RFID Bi-directional Authentication Protocol Based on Random Number and Hash Function

LIU Jian-dong, WANG Ye-quan, ZHANG Xiao, SHANG Kai

School of Information Engineering, Beijing Institute of Petro-chemical Technology, Beijing 102617, China

Keywords: RFID; Random number; Hash function; authentication protocol

Abstract: On the basis of the analysis of commonly used RFID authentication protocols' shortcomings, this paper proposes a random number and hash function based RFID bi-directional authentication protocol. This protocol can resolve eavesdropping, illegal access, location tracking, impersonation and replay attack.

1. Introduction

Many insecurity factors, such as unauthorized read, location tracking, eavesdropping, spoofing, and replay attack, are brought in to RFID due to its use of non-contact automatic identification technology [1-2].

In order to solve security problems of RFID, scholars both at home and abroad have conducted intensive researches [3-7]，including Hash Lock Protocol[5] proposed by Sarma et al., Randomized Hash-lock protocol proposed by Weis et al., and Hash chain protocol proposed by Ohkubo et al.[7]. All of above three classical protocols are realized based on one-way *Hash* function. Due to unidirectionality of Hash function, these protocols can solve some insecure problems, but there are still insecure factors[8-11].

To solve the security issues of RFID, the design of security authentication protocol must meet the following two conditions: (1) Hash value is used to replace information when conveying in insecure channels and the important information shall be accompanied with random numbers; (2) Bi-directional authentication function shall be placed between label and reader.

2. RFID Bi-directional Authentication Protocol based on Random numbers and Hash Function

Random numbers and Hash function are employed to build secure RFID bi-directional authentication protocol. Before being generated, each label needs to have a secret value S shared with backend database in addition to store its identification ID. A built-in random number generator is placed in the reader, and all of identification ID_i as well as secret value S_i corresponding to ID_i are stored in the backend database. The protocol process flow is illustrated in the Figure 1.

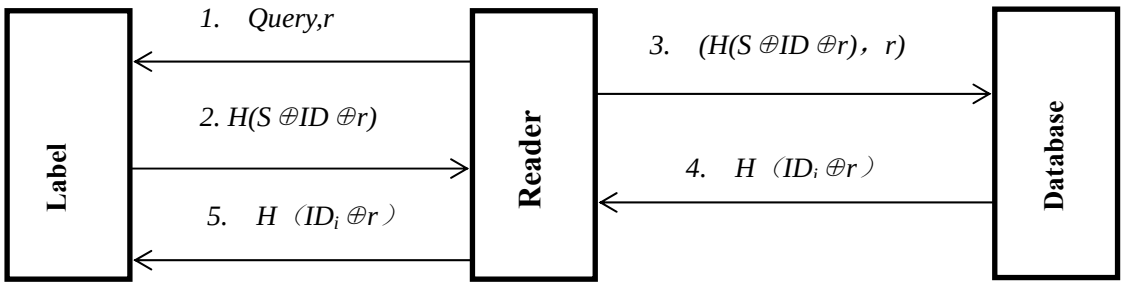

Figure 1 The flow chart of a randomized RFID bi-directional authentication protocol based on Hash function

2.1 Authentication Process

(1) *R-T*：reader generates a random number *r,* and sends the r and a Query authentication request to a label；

(2) *T-R*：After receiving the request, the label calculates the $H(S \oplus ID \oplus r)$，and sends the result to the reader and stores *r*；

(3) *R-D*：after receiving $H(S \oplus ID \oplus r)$ from the label，the reader will send it and r to database；

(4) *D-R*：database query is conducted and the calculation is made to identify whether there is a data pair(ID_i,S_i), which allows $H(S_i \oplus ID_i \oplus r)= H(S \oplus ID \oplus r)$; If it does not exist, the authentication fails；If it exists，then the calculation is made in database and the $H(ID_i \oplus r)$ is sent to the reader；

(5) *R-T*：after receiving the $H(ID_i \oplus r)$ from database，the reader will forward it to the label. After receiving $H(ID_i \oplus r)$，the label will calculate $H(ID \oplus r)$，and verify whether $H(ID \oplus r)$ is equal to $H(ID_i \oplus r)$. if yes, then it passes the verification, otherwise, it fails to pass the verification.

2.2 Performance Analysis

(1) Confidentiality: the Hash value acquired from Hash computation is transmitted during the interaction between reader and label. Even if an attacker intercepts transmitting information, he/she is not able to get the real message.

(2) Integrity：due to unidirectivity of *Hash* function，if transmitting data are falsified，they can not pass authentication, so that the integrity of the transmitting data is ensured；

(3) Security：Since the random numbers of each authentication are different, each Hash value is also different. Therefore, even if attracter intercepts the current information, it can not be used during next authentication.

(4) Database computation burden is small：Assuming that labels with the number of N are stored in the database, then the average computation burden of the database is $(1+N/2)H$ (*H* stands for *Hash* computation) and some simple exclusive-or operation. Therefore, the database is more efficient with small computation load.

(5) Bi-directional authentication between label and database is achieved. The validity of labels is verified by database through $H(S \oplus ID \oplus r)$, *and the* validity of database is verified by label through $H(ID_i \oplus r)$;

(6) It has effectively solved many insecure problems.

1) Preventing unauthorized read：The data on labels can only be read through authenticated reader, so that the unauthorized read is effectively avoided.

