Journal of Computers Vol. 28, No. 2, 2017, pp. 223-229
doi:10.3966/199115592017042802018

A Mutual Authentication Security RFID Protocol Based on Time Stamp

Changlun Zhang[1], Nan Ning[1], Wenqi Zhang[2], and Haibing Mu[2]

[1] School of Science, Beijing University of Civil Engineering and Architecture, Beijing, China
zclun@bucea.edu.cn ningnan@stu.bucea.edu.cn

[2] School of Electronics and Information Engineering, Beijing Jiaotong University, Beijing, China
hbmu@bjtu.edu.cn

Received 14 November 2015; Revised 07 March 2016; Accepted 28 December 2016

Abstract. In the RFID technology, the privacy of low-cost tag is a hot issue in recent years. A new mutual authentication protocol is achieved with the time stamps, hash function and PRNG. This paper analyzes some common attack against RFID and the relevant solutions. We also make the security performance comparison with original security authentication protocol. This protocol can not only speed up the proof procedure but also save cost and it can prevent the RFID system from being attacked by replay, clone and DOS, etc..

Keywords: mutual authentication, privacy security, RFID, time stamps

1 Introduction

RFID is a communication technology that can identify things quickly and accurately in automatic way using the radio frequency signal and its spatial coupling transmission characteristic, which is composed of tags, readers and server (including database). RFID system is vulnerable to attack for lacking a physical or visual contact. With the application of the RFID technology, threatens it faced become more and more serious, the protection of the security during the communication has drawn more and more attention [1-2].

In order to achieve the secure transmission of RFID system, people have proposed a lot of authentication schemes [3-6]. The two main mechanisms used in these schemes are physical mechanism and encryption mechanism. Because the physical mechanism needs extra equipments or components which brings in high cost and limited security, more and more researches focus on encryption mechanism recently which apply the mature cryptography technology into security authentication protocol in RFID. But the limited calculation and storage ability of RFID tags lead to a lot of difficulties in designing efficient security mechanism.

According to the requirements of privacy protection and deficiency of the existed protocols, we propose a new mutual authentication protocol using the timestamp and hash encryption in tag to protect the communication process between the tags and the server.

2 Relate Work

In 2003, Sarma [7] proposed Hash-lock protocol which used virtual ID instead of real ID, and then verified with hash function to prevent real information leakage. However, virtual ID did not change in the protocol and the real ID is also shown in the form of plaintext transmission. The Hash-lock protocol is vulnerable to the retransmission and impersonation attacks. To improve the security, A. Weis Stephen proposed random Hash-lock protocol [8]. Random Hash-lock protocol updates the authentication infor-

mation in the communication process through adding pseudo random number in the tag, thus the position tracking problem is resolved in a certain extent. But the real ID tags are still used in the unsafe channel, unable to resist replay and counterfeit attacks. Moreover, the cost of the protocol is high for the pseudo-random number generator and the communication overhead. M. Hash-chain proposed Ohkubo protocol in 2004 [9]. Protocol Hash-chain makes each communication information change through independent ID tag updating during the process of authentication, which have the indistinguishability and forward security. On the other hand, it is vulnerable to the retransmission and impersonation attacks due to the one way authentication and its cost is also higher because of the large amount of computation.

Tsudik proposed YA-TRAP protocol in 2006 [10]. Determine the reader's legitimacy through comparing the time stamp to protect the security of the certification process, but it is vulnerable to denial of service attacks. Luo proposed a RFID authentication protocol based on dynamic encryption algorithm in his graduation thesis [11]. The safety of the protocol is ensured by updating the random number and the new encryption algorithm is determined according to different random numbers. The attacker cannot pass the authentication of the database even though it eavesdrops successful. But there is still no good solution to eavesdropping attacks with potential safety hazard.

In 2011, Cho presents a hash-based mutual authentication protocol which is difficult for an attacker to launch successful brute-force attacks [12]. The scheme sends a random number to generate by a tag to a back-end server without disclosure, and it substitutes a random number with a secret value in a response message.

