A LIGHT-WEIGHT MUTUAL AUTHENTICATION PROTOCOL FOR ISO 18000-6B STANDARD RFID SYSTEM

Yonghao Gu[1], Weiming Wu[2]

[1] [2]School of Computer Science, Beijing University of Posts and Telecommunications, Beijing
[1]guyonghao@bupt.cn, [2]wuwming@bupt.edu.cn

Abstract

Low-cost Radio Frequency Identification (RFID) tags are highly resource and computational power limited, so that it can not support strong cryptography. To solve the security and privacy of low-cost RFID system, many schemes have appeared, but most of them are based on classical cryptographic primitives such as Pseudorandom Number Generators, hash functions, and block ciphers. A new approach is necessary to tackle the problem of resource consuming and synchronism of secrets updating, so we propose a light-weight mutual authentication protocol for RFID tags complied with ISO 18000-6B standard, which could be implemented in the low-cost tags as it only needs about 1000 gates. Through security analysis and performance analysis, the proposed protocol is approved to be very efficient.

Keywords: RFID; ISO 18000-6B；low-cost; mutual authentication; data synchronism

1 Introduction

Radio Frequency Identification is an automatic identification system, which can identify object and retrieve data using radio signal. The typical RFID system consists of tags, readers and back-end database. A secure RFID system has to avoid eavesdropping, tracking and other attacks. Due to the wireless characteristics between tags and readers, RFID technique causes serious privacy and security problem such as information exposure and user's location tracking [1]. All of the privacy problems should be solved before successful industrialization of RFID.

Recently, low-cost RFID has been attracting more interests from industry and academic fields. Such RFID system will be widely used in ubiquitous computing environment, such as access control, location tracking, and etc [2]. Considering the low computational power and memory size of low-cost RFID tags, it is very had to implement the existing cryptographic algorithms for authentication [3].

In this paper, we propose a robust mutual authentication protocol that fits the low-cost RFID system complied with ISO 18000-6B standard [4]. Our protocol meets the security requirement for tags, which require confidentiality, anonymity, and integrity in the cryptographic point of view. The proposed protocol is robust enough against many attacks such as the resend attack, man-in-the-middle attack as well as synchronism of secrets updating. Besides, our scheme is also forgery resistant against the attackers who copy a prevailing tag.

The remainder of the paper is organized as follows. We introduce related works of authentication protocols in section 2. In Section 3, we show the air-interface communication procedure of RFID complied with ISO 18000-6B standard. In Section 4, we propose a new authentication protocol. In Section 5, we make a comparison in security requirement and performance requirement between several schemes including our scheme. Finally, we conclude the paper in section 6.

2 Related Works

The existing RFID systems are vulnerable to many security risks and imply potential privacy problems, but it is hard to use existing cryptographic algorithms to solve these problems because of restricted memory size and computational power of tag. To solve security and privacy problem of low-cost RFID system, there have been a number of security schemes [5-19], which have its advantages and disadvantages. In the following, we introduce some typical schemes.

1) Hash Chain Protocol [10-11]. The protocol uses two has functions, one to refresh the secret in the tag, the other to make responses of the tag untraceable by eavesdroppers. However, this scheme needs many storage memory and time for authentication computation, as well as it can not prevent replay attack to a valid reader.

978-1-4244-4817-3/09/$25.00 ©2009 IEEE

2) Hash Lock Protocol [12]. The protocol mutually authenticates a tag and a reader, and provides anonymity on a tag's data. However, this scheme is not safety against eavesdropping because of tracking the ID number by attacker.

3) Henrici's Scheme [13]. The protocol is based on a hash function embedding in a tag and a random number generator on a back-end database to protect the user's privacy and the replay attack. However, this protocol can not resist against the man-in-the-middle attack. The attacker can be located between a legitimate tag and a legitimate reader and obtain the information exchanged, so that the attacker can be easily authenticated by the legitimate reader before the next session.