2) Preventing location tracking: during the process of each authentication, Hash value is different due to different random numbers, and the last authentication information is different with the current one, so that location tracking is effectively avoided.

3) Preventing eavesdrop：Since message is transmitted through Hash computation, and the Hash value can not reversely derive the real message, attackers are not able to get real information, and thus it can effectively prevent the eavesdrop;

4) Preventing counterfeit：both *ID* and *S* are confidential information of the system，attackers are not able to forge $H(S \oplus ID \oplus r)$ and $H(ID_i \oplus r)$，and thus they can not forge label and reader;

5) Preventing replay; due to different random number r, even though attacker intercepts the $H(S \oplus ID \oplus r)$ this time, they are not able to simulate the $H(S \oplus ID \oplus r)$ *of the next time, and thus the replay attack is effectively prevented.*

2.3 Performance Comparison

This protocol has overcome the safety defects existing in hash lock protocol, randomized Hash locking protocol and Hash chain protocol, as well as in *RFID bi-directional authentication protocol and RFID security authentication protocol based on Hash function.* Its performance comparison is illustrated in the Table 1, and the efficiency comparison is illustrated in the Table 2. In table 1, √ stands for secure, × stands for insecure; In table 2, L stands for the length of the ID, secret and

secret key, r stands for the random number and timestamp, and H stands for Hash function.

Table 1 Security comparison

	Hash Locking *protocol*	random *Hash* Locking protocol	*Hash* Chain protocol	RFID Mutual Authentication Protocol Based on Random Number and Hash Function	RFID Security Authentication Protocol Based on Random Number and Hash Function	Protocol in this paper
Anti tracks	×	×	√	×	×	√
Anti-hacking	×	×	√	√	√	√
Replay attack prevention	×	×	×	√	√	√
Security equipment coaxing	×	×	×	√	×	√
Mutual authentication	√	√	×	√	√	√
A distributed environment	√	√	√	√	√	√

Table 2 Protocol efficiency comparison

	Hash Locking *protocol*	random *Hash* Locking protocol	*Hash* Chain protocol	RFID Mutual Authentication Protocol Based on Random Number and Hash Function	RFID Security Authentication Protocol Based on Random Number and Hash Function	Protocol in this paper
Label Computation	*1H*	*1H,1r*	*2H*	*3H,2r, 1L*	*3H,1r*	*2H*
reader computation	—	*(n/2)H*	—	*1H, 1r*	*2H, 1r*	*1r*
database computation	—	—	*(tn/2)H*	*(2+n/2)H, 1L, 1r*	*(1+n/2)H*	*(1+n/2)H*
Label storage space	*2L*	*1L*	*1L*	*2L*	*1L,1r*	*2L, 1r*
reader storage space	—	—	—	*1H*	*1L, 1r*	*1r*
database storage space	*3nL*	*nH*	*2nL*	*3nL*	*2nL*	*2nL*

3. Conclusion

RFID is replacing traditional barcode, but its application is limited because the data transfer between label and reader is vulnerable to external attack. This paper, after having analyzed the security problems of RFID technology, has designed and strictly proved a safer and more efficient bi-directional authentication protocol of RFID, which can be widely applied in military, aviation, transportation, manufacture, medical and logistics sectors.

References

[1] Ranasinghe D, Engels D, Cole P. Low-cost RFID systems: Confronting security and privacy [C]. Proc of the Auto- ID Labs Research Work shop. Cambridge, MA: Auto-ID Labs, 2004.

[2] Kwak J, Rhee K, Oh S, et al. RFID system with fairness within the framework of security and privacy [C]. Proc of the European Workshop on Security and Privacy in Ad Hoc and Sensor Networks. Berlin: Springer, 2005: 142-152.

[3] Ding Zhenhua ,Li Jintao , Feng Bo . RFID authentication protocol Based on Hash functions[J].Computer research and development,2009,46(4):583- 592.

[4] Chen Keli, Guo Chunsheng . A two-layer / Mutual authentication of the random Hash Lock RFID Security Protocol [J]. Application of electronic technology .2008 (11) : 46-149 .

[5] SARMA S, WEIS S, ENGELS D. RFID systems and security and privacy implications[C]. Proc of CHES'02 Springer, 2002:454-469.

[6] WEIS S, SARMA S, RIVEST R. Security and privacy aspects of low-cost radio frequency identification systems[C]. Proc of Security in pervasive Computing'04, 2004: 201- 212.

[7] OHKUBO M, SUZUKI K, KINOSHITA S. Cryptographic approach to privacy-friendly tags[C]. Proc of RFID Privacy Workshop, USA MIT,2003.

[8] Zhang Nan , Chen Jianying , Fu Chun . RFID mutual authentication protocol Based on Hash functions[J]. Journal of Southwest University for nationalities , 2012,38 (6):969-972.

[9] Liu Mingsheng , Wang Yan, Xin sheng Zhao. RFID research of security authentication protocol Based on Hash functions[J]. Chinese Journal of sensors , 2011,24(9):1317-1321.

[10] Burrows M, Abadi M, Needham R. A Logic of Authentication[J]. ACM Transactions on Computer Systems, 1990, 8(1): 18-36.

[11] Needham. Using encryption for authentication in large networks of computers[J]. Communications of the ACM,1978,21(12):993- 999.