Proceeding of the 2015 IEEE
International Conference on Information and Automation
Lijiang, China, August 2015

Design and Analysis of Security Protocol for RFID without Back-End Database

HAO Yong-sheng
The Missile Engineering, Ordnance Engineering College, 050000, Shijiazhuang, China
1203213797@qq.com

REN Shao-jie
The Missile Engineering, Ordnance Engineering College, 050000, Shijiazhuang, China
RSJ5217@163.com

Abstract- **RFID security protocol is one of the most important ways to solve security problems of RFID system and it is the focus of current research. This article summarized and classified the common security protocols, then proposed a new mutual authentication protocol without the back-end database which aimed at the actual need of military applications and proved the correctness of the new protocol by GNY logic. Safety analysis shows that the new protocol can effectively protect privacy, prevent tracking and avoid synchronization attack and such common problems. The protocol has not only high security, but also the obvious advantage of flexibility.**

Index Terms-RFID; security protocol; back-end database

I. INTRODUCTION

RFID (Radio Frequency Identification, RFID) technology is a non-contact automatic identification technology can be used for information acquisition which has been widely used in buildings, transport, shopping malls, libraries and other fields. Since the initial idea is to use a completely open system, so that RFID system has a variety of potential security risks. At present, physical mechanism and security protocol are the two kinds of ways to solve the problem of RFID system security. Physical mechanism can improve the security of the system to a certain extent, but there are many defects and shortcomings, such as the need to auxiliary equipment, high cost and low repetition utilization. Especially in the field of military, affected by the operational environment and the operational object, the use of physical mechanism has great limitations [1]. Therefore, designing and improving the relevant security protocol to resolve the security issues of RFID system have a very important significance for further application of RFID technology in the military field.

II. RESEARCH STATUS

According to the define of ISO / IECI8000 standard [2], the communication model of RFID system consists of physical layer, communication layer and the application layer, as shown in Fig 1. Physical interface physical layer is mainly responsible for the management between the tag and reader, the definition of signal modulation, time, frequency and coding scheme; communication layer defines communication between tag and reader, the most important thing is to resolve collisions question; application layer is the user information processing layer which represents the tag identification solutions, certification and data processing logic. Normally, the discussed RFID security protocol refers to the application layer protocol, security protocol discussed in this paper also belongs to this category. Currently, the RFID security protocol issue has caused wide attention and further research of scholars both at home and abroad. The existing security protocol can be divided into security protocol with back-end database and security protocol without back-end database.

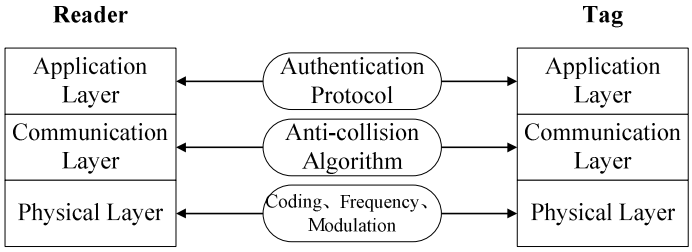

Fig.1 Communication model of RFID system

A. Security protocol with back-end database

The security protocol with back-end database can be applied to the RFID system which usually consists of tags, readers and back-end database, the insecure channel between the tag and reader is analyzed under the assumption that the back-end database has enough storage and computing power [3]. Such common security protocols include Hash-Lock protocol [4], Hash-Chain protocol [5], distributed inquiry - response protocol [6], LCAP protocol [7], the digital library RFID protocol [8] and the public based on encryption key mutual authentication protocol [9].

Hash - Lock protocol uses metaID instead of real ID of tag, effectively avoid the information leakage and tracking, however, due to the process of implementation of the protocol by the clear tag information in an insecure channel transmission, so protocol suffers greater risk of spoofing attack and retransmission attack; tag can automatically update tag ID in Hash -Chain protocol, but the protocol is

978-1-4673-9104-7/15/$31.00 ©2015 IEEE

actually a one-way authentication protocol because the implementation can't confirm the legitimacy of the reader, and the efficiency and cost will be adversely affected because of the two different Hash function the protocol contains; distributed inquiry-response protocol needs two hash operation when completed one certification, security is relatively high, but tag may permanent failure once the accident occurred in the process of certification; LCAP protocol also uses the ask - response mechanism, the tag ID in the implementation of the protocol will be refreshed after each random number encrypted manner so that the certification process can't be copied every time, track and replay attack are prevented efficiently, but there are database synchronization security risks; digital library RFID protocol is mainly based on pre-shared secret pseudorandom functions, so far, the obvious flaws are not found, but the design of tag circuit is complex and the cost is high; in public key cryptography based mutual authentication protocol, different tag and reader share a different key so that RFID system will have good security and privacy, but the efficiency of the protocol will be a sharp drop once tag number is too large.