4) David's Scheme [14]. In this protocol, readers and tags share secrets to provide authentication without revealing their identities to adversaries. Unfortunately, such changes will require more storage and computational power for privacy and security in the RFID setting, so that it is not well fit for low-cost RFID system.

5) Lee's Scheme [16]. This scheme needs only a one-way hash function operation to prevent leakage of information. By refreshing a message transmitted from a tag in each session, the proposed protocol provides location privacy and security against attacks such as eavesdropping, spoofing, replay and etc. This protocol needs several thousand logic gate to provide security and privacy.

The previous schemes have their disadvantages at least in one aspect, and all protocols can not provide data synchronism between tag and database. In order to provide mutual authentication between reader and tag, the previous protocols at least need several thousand logic gates in tags, while most of these problems will be solved in our proposed protocol.

3 Communication Procedure of RFID Complied with ISO 18000-6B Standard

ISO 18000-6B, as the RFID air interface communication standards at 860-930 MHz, is widely used in many aspects. In this standard, data memory size is 1024 bits or 2048 bits, and 98 bytes or 216 bytes for user data storage. Besides these, multiple tags can be read at 40kbps at the same time. The communication procedure of this standard in Figure 1 will be described as the following.

Step 1 Binary Tree Collision Arbitration

Reader sends commands such as ***Group_select/Group_unselect*** to select responsive tags and send commands such as ***Fail/Success*** to select the target tag. The selected tag sends its ID number to the reader.

Step 2 Send Other Commands

Reader sends commands such as ***Group_select/Group_unselect*** to select responsive tags and send commands such as ***Fail/Success*** to select another target tag, and the selected tag sends its ID number back. Besides, reader may send commands such as ***Read/Write*** to read or write the tag's memory.

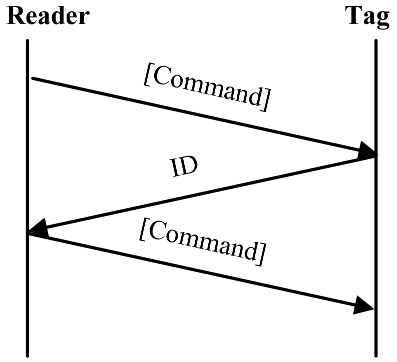

Figure 1. Communication Procedure of ISO18000-6B Standard

During the collision arbitration, ID number is sent without being enciphered, which is vulnerable to many risks such as tracking, replay attack and etc. So, secured communication protocol with authentication must be provided for this standard.

4 Our Proposed Scheme

Our proposed scheme provides a protocol shown in Figure 2, in which **Reader** stands for both the reader and the back-end database. The detailed procedures for each step are described.

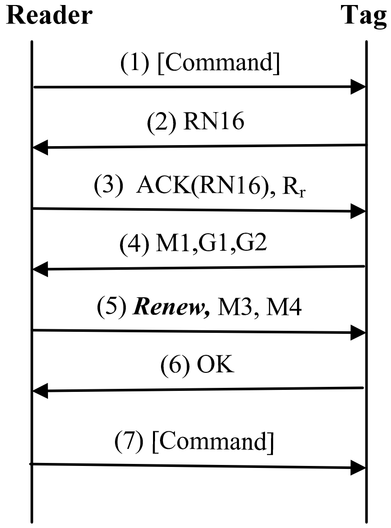

Figure 2. Proposed Mutual Authentication Protocol

4.1 Initial Setup

Before the protocol is started, the reader and the tag must be initiated as follows.

The tag is marked with a unique ID number and it stores two shared secrets K_1 and K_2.The reader should store a list, in which all tags information is kept. There are six items（ID，K_1，K_2，K_{t1}，K_{t2}，Data）in the list. ID stands for the identification of a tag; K_{t1} and K_{t2} stand for temporarily shared secrets, which are initiated with 0. Data stands for the secret information of tags, such as food price, production place and etc.

4.2 Detailed Description

Step 1 Binary Tree Collision Arbitration

Reader sends commands such as ***Group_select/Group_unselect*** to select responsive tags and send commands such as ***Fail/Success*** to select the target tag. The selected tag sends a 16-bit random number (RN16) to the reader.

