] for distributed RFID systems. In this protocol, all the tags are divided into several groups and are sequentially checked. This protocol provides strong protection on privacy and is resistant to various attacks. However, the checking sequence of the tags is required to be arranged in advance. A RFID authentication protocol for multiple tag arrangement [8] is proposed by S. Dhal and I. S. Gupta in 2014. In the assumption multiple numbers of RFID tags are attached in one object in order to increase the detection probability.

2.2 Some problems of hash-based RFID security protocol by Sun and Zhong

The hash-based RFID security protocol proposed by Sun and Zhong has some problems that may damage the RFID system. In the protocol, the ID-updating is conducted in both the BPS and the tag, which may cause de-synchronization attack. For example, the adversary could block the third pass so that the current session run will be terminated according to the protocol. The authors were intended to design this for security consideration to prevent the BPS and the tag from tracing attack. However, when the authentication session runs are terminated unsuccessfully for certain times, the identifier stored in the tag is not updated at all [11]. Additionally, the BPS cannot identify the tag in this assumption as the BPS updates the identifier in every unsuccessful session run. As a result, the de-synchronization attack is possible in this protocol.

On the other hand, according to this protocol, the BPS is arranged to conduct complex computations and comparisons. It may works well in the occasion with single RFID tag. When it comes to the extension with multiple tags and tag groups, the BPS has to conduct vast computations and comparisons, which is not efficient for fast scanning of low-cost passive tags. As a result, the authentication protocol should considerate its extendibility in further grouping authentication scenarios.

2.3 Idea of our protocol

We proposed an enhanced ID-updating hash-based RFID authentication protocol with strong privacy protection in this paper. Our protocol is based on Sun and Zhong's protocol. The identifier of the tag applied in our protocol is updated as designed so that it will be difficult for the adversary to conduct tracing attack against the specific tag. Moreover, considering of the existing security threats and privacy risks in their protocol, we improve our protocol so that the proposed protocol is resistant to de-synchronization

attack. The main idea of our protocol is to replace the ID used as the verifying number for the RFID entities to distinguish with the others. Random number generator is available in our scheme so that every session run is different, preventing tracing problem [13]. On the other hand, the state number is designed and checked at the beginning of the authentication process. We analyze different situations that may happen in the previous session run and choose the appropriate way to deal with the updated ID. Note that the computation about hash function is more complex than that in the previous protocols.

3 Protocol Design

In this part we explain the detailed process of the proposed RFID protocol. For better explanation, we divide the entire protocol into two different phase including the main authentication phase and ID checking phase. The main authentication phase describes the entire communication passes between the BPS and the reader except for the checking of the state number. The BPS collects necessary information for authentication and exchange message with the tag mutually. As the second phase of the proposed protocol, the ID checking phase checks the state number to judge whether the previous session run is successfully terminated. Different solutions are given according to different results of the previous session. We would like to note that the structure of the protocol is based on the one in Sun and Zhong's protocol, where the BPS and the reader are considered as one entity. In addition, we describe our idea in single-tag assumption for better explanation. However, our protocol can be extended to the complex scenarios with more readers and multiple RFID tags. The notations used in our proposed protocol are provided in Table 1.

Table 1. Notations

Notation	Description
BPS	Backend processing system
r_0, r_1, r_3, r_5	Random numbers generated by BPS
r_2, r_4	Random numbers generated by tag
ID	Identifier of the RFID tag
S_k	Secret key of the RFID tag
$H()$	Cryptographic hash function
$H^i()$	Iterating the hash function for *i* times
I	Initial value of *Q*
Sync	State number for ID-updating
TempID	The temporary identifier of the tag

3.1 Main authentication phase

In this phase which is the primary part of the entire protocol, the BPS and the tag conduct several communicating passes to confirm the identity of each other as well as acquire key information for ID-updating. The receiver of the messages will check the acquired information for secure requirements. Note that the received message is assumed to be checked during every communication pass of the session. In our assumption, the ID-updating is conducted attached with the random numbers to improve the uncertainty of authentication. As we have described above, the core of our protocol is to prevent the RFID system from damage of the block attack, where the adversary is able to block the legal message to desynchronization the key information in both the reader side and the tag side.