In 2013, Xu proposed a new one-way hash function based mutual authentication protocol [13]. In the schemes, access list and pseudorandom flags are adopted for quick search, to ensure good efficiency and scalability.

From the existing research achievements, most previous attention focus on increasing the complexity of the encryption method and the degree of difficulty of the attackers to decipher the information, rather than preventing leakage of private information within the label by programming with existing conditions. Hash function is very suitable for RFID authentication with fast operation, high security and relatively low cost. Therefore, more and more RFID Security Authentication Protocol based on the hash function is concerned. We adopt MD_5 algorithm as hash function in the authentication protocol here.

3 The Authentication Protocol with Time Stamp

3.1 Time Stamp

Time stamp, a variant application of digital signature technology, is the time of creation, modification and access in file attributes. The time stamp function (UNIX timestamp) mainly applied in this paper is an expression of time and its value is the total number of seconds since 1970 January 1st (00:00:00 GMT) to the current time. Therefore, the timestamp converts the time to a calculated string calculating conveniently and cannot be repeated.

3.2 Notations

In the initialization, the time stamp T0, the limit time stamp T_{max}, the unique identifier ID, and the ID_r of all valid readers are stored in tags before authentication. The unique identifier ID of each tag and ID_r of all legal readers are stored in Database.

The terms used in protocol are as follows:

- ID is the unique identifier of the tag
- ID_r is the unique identifier of the reader
- H() is Hash operation
- $\oplus$ is XOR symbol
- T is the value of the time stamp for current communication
- T_0 is the value of the time stamp for latest communication
- T_{max} is the limit value of time stamp according to the different environment settings

3.3 Protocol Process

In this section, the detailed interaction of protocol between Tag, Reader and the Database is given.

Fig. 1 shows the detailed authentication process:

1. At the beginning, reader converts the current time to time stamp T and $H(ID_r \oplus T)$ is got by a hash operation after XOR of T and ID_r.

2. Reader sends $H(ID_r \oplus T)$ and T to the tag.

3. After receiving the tag response, the reader sends $H(ID \oplus T \oplus r)$, r, $H(ID_r \oplus T)$ and T to Database for authentication.

4. After receiving data, the backend server looks for an ID_r" to see if $H(ID_r" \oplus T)$ equals $H(ID_r \oplus T)$. If there is, then tag is valid, the server/database generates a new random r_2 and calculate $H(ID' \oplus r_2)$. It sends $H(ID' \oplus r_2)$ and r_2 to Reader. Else, reader or tag is illegal and communication is terminated.

5. The reader forwards the information sent by database to the tag. The tag calculates $H(ID \oplus r_2)$ and compares if $H(ID \oplus r_2)$ equals $H(ID' \oplus r_2)$. If true, the tag updates time stamp T_0 to T. Else, database or reader is illegal, and T_0 keeps unchanged.