Step 2 Reader Acknowledgement

The Reader sends back the acknowledgment information including ACK (RN16) and R_r after receiving RN16. R_r is the random number generated by the tag.

Step 3 Tag Authenticate RN16

At the tag side, RN16 in the ACK (RN16) is compared with the random number generated at the first step. If it is equal, the following computations are performed. $M_1=CRC(ID_x \oplus R_r) \oplus K_1$，$M_2=CRC(ID_y \oplus R_t) \oplus K_2$，$G_1=M_1 \oplus M_2$, $G_2=R_t \oplus K_1 \oplus K_2$. And then ($M_1$, G_1, G_2) is sent to the reader, in which ID_x stands for the first half part of ID, ID_y stands for the latter part of ID, and R_t is the random number generated by the reader.

Step 4 Reader Get ID

The reader queries the tag list in the database and performs the following operations for each tag.

If K_{t1} and K_{t2} are both 0, perform $R_t = G_2 \oplus K_1 \oplus K_2$，$M_2 = G_1 \oplus M_1$，$L_1= M_1 \oplus K_1$，$L_2= M_2 \oplus K_2$，$L_1'= CRC(ID_x \oplus R_r)$, $L_2'= CRC(ID_y \oplus R_t)$.

If K_{t1} and K_{t2} are not 0, perform $R_t = G_2 \oplus K_1 \oplus K_2$，$M_2 = G_1 \oplus M_1$，$L_{1t}= M_1 \oplus K_{t1}$，$L_{2t}= M_2 \oplus K_{t2}$，$L_{1t}'= CRC(ID_x \oplus R_r)$, $L_{2t}'= CRC(ID_y \oplus R_t)$.

If one tag satisfies one of the following conditions, the reader gets the ID number.

(1) $L_1= L_1'$ and $L_2'= L_2$ (2) $L_{1t}= L_{1t}'$ and $L_{2t}'= L_{2t}$

Step 5 Reader Send Renew Command

The reader generates Random number R_{TEMP}, computes $M_3=CRC[(IDx \oplus IDy) \oplus (K_1||K_2||Rr||Rt)]$, $M_4=R_{TEMP} \oplus K_1 \oplus K_2$, and then sends ***Renew*** and (M_3，M_4) to the tag, in which ***Renew*** is the renew query command.

At the same time, compute $K_{t1}=R_{TEMP} \oplus K_1$，$K_{t2}=R_{TEMP} \oplus K_2$ and get ready to update the shared secrets K_1, K2.

Step 6 Tag Authenticate Reader

When the tag receives ***Renew*** and (M_3，M_4), it validates whether ID_x，ID_y，R_t，K_1 and K_2 satisfy $M_3 = CRC[(ID_x \oplus ID_y) \oplus (K_1||K_2||R_r||R_t)]$. If the equation is satisfied, the tag updates its secrets through the following and sends ***OK*** command back to the reader.

$R_{TEMP}=M_4 \oplus K_1 \oplus K_2$，$K_{t1}=R_{TEMP} \oplus K_1$，$K_{t2}=R_{TEMP} \oplus K_2$.

Step 7 Reader Updates Secrets

When the reader receives the OK command, it updates the secrets by K1 =Kt1 and K2 =Kt2. If the OK command is not received, it shows that the OK command may be lost. So, the reader keeps both of these two secrets（K1，K2）and（Kt1，Kt2）until the same tag is authenticated successfully. Then, the reader may perform other commands.

5 Evaluation

5.1 Security Analysis

We evaluate our protocol in the view point of the security requirement.

(1)Guarantee mutual authentication. In the protocol, step 1 to step 4 realize the tag's authentication to the reader and step 5 to step 7 guarantees reverse authentication.

(2)Guarantee tag ID anonymity. The messages sent and received between the tag and the reader is different each time during all the authentication procedures. It is impossible to track the tag's location or decode the ID number through the previous messages, because different messages are exchanged each time due to the sending of the random number and the split ID with XOR operation.