The detailed steps of the main authentication phase are as follows:

- The BPS computes $N = H^{Q}(ID \,||\, s_k)$. After that, a random number r_1 is generated.
- The BPS computes $W = H^{r_1}(N)$ using the generated r_1.
- As soon as the BPS finishes the above computations, it sends $(Query, W, r_1)$ to the RFID tag.
- The RFID tag computes $M = H^{Q'}(ID \,||\, s_k)$ and $S = H^{r_1}(M)$, both of which are used to check if $S = ?W$.
- The RFID tag generates r_2 and computes $P = H^{r_2}(S)$.
- The message (P, r_2) is arranged to send to the BPS from the tag.

- After receiving the message form the tag, the BPS computes $A = H^{r_2}(W)$ using the acquired r_2 and the stored value of *W*.
- After that, the BPS will also check whether $A = ?P$. If this equation is proved to be right, the BPS computes $Q = r_1 + r_2 + Q$ and $TempID = H_1(A||r_1||r_2)$. Consequently the BPS generates the random number r_3 and computes $H(Q||r_3)$. Finally the BPS delivers message $(H(Q||r_3), r_3)$ to the tag.
- The tag computes $Q' = r_1 + r_2 + Q'$ and checks if the received message is right. If the message passes the verification, the tag computes $TempID' = H_1(P||r_1||r_2)$ and $C = H(LT(TempID'||r_4))$, where r_4 is the generated random number by the tag. The tag then sends (C, r_4) to the BPS.
- The BPS checks the received message and computes $D = H(RT(TempID||r_5))$ and $ID = TempID$ using the generated r_5.
- The tag checks the received message and gives out different solutions. Then $(H(D), E)$ is delivered to the BPS, which is the least communicating pass.
- The BPS checks the message and shows different results according to various situations that may happen in the authentication process.

The brief description of this phase is shown in Fig. 1.

3.2 ID checking phase

In this phase, both the BPS and the RFID tag check the value of *Sync* which functions as the state number indicating the synchronization result of the last authentication between the BPS and the tag. In other word, every communicating process of the protocol is under verification at the beginning of the next session. The main purpose of this phase is to guarantee the ID-updating process. A state value is available in our protocol which is assigned to show different condition about ID-updating. In conclusion, this phase is necessary to improve the security of the entire protocol and provides strong resistance to de-synchronization attack.

The detailed steps of this phase are as follows.

- The BPS generates random number r_0 and checks the value of *Sync* which indicates the result of last session before the main authentication phase starts. If *Sync*=1, the BPS computes $ID = H(I||s_k), Sync = 0$ and sends $("Failed", H^{r_0}(s_k), r_0)$ to the tag; If *Sync*=0, the BPS sends $("Updated", H^{r_0}(s_k), r_0)$ to the tag.
- The tag checks the value of *Sync* and the received $H^{r_0}(s_k)$. If *Sync*=0 and $H^{r_0}(s_k)$ is right, the tag checks the delivered message. $\{ID = H(I||s_k), Sync = 0\}$ is executed if the message is *"Failed"*, which means that the ID-updating in the tag is successful but the one in the BPS is failed. In this case, the *ID* of the tag will be reset to the original value $H(I||s_k)$.
- Another situation is when *Sync*=1, in this case, the *ID* of the tag will be reset to the original value $H(I||s_k)$. This case refers to the situation that the ID-updating in the tag itself is unsuccessful.
- It is necessary to note that the ID checking phase is designed to work before every session run with the intension of guaranteeing the ID-updating of the previous session run is valid so that the de-synchronization attack is prevented.

The brief description of this phase is shown in Fig. 2.