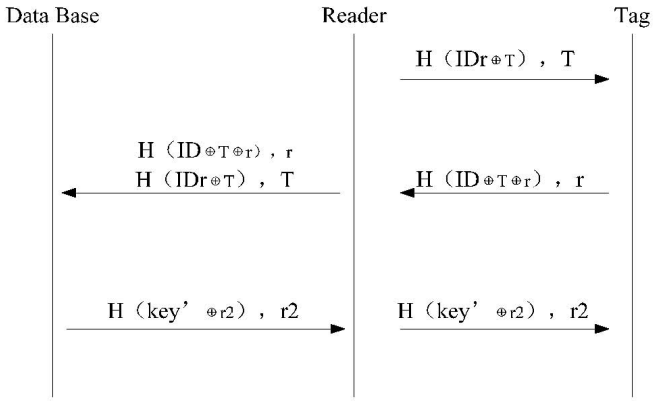

Fig. 1 The authentication process of the protocol

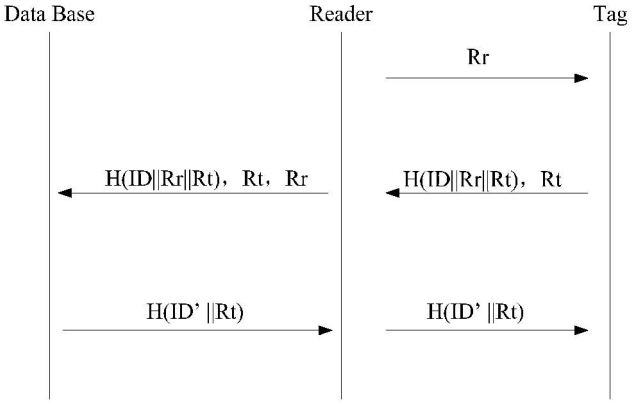

Fig. 2 The authentication process of Challenge-response protocol

4 Security and Performance Analysis

4.1 Comparison with Challenge-response Protocol

In 2005, Rhee, Kwak, Kim and Won proposed a distributed challenge-response protocol [14], which is also a mutual authentication protocol with high security. The protocol has some similarity with our proposed protocol since they are both challenge-response mode, and its security is relatively high, but there are still potential risks in it. With Rhee's protocol, the attacker can pretend a reader to send tag R_r due to

the absence of the legitimacy of the reader authentication. Therefore, the tag will continue to produce new R_t, and new R_t will cover the old R_t, so $H(ID||R_t)$ sent back by DB can't be verified. Attackers implemented the de-synchronization attack successfully and tag's computation overhead increases greatly. Our protocol sets identifier ID_r for Reader firstly, forged reader cannot verified by $H(ID_r (T) = H(ID'_r (T)$. In this paper, the time stamp of reader compares T sent by reader with T_0 and T_{max} stored in tag. Only T meets $T_0<T<T_{max}$, would work, which makes the attacker difficult to disguise as a legitimate reader. In addition, in the last step of our protocol, tag verified the backend database by calculation with the new random number r_2 which generated by data base, nothing to do with R_t.

4.2 Seuritys Analysis

Tag privacy. In this protocol, the important privacy information ID and K are not transmitted in the channel in plain text. When the attacker intercepted the transmission data, it can get the time stamp T, random number r generated by tag and random number r_2 generated by database in plain text, as well as the important data ID, ID_r in cipher text with hash operating. The security of Hash guarantees the important privacy information of tag not to be cracked, such as ID, ID_r. In the protocol proposed in this paper, important information is involved in every step of authentication, so an attacker, even get a random number and time stamp cannot attack RFID system, so as to protect the security of privacy information.

Man-in-the-middle attack. the reader in this protocol has the unique identifier ID_r and transfers the encrypted text after the hash operation. When the attacker disguised as a legitimate reader communicated with tag, the tag will verify the reader's legitimacy. Because of the security of hash operation, even if the attacker intercepted the identifier information in hash function that the reader sent, it also cannot get the reader identifier. So attackers cannot be authenticated by the tag and pretend legitimate reader to communicate with tag. It also cannot disguise as a legitimate tag by obtaining tag's response to implement the next attack.

Spoofing attack. In this protocol, T which is sent to tag by reader changes with time. Attacker can intercepted r and tag response $H(ID \oplus T \oplus r)$ in the first round of communications. However, the value of T has been changed due to the different time when the reader sends the authentication request next time. The response $H(ID \oplus T \oplus r)$ that attacker intercepted last time becomes useless for it cannot meeting the requirements $H(ID' \oplus T \oplus r)=H(ID \oplus T \oplus r)$ in database to achieve spoof attack. When the attacker in a similar way to capture reader authentication request $H(ID_r \oplus T)$, and in the next round sent it to tag, T would not meet the $T_0<T<T_{max}$ due to time stamp has been updated to $T_0=T$, so it can neither implement the trick attack.