Different back-end database security protocols have their own advantage and disadvantage. The biggest mutual problem of this kind of protocol is that all parts of RFID system will be unable to work normally once the back-end database failed.

B. Security protocol without back-end database

Security protocol without back-end database was first proposed by Tan et al. Tan's protocol [10] can be successfully resisted in the absence of back-end database to track cases, eavesdropping, cloning and loss of privacy and other attacks, but it is not mutual authentication protocol in the strict sense. The protocol is unable to make effective prevention of synchronized attacks, the anonymity of tag ID can't be guaranteed and repeated Hash functions also brought problems of system efficiency, cost and other aspects. While the security protocol without back-end database put forward relatively late, but soon got the attention of many scholars. References [11-13] have carried out in-depth research on security protocol without back-end database and have achieved some results. In real life, with the application of RFID technology more and more widely, it is of important significance to research the security protocol without back-end database.

In short, there are a lot of security protocols differ in their breach at the present stage, but they can only meet the needs of specific RFID system applications in some ways and can't completely solve the security problems.

III. PROTOCOL DESIGN

In military field, the troop in modern high-tech warfare must have good flexibility, which put forward higher requirements for the reader in portability, mobility, field applicability and other aspects. In this case, the security protocol must also have effective security in the offline (no back-end database) state. Based on this idea, the paper proposed a new RFID security protocol without back-end database.

A. Protocol Initialization

First, the symbols appearing in the protocol is defined as shown in Table 1.

Tab.1 The symbol definitions of new protocol

Symbol	Meaning
C	Certification Center
R_i	The Reader R_i
T_j	The Tag T_j
r_i	The Identity of R_i
t_j	The Key of T_j
ID_j	The Identity of T_j
r_{R_i}	Random Number Generated by R_i
r_{T_j}	Random Number Generated by T_j
$h()$	Hash Function
$w()$	Pseudo-random Function with 2l-bit Output Length
S_m	Communication Seed Updated
S_m^*	Communication Seed before Updating
L_i	Index Table
$\|\|$	Cascade Operation

The new protocol only contains two entities that the reader R and tag T, different reader and tag are distinguished by the subscript i and j, but must introduce the third-party certification center C. The certification center C is not directly involved in each certification, the function of C are mainly reflected in two aspects: on the one hand, C can configure any tag T_j and make the tag T_j get the seed $S_j = h(r_i||t_j)$ which can be used to communicate with specific reader R_i, t_j is key to tag; on the other hand, the certification center C can authenticate any reader R_i and make R_i get the index table L_i which contains all information of tags. Assuming the number of tag is n, so the specific forms L_i can be expressed as:

$$L_i = \begin{cases} S_1 \ , \ S_1^* \ : \ ID_1 \\ \vdots \quad \vdots \quad \vdots \\ S_n \ , \ S_n^* \ : \ ID_n \end{cases}$$

R_i and T_j can calculate pseudo-random function $w()$ and individual hash function $h()$, their respective identities r_i and ID_j don't appear in the authentication process and only used for the configuration of authentication center C. It should be noted that it is safe and reliable for certification center C to configure reader R over a wired connection by SSL protocol.

B. Protocol Description

The process of implementation of the protocol was shown in Figure 2

The process of implementation of the protocol can be described in detail as follows:

$a)$ $R_i \rightarrow T_j$: The reader R_i generates a random number r_{R_i}, and sends it to the tag T_j as $Request$.

$b)$ T_j: The tag T_j generates a random number r_{T_j} after receiving $Request$ from R_i and computing $n_t = w(S_j \oplus (r_{R_i}||r_{T_j})) = n_{t_1}||n_{t_2}$ (" || "represents concatenation operation) according to its own internal seed S_j.

