Advanced Engineering Forum *Online: 2012-09-26*
ISSN: 2234-991X, Vols. 6-7, pp 1072-1077
doi:10.4028/www.scientific.net/AEF.6-7.1072

Secure Authentication Protocol of RFID System Based on Access Control

Gui-Chao Wang [a], Ai-Li Zhang[b] and Yong-Zhen Li[c]

Network & information Security Lab., Dept. of Computer Science & Technology

Yanbian University, Yanji, China

[a] wangguichao630@126.com, [b] 2011010549@ybu.edu.cn, [c] lyz2008@ybu.edu.cn

Keywords: Authentication Protocol; RFID System; Access Control

Abstract. The security and privacy problem of low-cost RFID system is one of the most difficult conundrums in the RFID research field. A protocol based on access control was proposed in this paper, which used the reader access, partial ID, XOR operation, etc. By using of the reader authority distribution method, the unauthorized tag`s information was prevented give-away and it can avoid the lawful reader attack, location privacy attack, etc. Function of the reader was fully used. At the same time, the back-end database`s load and the time of the tag`s answer were reduced. Compared with several traditional security authentication protocols, this protocol is more security, lower energy consumption and more suitable for low-cost RFID system.

Introduction

Following the development of the Internet of things and the mature of related technology, the RFID technology is more and more attention by people. But because of the particularity of the RFID system, people begin to attach importance to its security and privacy. So far, although many RFID security agreements have been proposed, each agreement has its own shortcomings. On the base of analysis of the existing agreement, this paper proposes a kind of RFID secure authentication protocol based on access control. This protocol controls the reader through the back-end database, thus effectively prevents illegal reading of unauthorized tags information and enhances the RFID system's security. Also, some of the ID[1] and the bit operation, reduce the times of security of authentication protocol and make full use of the reader resources, which is more suitable for the low-cost RFID system.

Authentication Protocol for RFID System

In order to solve the security and privacy issues, the usually method is using password-based security protocols which used random number, hash function or encryption function[2]. There are some common RFID security protocols, which are used to analyze their advantages or disadvantages.

Hash-Lock protocol: Hash-Lock protocol[3] was proposed by Sarma and others. This protocol is used to avoid information disclosure. This protocol uses metaID taking the place of the real tag ID. The process of this protocol shows in Fig 1.

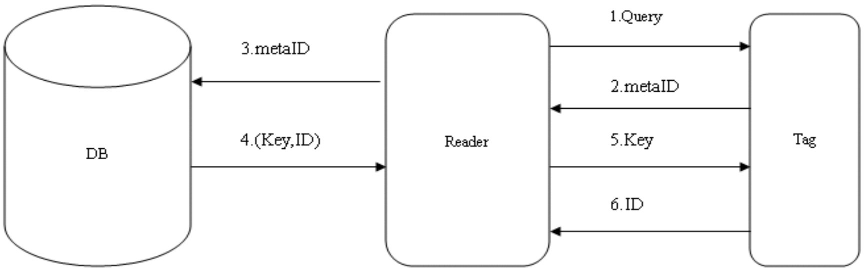

Fig. 1 Hash-Lock protocol

This protocol can prevent the illegal reader reading the tag ID in some ways. But in its certification process, the metaID is unchanged, and the key and tag ID are sent in plaintext over an insecure channel. So this protocol is easily attacked by spoofing attack, reply attack and location tracking[4]. Others, if the reader keeps the tag ID when it gets the information from the tag, this protocol can`t against lawful reader attack[5]. On the other hand, this protocol also cannot guarantee that unauthorized tag`s information. In this protocol, the reader deals with all the information from tags and sends it to the database. If the effective information is too little, it would case a serious waste of the database and reader resources.

Randomized Hash-Lock protocol: Randomized Hash-Lock protocol uses a ask - response mechanism which based on random. The authentication information which is sent to the reader from the tag is random variation. This protocol is shown in Fig 2.