(3)Against replay attack. In the proposed protocol, the replay/resend attack is prevented by generating the pseudo random number R_t, K_1, K_2, while the attacker can only get M_2, with which the random number can not be decoded.

(4)Against man-in-the-middle attack. Attackers can disguise as the middle man between the tag and reader to intercept the exchanged messages. The proposed protocol can prevent such attack by pseudo random number R_t and the split ID, which can not be easily decoded with the eavesdropping messages.

Table 1 shows the comparison of the security requirements between several typical authentication protocols. Our protocol satisfies nearly all security requirements, which is better than the other protocols.

Table 1 Security Comparison between Protocols

Protocol	TA	DI	MA	FS	RAP	DS
[11-12]	△	○	×	×	○	×
[10]	○	○	×	×	○	×
[13]	△	○	△	×	○	×
[14]	○	△	○	○	○	△
[15]	○	△	○	○	○	△
[16]	○	△	○	○	○	×
[17]	△	○	○	×	○	×
Our Scheme	○	○	○	△	○	○

***Notation**
TA: Tag Anonymity; DI: Data Integrity; MA: Mutual Authentication; FS: Forward Security; RAP: Replay Attack Prevention; DS: Data Synchronism
× Not Satisfied △ Partially Satisfied ○ Satisfied

5.2 Performance Analysis

Table 2 shows the performance comparison between several protocols. To realize our protocol, it only needs several basic operation and RNG operation. Besides, it only needs several hundred logic gates for tag, which is much less than the other protocols. So the proposed protocol is fit for the low-cost RFID authentication complied with ISO 18000-6B.

Table 2 Performance Comparison between Protocols

Protocol	Entity	HS	RNG	BO	AS	GN
[11-12]	Tag	1	¬	¬	6	1.5K-2K
	Reader	1	¬	¬		
[10]	Tag	1	¬	1	5	1.5K-2K
	Reader	1	¬	¬		
[13]	Tag	3	¬	3	5	5K-6K
	Reader	3	¬	3		
[14]	Tag	¬	1	1	5	3K-4K
	Reader	¬	1	1		
[15]	Tag	2	¬	3	5	3K-4K
	Reader	2	¬	3		
[16]	Tag	3	¬	2	5	5K-6K
	Reader	3	¬	2		
[17]	Tag	¬	1	10	7	3K-4K
	Reader	¬	1	10		
Our Scheme	Tag	¬	2	15	4	About 1K
	Reader	¬	1	15		

***Notation**
HO: Hash Operation; RNG: Random Number Generation Operation; BO: Basic Operation (⊕: XOR; ∧: Bitwise AND; ∨: Bitwise OR; +: Module addition); AS: Authentication Steps; GN: Gate Number for tag
¬: No need

6 Conclusions

Previous RFID techniques, cause serious privacy and security problem such as excessive information exposure and user's information tracking due to the wireless characteristics of air-interface and the limitation of RFID systems. So, development of cost effective and hardware efficient authentication algorithms will popularize the usage of low-cost RFID tags complied with ISO 18000-6B standard.

In this paper, the proposed light-weight mutual authentication protocol for ISO 18000-6B type tags is adopted to resist replay attack and man-in-the-middle attack. The cryptographic algorithm is implemented using simple basic operations such as XOR, CRC, module addition and etc, which uses about 1000 logic gates for tags. The integration of proposed security scheme will make unauthorized access to the tag's memory and also keep synchronism of secrets updating between tags and database.