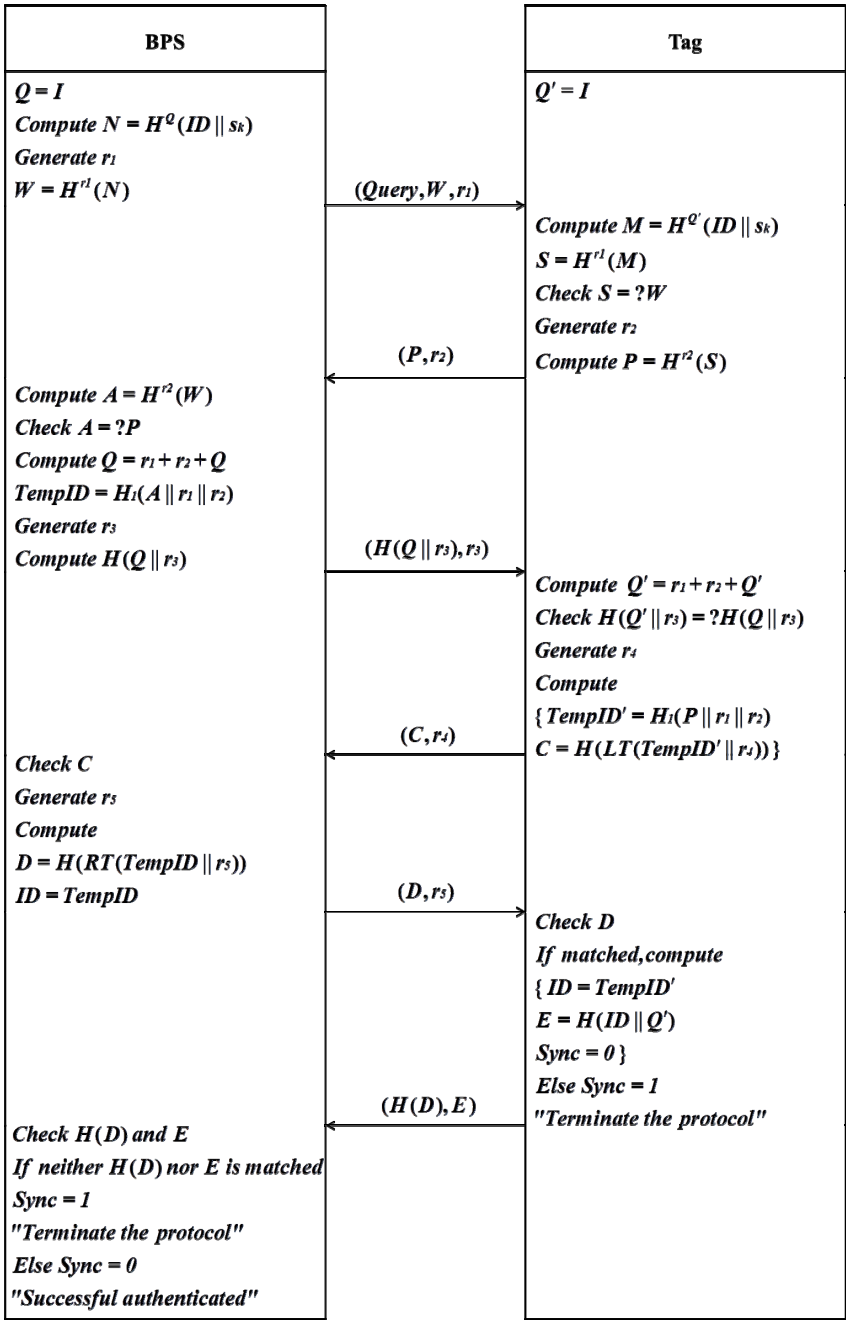

Fig. 1. Main authentication phase of the proposed protocol

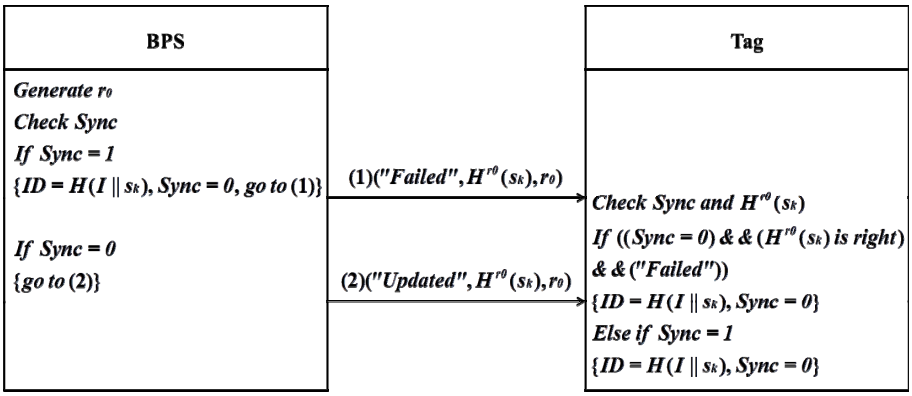

Fig. 2. ID checking phase of the proposed protocol

4 Security Analysis

In this section, we analyze the security properties of our proposed protocol in the purpose of proving that our protocol is reliable and resistant to various kinds of attacks. The entire RFID system of our protocol is effective and has large potential in the practical situations. In addition, the key information of the tag is updated in every successful session. Both the BPS and the tag are able to be informed. At the beginning of the next communication session, the two RFID entities check the state value and give out different solutions according to different results. We design effective security mechanism to prevent de-synchronization attack, which is the core of our protocol [19].