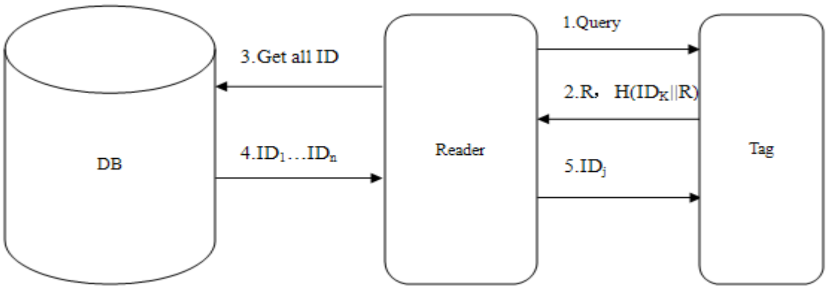

Fig. 2 Randomized Hash-Lock protocol

In this protocol, the tag ID is still sent in plaintext over an insecure channel, so it is easily attacked by location tracking. At the same time, the back-end database sends all the tag ID that it stored to the reader each time. The amount of communication data is very much. So this protocol is not only unsafe but also not useful.

Hash-chain protocol: Hash-chain protocol is a protocol which based on shared secret inquiry – response. In Hash-chain protocol, the tag uses two different hash functions. When the reader reads the information from tag, the tag will send different responses each time. This protocol is shown in Fig 3.

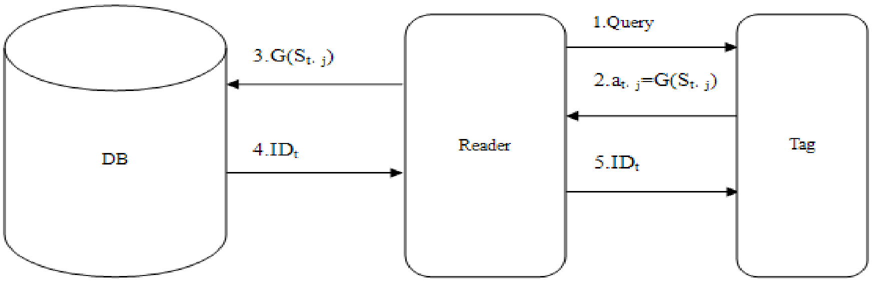

Fig. 3 Hash Chain protocol

In this protocol, the tag ID can be updated by itself, but it is very easily attacked by reply attack and spoofing attack. The back-end database will do j hash functions each time, so the computation is very much. Others, this protocol needs two different hash functions, the cost is very high[6].

All of the above, these protocols all have some problems, such as lawful reader attack, unauthorized tag`s information disclosure, etc. At the same time, the reader will read all of the tag`s information that it can get though the whole certification process. This cases serious waste of resources. In order to make up all the shortages, a protocol based on access control was proposed in this paper.

Proposed Authentication Protocol

To compensate for the shortcomings and deficiencies of RFID security protocols, this paper proposed a protocol which based on access control. This protocol effectively solved the security and privacy problem of the RFID system. The unauthorized tag`s information can`t be illegal to read by setup the reader's right. Furthermore, it also can avoid the lawful reader attack, reduce the database load and make full use of the reader's resources. Its specific certification process is shown in Fig 4.

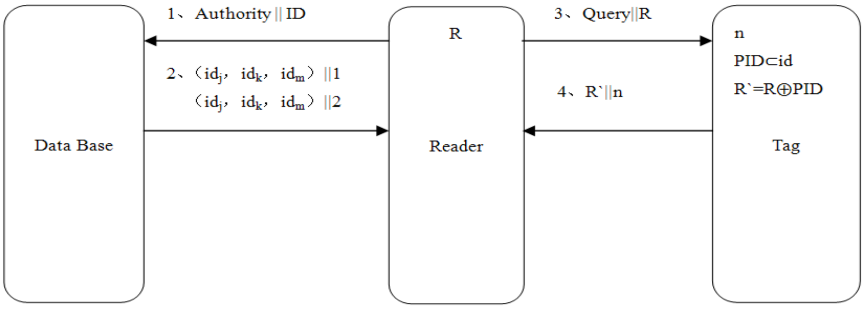

Fig.4 Proposed protocol

The proposed protocol is comprised of 4steps as shown in the figure 4.

Step 1. Apply for the right: the readers send its own ID and the back-end database`s DID which belongs to the back-end database along with the authority information.