References

[1] M. W. Johnson,A. Hately,B. A. Miller,R. Orr . Security and Privacy: A research survey [J].IEEE Journal on Selected Areas in Communications.Vol.24, No.2.February 2006.
[2] Weis S. A., Sarma S. E., Rivest R. L.. Security and privacy aspects of low-cost radio frequency identification systems. In: Proceedings of the 1st International Conference on Security in Pervasive Computing. LNCS 2802. Berlin: Springer-Verlag , 2004, 201～212.
[3] Molnar D, Wagner D.. Privacy and security in library RFID: issues, practices, and architectures. In: Proceedings of the 11th ACM Conference on Computer and Communications Security (CCS'04) , Washington , DC , USA , 2004 , 210～219.
[4] Information Technology - Radio Frequency Identification (RFID) for Item Management - Part 6: Parameters for Air Interface Communications at 860-930 MHz. ISO/IEC 18000-6B.
[5] Juels A. . Minimalist cryptography for low-cost RFID tags. In: Blundo C., Cimato S. eds.. Proceedings of the 4th International Conference on Security in Communication Networks (SCN 2004). Lectures Notes in Computer Science 3352. Berlin: Springer-Verlag , 2005 , 149～164.
[6] Lee S. M., Hwang Y. J., Lee D. H.. Efficient authentication for low-cost RFID systems. In:

Proceedings of t he International Conference on Computational Science and It s Applications (ICCSA 2005). LNCS 3480. Berlin: Springer-Verlag , 2005 , 619～627.

[7] Rhee K., Kwak J., Kim S.. Challenge-response based RFID authentication protocol for distributed database environment. In: Proceedings of the 2nd International Conference on Security in Pervasive Computing (SPC 2005). LNCS 3450. Berlin: Springer-Verlag , 2005 , 70～84.

[8] Damith C.R., Daniel W.E.. Low-Cost RFID Systems: Confronting Security and Privacy. 2004.

[9] Pedro P.L., Julio C.H., Juan M.E. and etc. M2AP: A Minimalist Mutual-Authentication Protocol for Low-cost RFID Tags. 2006.

[10] Ohkubo M. , Suzuki K. , Kinoshita S. . Hash-chain based forward-secure privacy protection scheme for low-cost RFID. In: Proceedings of the 2004 Symposium on Cryptography and Information Security (SCIS 2004) , Sendai , 2004 , 719～724.

[11] S. A. Weis, "Radio-frequency identification security and privacy", Master's thesis, M.I.T. 2003.

[12] Sarma S. E., Weis S. A. , Engels D. W. . Radio frequency identification: Secure risks and challenges. RSA Laboratories Crypto bytes, 2003, 6 (1) : 2～9.

[13] D. Henrici and P. Muller, "Hash-based Enhancement of Location Privacy for Radio-Frequency Identification Devices using Varying Identifiers", PerSec'04 at IEEE PerCom, pp.149-153, Mar. 2004.

[14] Molnar D, Wagner D.. Privacy and security in library RFID: issues, practices, and architectures. In: Proceedings of the 11th ACM Conference on Computer and Communications Security (CCS'04) , Washington , DC , USA , 2004 , 210～219.

[15] Rhee K., Kwak J., Kim S., Won D.. Challenge-response based RFID authentication protocol for distributed database environment. In: Proceedings of the 2nd International Conference on Security in Pervasive Computing (SPC 2005). LNCS 3450.Berlin: Springer-Verlag, 2005, 70～84.

[16] Lee S. M., Hwang Y. J.. Efficient authentication for low cost RFID systems. In: Proceedings of the International Conference on Computational Science and Its Applications (ICCSA2005). LNCS 3480. Berlin: Springer-Verlag , 2005 , 619～627.

[17] Duc DN , Park J , Lee H . Enhancing security of EPC global GEN-2 RFID tag against traceability and cloning . Symposium on Cryptography and Information Security，2006.

[18] Yossef Oren and Martin Feldhofer. A Low-Resource Public-Key Identification Scheme for RFID Tags and Sensor Nodes. In Proceedings of the second ACM Conference on Wireless Network Security - WiSec'09, Zurich, Switzerland, March 2009.

[19] Bongno Yoon. HB-MP++ Protocol: An Ultra Light-weight Authentication Protocol for RFID System. In IEEE International Conference on RFID - RFID 2009, Orlando, Florida, USA, April 2009.