Reply attack. The time stamp T in this protocol updates in each session and the response from the tag is different each time for the new generated random number r. The replay attack is similar to trick attack, which only sends the intercepted response repeatedly. When attacker intercepts the last response from tag to reader and sent to the database repeatedly, it cannot implemented replay attack successfully because the value of T is changed and not meets the requirements $H(ID' \oplus T \oplus r)=H(ID \oplus T \oplus r)$.

Tracking attack. The attacker sends authentication request to tag in the first round of communication, and record tag's response $H(ID \oplus T \oplus r)$. It would like to use the same authentication request in the next round, if the tag's response is the same as the one in previous round, the attacker can track the tag with this. However, as introduced in the front, our protocol can effectively prevent man-in-the-middle attack, so an attacker can't pretend reader to send the authentication request to tag. Also, for the random number r is new in each response of tag, the responses are too chaotic for attacker to track the location of the label.

De-Synchronization attack. In this protocol, after the last step tag will update the latest communication time stamp T_0 to T. When the attacker intercepted authentication information reader send to database, the T_0 in tag will not be updated. However, when the time stamp is judged in the next session, authentication process will not be affected, because the criterion is if T is greater than T_0 and the legal new time stamp still meets the conditions. And as long as there is update information sent to tag from Reader, T_0 can be re-synchronized again.

Mutual authentication. Our protocol uses the challenge-response mechanism which can be authenticated mutually. Tags, readers, and database can verify the identity between each other and protect the system security.

According to the Table 1, we compare our protocol with some previous RFID protocols on several

common threats. Through the analysis of the protocols, the authentication protocol in this paper can protect the privacy of tag, and resists attacks by spoofing, position tracing, replay and etc..

Table 1. Security of different protocols

Function index	Hash-lock	Random Hash-lock	YA-TRAP	Challenge-response	LCAP	NTRU	This protocol
Tag privacy	×	×	√	√	√	√	√
Man-in-the-middle attack	×	×	×	×	×	×	√
Spoofing attack	×	×	√	√	√	√	√
Reply attack	×	×	√	√	√	√	√
Tracking attack	×	√	√	√	×	×	√
Synchronization attack	√	√	×	×	×	×	√
Mutual attack	×	√	×	√	√	√	√

4.3 Performance Analysis

There are strict restrictions in storage capacity and computing power of RFID tag for applications. The design of RFID security authentication protocol should consider not only its security, but also its computation time and storage capacity and other factors. It is an aim to reduce the amount of computation as well as store data as much as possible, thereby reducing the cost of the tag and the entire RFID system. We will analyze the performance of the protocol mainly from storage quantity, computation quantity (also equivalent to computation time) and the amount of communication which are required by tag, reader and database.

The length of the unique identifier ID, the secret value key, the private key f, the time stamp T, and the output of hash operation or public key encryption are all set to l, the length of the public key length is 2l. A hash calculations is H, computation of generating a random number is r, the computation of converting a timestamp is t, computation of a public or private key encryption or decryption is s, the number of reader is m, the number of tags is n. (the length of the random number r and XOR computation is relatively small, which are not considered in the analysis and the public key and private key encryption and decryption computation is far greater than ordinary hash operations)

According to the comparison in Table 2, Table 3 and Table 4, the protocol in this paper has stronger security, but storage capacity, computing and communication overhead is relatively high. However, comparing to the great complexity authentication protocols based on public key encryption algorithm such as NTRU, the performance of it can be accepted. There are various applications of RFID. The design of security protocols must consider the trade-offs between security and cost according to the different environment and demand, achieving low cost and reliable security as far as possible.