$c)$ $R_i \leftarrow T_j$: The tag T_j sends $r_{T_j}$and n_{t_1} to the reader R_i.

$d)$ R_i: The reader R_i matches the seeds in index table one by one after receiving the returned messages from tag T_j. Calculating $n_m = w(S_m \oplus (r_{R_i}||r_{T_j})) = n_{m_1}||n_{m_2}$, which $m \in [1,n]$ .If $n_{m_1} == n_{t_1}$, going to step $e)$ directly and upgrading the index table seed $S_m = h(S_m)$; otherwise, calculating $n_m = w(S_m^* \oplus (r_{R_i}||r_{T_j})) = n_{m_1}||n_{m_2}$, at this time, if $n_{m_1} == n_{t_1}$, the process goes to step $e)$ and updates the index table seed $S_m = h(S_m^*)$ at the same time .

$e)$ $R_i \rightarrow T_j$: The reader R_i will send $n_{m_2}$to the tag T_j for verification;

$f)$ T_j: The tag compares n_{m_2} and n_{t_2} calculated in step b) when receives n_{m_2} from the reader. If $n_{t_2} == n_{m_2}$, the authentication is successful and the tag $S_j = h(S_j)$.

In the process, n_{t_1} and n_{t_2}represent the front and rear l bits of n_t, n_{m_1} and n_{m_2} correspond front and rear l bits of n_m. Any step from step a)to step f)is not certified will lead to fail.

IV. GNY LOGIC ANALYSIS

Many times, people evaluate the merits of the protocol only by the reasonable degree of the protocol, the correctness of the protocol itself is often ignored. But, the security protocol is different from other protocols, any flaws in design may become the targets of attackers. Therefore, an supplementary analysis of the protocols is very necessary. Formal analysis is such a protocol analysis tool.

GNY logic is one of the most common and the biggest impact of formal analysis method which was proposed in 1990 by Gong, Needham and Yahalom[14]. In fact, GNY logic also belongs to BAN logic class and has the same identifier with BAN logic, but the difference is that GNY logic eliminates the message source and identification assumptions, expands the scope and type of protocol analysis, the definition of relevant rules are more comprehensive and detailed. So, GNY logic has better features and the ability to use.

Next, we will use the GNY logic to judge whether the proposed protocol security and flawed.