Step 2. Assign the right: the back-end database inquires the ID and DID which it received from the readers in its own database. If it finds a legitimate ID which is the same as it received, the back-end database compares the readers`s new permissions with its old permissions, and marks the increased tag ID with 1 and the reduced tag ID with 2. Then sending (idj，idk，idm) || 1, (ida，idb，idc) || 2 to the reader; The reader updates its list of permissions according to the information that received from the back-end database. Or the back-end database gives the reader the basic permissions and marks it as the roaming reader. The back-end database`s projects are shown in the table 1.

Tab.1 Lists in back-end database

Number	The readers`s ID	The new permissions	The old permissions
1	ID_1		id_1，id_2，id_3 … id_n
2	ID_2	id_6，id_8，id_9，id_{13}	id_3，id_8，id_{11}
3	ID_3	id_2，id_5，id_9	
…	…	...	…
M	ID_M	id_k，id_m，$id_{n...}$	id_a，id_b，$id_{c...}$

For the roaming reader, the local database communicates with the DID database on the basis of the DID which it got from the roaming reader and determines the readers` legitimacy or not. If the DID database has the reader`s ID, the reader is lawful. Otherwise, the reader is unlawful.

Step 3. The tag Authentication: the reader generates the random number R and sends it to the tag along with the inquiry information; the tag generates the random number n and calculates R` by XOR R and PID. The R is received from the reader and the PID is selected from the start location of id. Then the tag sends R` and n to the reader.

Step 4. The reader Authentication: when the reader received the responses from the tag, it calculates PID by XOR R` and R . Then the reader calculates each PIDi=（idi，n）according to its tag access list and the n which received from the tag. If there is a PIDi identical to the value of the PID that the reader received from the tag, then the reader marks the idi and the authentication is successful. Otherwise, the authentication is failure.

Security Analysis

The secure protocol which is proposed in this paper is a typical inquiry-response authentication protocol. In this protocol, both the tag and the reader use the random number and XOR computation, so this protocol is very secure. The following are several typical attacks which were analyzed.

(1) Safety against spoofing attack: In order to guarantee the secrecy of the message between the tag and the reader, this protocol uses the random number to guarantee the message. Even though the attackers get the reader`s random number R and the tag`s response R` and n, then use the formula R`=R⊕PID to get PID, they can`t use PID and n to get the tag`s id. So the proposed protocol can adjective avoid spoofing attack.

(2) Safety against Reply attack: There are two kinds of attack: disguising as a reader or a tag. If the attacker disguises as a reader, the attacker eavesdrops on the message sent from the reader to the tag and resends it. Because each certification process has a random number to participation, so the attacker can`t get the lawful DID. The attacker is unable to pass the reader`s certification, and it is safe against replying attack.

(3) Safety against location privacy: The attacker disguises as a reader and sends the inquiry information to the same tag[7]. If the tag`s responses is same in each time, the attacker can get the tag`s location based on the tag`s responses. In this proposed protocol, the tag generates a random number each time, so the PID also is different every time. The attacker can`t make sure the tag is the same tag using the different PID.

(4) Safety against Non-authorized tag attack: In connection with the traditional RFID security protocols, the reader responds all the tag`s inquiry which is able to received. All the lawful tags can be authenticated, thus this leads to the information of the non-authorized tag which belongs to lawful tags being leaked. But in this proposed protocol, the reader`s read permission is controlled by the back-end database. The reader can only read the tag which it has the permissions, and the non-authorized tag can`t pass the certification. So in this protocol, the personal information of the non-authorized tag can`t be let out.

(5) Safety against the lawful reader attack: In traditional cases, the security protocol did not consider the problem of the lawful reader. The lawful reader in the RFID system knows the whole certification process, so when a lawful reader passed a legitimate certification process, it could store the response information of the tag. For the Hash Lock protocol, Randomized Hash Lock protocol and Hash Chain protocol etc, the reader can immediate read the tag`s information without the back-end database. This loophole could lead to disclose the tag`s information. But in this proposed protocol, if the reader`s permissions have changed, the reader can`t find the same PID between the reader and the tag. So the tag`s certification can`t be certified, and this proposed protocol can be effectively against the lawful reader to attack.

All of the above, this proposed protocol is more secure. The table 2 shows a result of comparing and analyzing the security of the traditional protocols and the proposed protocol[8].