Table 2. Storage overhead

	Hash-lock	Random Hash-lock	YA-TRAP	Challenge-response	LCAP	NTRU	This protocol
Tag	2l	l	l	l	l	2l	(m+1)l
Reader	0	0	0	0	0	0	l
DB	3nl	nl	l	nl	2nl	3nl	(m+n)l

Table 3. Calculation overhead

	Hash-lock	Random Hash-lock	YA-TRAP	Challenge-response	LCAP	NTRU	This protocol
Tag	h	h+r	h	2h+r	2h	3s	(m+1)h/2+2h+r
Reader	0	(n+1)h/2	t	r	r	r	h+t
DB	0	0	(n+1)h/2	(n+1)h/2+h	h	3s+r	(m+n+2)h/2+h+r

Table 4. Communication overhead

	Hash-lock	RandomHash-lock	YA-TRAP	Challenge-response	LCAP	NTRU	This protocol
Tag	2l	l	l	l	2l	2l	l
Reader	2l	2l	3l	2l	3l	3l	4l
DB	l	l	0	l	l	l	l
Num	5l	4l	4l	4l	6l	6l	6l

5 Conclusion

We propose a lightweight mutual authentication protocol satisfying privacy protection and security needs of current RFID protocols. In the authentication process, we introduce the time stamp to keep the freshness of the challenge-response information in each communication round. This helps to protect the tag privacy and prevent the tracking from the attacker. Comparing with the existing protocols, this protocol has high security and moderate cost, so the protocol has a practical significance. We will add anti-collision technology to the security protocol in the next step of the study.

Acknowledgment

This work is supported by National Natural Science Foundation of China (61401015 and 61201159) and The Foundation of the BUCEA (00362016168).

References

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

[2] K.P. Fishkin, S. Roy, B. Jiang, Some methods for privacy in RFID communication, Lecture Notes in Computer Science 3313(2016) 42-53.

[3] A. Mitrokotsa, M.R. Rieback, A.S. Tanenbaum, Classifying RFID attacks and defenses, Information Systems Frontiers 12(5)(2010) 491-505.

[4] H.S. Zhang, H.S. Guan, H.Q. Han, Public key based mutual authentication protocol for RFID system, Computer Engineering and Applications 46(5)(2010) 69-72.

[5] K.P. Fishkin, S. Roy, B. Jiang, Security analysis and strengthening of an RFID lightweight authentication protocol suitable for VANETs, Lecture Notes in Computer Science 3313(2016) 42-53.

[6] I. Erguler, C. Unsal, E. Anarim, G. Saldamli, Security analysis of an ultra-lightweight RFID authentication protocol-SLMAP, Security & Communication Networks 5(3)(2012) 287-291.

[7] S.E. Sarma, S.A. Weis, D.W. Engels, Radio frequency identification: security risks and challenges, RSA Laboratories Cryptobytes 6(1)(2003) 2-9.

[8] S.A. Weis, S.E. Sarma, R.L. Rivest, D.W. Engels, Security and privacy aspects of low-cost radio frequency identification systems, Computer Science 2802(2004) 50-59.

[9] M. Ohkubo, K. Suzuki, S. Kinoshita, Hash-chain based forward-secure privacy protection scheme for low-cost RFID, in: Proc. the SCIS 2004, 2004.

[10] G. Tsudik, YA-TRAP: yet another trivial RFID authentication protocol, in: Proc. IEEE International Conference on Pervasive Computing and Communications, 2006.

[11] B. Luo, Security research and design of RFID system based on dynamic encryption algorithm, in: Proc. Beijing University

of Post and Telecommunication, 2010.

[12] J.S. Cho, S.S. Yeo, S.K. Kim, Securing against brute-force attack: A hash-based RFID mutual authentication protocol using a secret values, Computer Communications 34(3)(2011) 391-397.

[13] X. Ren, X. Xu, Y. Li, An One-way Hash Function Based Lightweight Mutual Authentication RFID Protocol, Journal of Computers 8(9)(2013) 2405-2412.

[14] K. Rhee, J. Kwak, S. Kim, D. Won, Challenge-response based RFID authentication protocol for distributed database environment, in: Proc. International Conference on Security in Pervasive Computing, 2005.