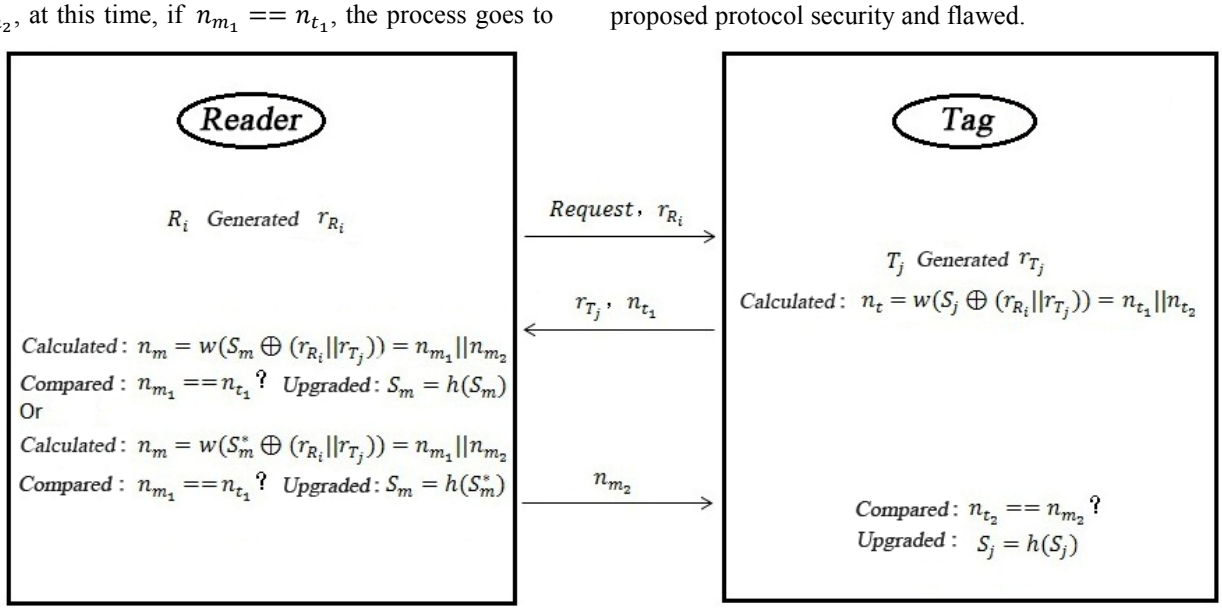

Fig.2 The execution of the protocol

The first step: Established the initial assumptions of protocol

It is assumed that the initial assumptions of protocol can be formalized as follows:

A1: $R_i| \equiv \#r_{R_i}$ A2: $T_j| \equiv \#r_{T_j}$

A3: $R_i| \equiv R_i \overset{h(r_i||t_j)}{\longleftrightarrow} T_j$ A4: $T_j| \equiv T_j \overset{h(r_i||t_j)}{\longleftrightarrow} R_i$

A5: $R_i \ni r_i$ A6: $T_j \ni t_j$

A7: $R_i \ni w()$ A8: $T_j \ni w()$

A9: $R_i \ni h(r_i||t_j)$ A10: $T_j \ni h(r_i||t_j)$

The second step: Established idealized model of protocol

Regulated the execution of agreement with GNY logic language, then obtained the idealized model of the protocol:

M1: $T_j \lhd * r_{R_i}$

M2: $R_i \lhd * r_{T_j}$, $* n_{t_1}$

M3: $T_j \lhd * n_{m_2}$

The third step: Established the security objective of the protocol

The security objective was to demonstrate the reader and tag believe that the freshness of the information interacted with each other, and formalized as:

O1: $R_i| \equiv T_j| \sim \#n_{t_1}$

O2: $T_j| \equiv R_i| \sim \#n_{m_2}$

The fourth step: Proved the protocol

In order to permit $R_i| \equiv T_j| \sim \#\mathrm{n}_{\mathrm{t}_1}$, only need to permit $R_i| \equiv T_j| \sim \# w\left(h(r_i||t_j) \oplus (r_{R_i}||r_{T_j})\right)$

The M2: $R_i \lhd * r_{T_j}$ and receiving rules T_1: $\frac{P \lhd * X}{P \lhd X}$ can deduce:

$$R_i \lhd r_{T_j} \qquad (1\text{-}1)$$

By having rules P_1: $\frac{P \lhd X}{P \ni X}$ and formula (1-1) can be obtained:

$$R_i \ni r_{T_j} \qquad (1\text{-}2)$$

Though formula (1-2),assumption A5 : $R_i \ni r_i$,assumption A7 : $R_i \ni w()$,assumption A9 : $R_i \ni h(r_i||t_j)$ and having rules P_2: $\frac{P \ni X,\ P \ni Y}{P \ni (X,\ Y),\ P \ni F(X,\ Y)}$,we can get:

$$R_i \ni w\left(h(r_i||t_j) \oplus (r_{R_i}||r_{T_j})\right) \qquad (1\text{-}3)$$

Then, the having rules P_1: $\frac{P \lhd X}{P \ni X}$ and formula (1-3) can push:

$$R_i \lhd w\left(h(r_i||t_j) \oplus (r_{R_i}||r_{T_j})\right) \qquad (1\text{-}4)$$

Obviously, formula (1-4) and formula (1-5) can be obtained by the execution of the protocol:

$$R_i| \equiv \otimes(R_i) \qquad (1\text{-}5)$$

$$R_i| \equiv \emptyset\left(w\left(h(r_i||t_j) \oplus (r_{R_i}||r_{T_j})\right)\right) \qquad (1\text{-}6)$$

Though assumption A3 : $R_i| \equiv R_i \overset{h(r_i||t_j)}{\longleftrightarrow} T_j$, assumption A9: $R_i \ni h(r_i||t_j)$, formula (1-4), formula (1-5) , formula (1-6) and message interpretation rule P_2: $\frac{P \ni X,\ P \ni Y}{P \ni (X,\ Y),\ P \ni F(X,\ Y)}$,we can know:

$$R_i| \equiv T_j| \sim w\left(h(r_i||t_j) \oplus (r_{R_i}||r_{T_j})\right) \qquad (1\text{-}7)$$