Tab.2 Analysis of security

Security protocol	Spoofing attack	Reply attack	Location privacy	The lawful reader attack	Non-authorized tag attack
Hash-Lock	F	F	F	F	F
Randomized Hash-Lock	F	T	T	F	F
Hash Chain	F	F	T	F	F
public key encryption protocol	T	T	T	F	F
proposed protocol	T	T	T	T	T

Remark: T : this protocol can prevent the attack, F: this protocol can`t prevent the attack.

Efficiency Analysis

In the low-cost RFID system, the tag`s computing, storage and other hardware conditions are extremely limited[9]. So the security protocol of the low-cost RFID system must guarantee the hardware requirements of the tag. The efficiency analysis of the RFID security protocol is main analyzed form three aspects of the storage, computing and the amount of continuous session times[10]. The efficiency analysis is shown in the table 3.

Tab. 3 Analysis of performance

Security protocol	Hash-Lock	Randomized Hash-Lock	Hash Chain	The proposed
Tag`s computing	1h	1h+r	lh	1x+r
Tag`s storage	1l	1l	1l	1l
Reader`s computing	0h	ih	i*h/2	n*x+r
Reader`s stroage	1l	il	i*l	n*l
Continuous session times	6	5	5	4

Remark: l: ID`s length; r: random number; h: hash function; x: XOR; i: the tag`s amount; n: the authorized tag`s amount.

It can be seen from the table 3, Hash-Lock protocol uses the hash consideration, so its computing is more than the proposed protocol. On the other hand, the proposed protocol makes full use of the reader`s computing ability. At the same time, reducing the amount of continuous session and reducing the energy consumption of the whole system. The proposed protocol reduces the requirements for the tag, so it is more suitable for low-cost RFID system.

Conclusions

This paper proposes the secure authentication protocol of RFID system based on access control, which uses the back-end database to control the reader`s permission to access the tag. In this way, this protocol can be effective to resist the unauthorized tag`s information, and solve the problem of internal legal reader attack. Simultaneously, this protocol can effectively control the access range of the reader, and reduce the amount of data communication between the reader and the back-end database. Furthermore, it also reduces the database load and makes full use of the reader`s resources. On the other hand, this protocol greatly reduces the computation and storage requirements on tags, and it is more suitable for low-cost RFID systems.

References

[1] Li yong-zhen, Cho Young-Bok, Um Nam-Kyoung, and Lee Sang-Ho. Security and privacy on authentication protocol for low-cost RFID [C]. Proceedings for 2006 International Conference on Computational Intelligence and Security. Guangzhou, China, November 3-6, 2006, pp.1101-1104.

[2] Zhou xiaoguang, Wang xiaohua. Radio Frequency Identification (RFID) technology principle and application examples [M]. Beijing: Posts & Telecom Press, 2006.

[3] WEIS S A. Security and privacy in Radio-frequency identification devices [D]. Department of Electrical Engineering and Computer Science of MIT, 2003.

[4] Enzelleer k. RFID handbook Z: Radio-Frequency Identification Fundamentals and Applications [M]. Second edition. New York: John Wiley and Sons Ltd, 2003

[5] Xie chuan. Combination of Hash functions and key array of RFID security authentication protocol. Journal of Computer Applications. 2011, 31(3), pp.805~808.

[6] Chen ruixin, Zou chuanyun, Huang jingwu. RFID cryptographic protocol based on ID change. Application of Electronic Technique. 2009, 35(9), pp.157~160.

[7] Shao qian, Chen yue, Chang zhenhua. Design of RFID tag Ownership Transfer Mode and Protocols. Computer Engineering, 2009:35(15), pp.143~145.

[8] Ding zhenhua, Li jintao, Feng bo. Research on Hash-Based RFID Security Authentication Protocol. Journal of Computer Research and Development. 2009, 46(4), pp. 583~592.

[9] Zhu min. A Survey on Ultra-lightweight Security Mechanism in Low-cost RFID. Computer Knowledge and Technology. 2010:6(33), pp.9221~9224.

[10] Tsudik G. YA-TRAP, yet another trivial RRID authentication protocol [C] // Proc of the 4th Annual IEEE Int Conf on Pervasive Computing and Communications Workshops. Los Alamitos, CA: IEEE Computer Society, 2006, pp.640~643.