4.1 Tag anonymity

In the proposed protocol, the privacy information of the tag is well preserved. As we have described above, the identifier of the tag is updated in every session run. Moreover, random numbers are combined with the secret key during the hash functions. The adversary cannot acquire the real identity of the tag through eavesdropping. All the necessary messages are encrypted in every communication pass, which meets the practical requirement in RFID authentication [20].

4.2 Location privacy

When the tag contacts with the BPS, the location of the tag can be leaked, which may damage both the user and the RFID system. In our proposed protocol, as we have explained above, the identifier of the tag is not transmitted between the tag and the BPS. The generated random number performs as the distinction mark instead of the identifier. The identifier of the tag is temporarily available in one session [21]. After one successful authentication, the temporary identifier is updated with cryptographic hash function. In this occasion, the tracing towards the specific tag is difficult for the adversary. Hence the location privacy of the tag can be protected. As a result, the protocol is resistant to tracing problem.

4.3 Replay attack

The proposed protocol is resistant to replay attack. As we know, the replay attack is possible when the reused of previous messages is available and can be accepted by the BPS. In this assumption, the adversary should successfully pass the verification using the old messages, which will not come true in our protocol. Both the BPS and the tag check the validity of the received messages at first. Note that the transmitted messages are quite different with the ID-updating mechanism and random number generator. For example, in the main authentication phase, assuming that the adversary acquires the transmitted message $(H(Q||r_3),r_3)$ from the BPS, in the next authentication session, the adversary sends $(H(Q||r_3),r_3)$ to the tag with the intension of receiving privacy information of the tag and the system. As assigned in subsection 3.1, the tag will check the received $(H(Q||r_3),r_3)$. However, in this session, both the Q and r_3 is brand new so that the adversary will not pass the authentication. On the other hand, the adversary cannot damage the system by disturbing the normal communication even if the adversary succeeds in the cheating [1, 22-23].

4.4 De-synchronization attack

This protocol is mainly arranged for solving the de-synchronization attack which is possible in Sun and Zhong's protocol. In our protocol, we give out different solutions in the subsection 3.2. Assuming that the adversary has the ability to block the messages between the BPS and the tag, the six passes are all possible to be blocked. For example, if the fifth pass which transmits (D,r_5) to the tag by the BPS after temporarily updating the *ID*, the situation is that the tag will not update the *ID* as it does not received (D,r_5) which has been blocked by the adversary. As a result, the tag will terminate the protocol and computes *Sync*=1 so that the RFID system is prevented from de-synchronization attack. So it is with the one in the last pass.

5 Conclusion

In this paper we propose an enhanced ID-updating hash-based RFID authentication protocol with strong privacy protection. We analyze the protocol proposed by Sun and Zhong and its theoretical weakness in preventing de-synchronization attack. In order to solve this problem as well as strengthen the RFID system, the proposed protocol conducts ID-updating in every session run. The ID-updating process consists of the part in the subsection 3.2, which is the verification of the last ID-updating process. As we have described above, our protocol is resistant to tracing problem and de-synchronization attack, which shows superiority in practical applications. We develop our protocol in the basic BPS and tag structure for better description. However, the entire protocol can be extended to the multiple-tags authentication as future work, which is the hotspot in lightweight RFID research area.

Acknowledgement

This work is supported by the National Science Foundation of China under Grant No. 61300237, No. U1405254, No. 61232016 and No. 61402234, the National Basic Research Program 973 under Grant No. 2011CB311808, the Natural Science Foundation of Jiangsu province under Grant No. BK2012461, the research fund from Jiangsu Technology & Engineering Center of Meteorological Sensor Network in NUIST under Grant No. KDXG1301, the research fund from Jiangsu Engineering Center of Network Monitoring in NUIST under Grant No. KJR1302, the research fund from Nanjing University of Information Science and Technology under Grant No. S8113003001, the 2013 Nanjing Project of Science and Technology Activities for Returning from Overseas, the Project of six personnel in Jiangsu Province under Grant No. 2013-WLW-012, the CICAEET fund, and the PAPD fund.

References

[1] A. Juels, RFID security and privacy: a research survey, IEEE Journal on Selected Areas in Communications 24(2)(2006) 381-394.

[2] J. Satio, K. Sakurai, Grouping proof for RFID tags, in: Proc. of the 19th International Conference on Advanced Information Networking and Applications, 2005.

[3] A. Juels, Yoking-proofs for RFID tags, in: Proc. of the Second IEEE Annual Conference on Pervasive Computing and Communications Workshops, 2004.

[4] Y. Lien, X. Leng, K. Mayes, J.H. Chiu, Reading order independent grouping proof for RFID tags, in: Proc. of IEEE International Conference on Intelligence and Security Informatics(ISI'2008), 2008.

[5] S. Piramuthu, On existence for multiple RFID tags, in: Proc. of IEEE International Conference on Pervasive Services (ICPS'06), 2006.

[6] J. Shen, D. Choi, S. Moh, I. Chung, A novel anonymous RFID authentication protocol providing strong privacy and security, in: Proc. of MINES 2010, 2010.

[7] J. Hermans, R. Peeters, B. Preneel, Proper RFID privacy: model and protocols, in: Proc. of IEEE Transactions on Mobile Computing, 2014.

[8] A. K. Singh, S. Dhal, I. Sengupta, An approach to solve tracking and message blocking problems in RFID, in: Proc. of 2014 Fourth International Conference on Communication Systems and Network Technologies (CSNT), 2014.

[9] B. Gu, V.S. Sheng, Feasibility and finite convergence analysis for accurate on-line v-support vector learning, IEEE Transactions on Neural Networks and Learning Systems 24(8)(2013) 1304-1315.

[10] H.Y. Chien, S.B. Liu, Tree-based RFID yoking proof, in: Proc. of Wireless Communications and Trusted Computing

(NSWCTC'09), 2009.

[11] C.C. Lin, Y.C. Lai, J.D. Tygar, C.K. Yang, C.L. Chiang, Coexistence proof using chain of timestamps for multiple RFID tags, in: Proc. of Advances in Web and Network Technologies, and Information Management, 2007.

[12] H. Liu, H. Ning, Y. Zhang, D. He, Q. Xiong, L.T. Yang, Grouping-proofs-based authentication protocol for distributed RFID systems, in: Proc. of IEEE Transactions on Parallel and Distributed Systems, 2013.

[13] J. Wang, X. Yang, B. Li, S. Lee, S. Jeon, A mobile sink based uneven clustering algorithm for wireless sensor networks, Journal of Internet Technology 14(6)(2013) 895-902.

[14] D.Z. Sun, J.D. Zhong, A hash-based RFID security protocol for strong privacy protection, in: Proc. of IEEE Transactions on Consumer Electronics, 2012.

[15] Z. Fu, X. Sun, Q. Liu, L. Zhou, J. Shu, Achieving efficient cloud search services: Multi-keyword ranked search over encrypted cloud data supporting parallel computing, IEICE Transactions on Communications E98-B(1)(2015) 190-200.

[16] J. Shen, W. Zheng, J. Wang, Y. Zheng, X. Sun, An efficient verifiably encrypted signature from weil pairing, Journal of Internet Technology 14(6)(2013) 947-952.

[17] J.C. Ha, J.H. Ha, S.J. Moon, C. Boyed, LRMAP: lightweight and resynchronous mutual authentication protocol for RFID system, in: Proc. of Ubiquitous Convergence Technology: First International Conference, 2006.

[18] L. Bolotnyy, G. Robins, Generalized "Yoking-proofs" for a group of RFID tags, in: Proc. of International Conference on Mobile and Ubiquitous Systems, 2006.

[19] J. Cho, S. Yeo, S. Huang, S. Rhee, S. Kim, Enhanced yoking proof protocols for RFID tags and tag groups, in: Proc. of 22nd International Conference on AINA-Workshops, 2008.

[20] X. Leng, Y. Lien, K. Mayes, J.H. Chiu, Select-response grouping proof for RFID tags, in: Proc. of First Asian Conference on Intelligent Information and Database Systems (ACIIDS 2009), 2009.

[21] J. Li, X. Li, B. Yang, X. Sun, Segmentation-based image copy-move forgery detection scheme, IEEE Transactions on Information Forensics and Security 10(3)(2015) 507-518.

[22] S. Sundaresan, R. Robin, W. Zhou, RFID tags-grouping proof with forward security, in: Proc. of 2013 IEEE International Conference on RFID-Technologies and Applications (RFID-TA), 2013.

[23] S. Sundaresan, R. Doss, W. Zhou, Offline grouping proof protocol for RFID systems, in: Proc. of 2013 IEEE 9th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), 2013.