According to assumption A1 : $\mathrm{R_i}| \equiv \#\mathrm{r_{R_i}}$ and message fresh rule, it's easy to know:

$$R_i| \equiv \# w\left(h(r_i||t_j) \oplus (r_{R_i}||r_{T_j})\right) \qquad (1\text{-}8)$$

Finally, formula (1-7), formula (1-8) and the definition of the freshness can deduce:

$$R_i| \equiv T_j| \sim \# w\left(h(r_i||t_j) \oplus (r_{R_i}||r_{T_j})\right) \qquad (1\text{-}9)$$

In other words, the security objective $R_i| \equiv T_j| \sim \#n_{t_1}$ was proved.

Similarly, another security objective can also be proved by many times use of the message fresh rules, receiving rules message interpretation rule and initial assumptions of the protocol .There will not be a detailed proof.

V. Safety Analysis and Comparison

The article will analyze the security performance of the improved protocol from the following several aspects.

A. Anonymity

Anonymity refers to that the tag ID will not be exposed to steal user privacy in the process of implementation, exposed the privacy protection. In this protocol, the reader obtains the tag information through a hash function $h(r_i||t_j)$, and the seeds in the communication process has been a pseudo-random function $w(S_j \oplus (r_{R_i}||r_{T_j}))$further disguise. According to the unpredictable characteristics of one-way hash function and pseudorandom function , an attacker can't obtain the tag real ID, so the protocol has a good anonymity.

B. Tracking

If attackers can distinguish one tag with other tags according to the content of the communication, we can also say that the tag was tracked. The reader will produce different random number as a request sent to the tag in each certification process, and the tag will reply a new pseudo-random number, so the communication process updated constantly. Therefore, the attacker can't get the same inquiry or response information and it will not track the tag.

C. Replay Attack

Replay attack refers to that the attacker resends the intercepted response message in next process of authentication to obtain certification form tag. This protocol introduces random and pseudo-random number to get involved in the calculation, both the authenticated messages sent form tag to the reader and the authenticated messages form reader to the tag will be different. Even if the attacker intercepts a particular communication message, it is impossible to complete the communication by replaying the intercepted message.

D. Mutual authentication

As can be seen from the execution of the protocol, the tag T_j authenticates the reader R_i by n_{t_1} in step c) and the reader R_i carries on the tag T_j certification through $\mathrm{n}_{\mathrm{m}_2}$ in step e). It's a successful authentication only when the two certification through, which makes the protocol with higher reliability.

E. Desynchronization

To prevent the synchronization attacks, the seed S_j and seed S_j^* before updating are all stored in the index table L_i at the same time in the protocol. It can use the seed last communication saved to obtain certification if the reader updated loss of synchronization between the reader R_i with the tag T_j.

F. Eavesdropping

Attackers intercept communication messages between the reader and the tag and use these messages to develop the strategy to attack the system. In this protocol, the communication data will be changed every time, because each reader will generate a new random number and each hash function of communication seeds can be updated constantly. The eavesdropped messages are different every time, so the attacker can't effectively attack the system according to the eavesdropped messages.

The safety performance of common protocol and the protocol this paper proposed are compared in table 2.Where, √ indicates the protocol have this feature, × indicates the protocol does not have this feature. It is easy to see that the proposed protocol in this paper performs better than other protocol in terms of security.

Tab.2 Security performance comparisons for several protocols

Performance Indicators	Reference [4]	Reference [5]	Reference [6]	Reference [9]	Reference [10]	The Proposed Portocol
Anonymity	√	√	×	√	√	√
Ttracking	×	×	√	√	√	√
Replay Attack	×	√	√	√	√	√
Mutual Authentication	×	×	√	√	×	√
Desynchronization	×	×	×	×	×	√
Eavesdropping	×	×	×	√	√	√

CONCLUSION

In this paper, common security protocols are summarized, classified and compared. Then, combined with the actual needs of RFID technology in the military field applications, a new mutual authentication protocol without back-end database was proposed which a hash function and a pseudo-random function were introduced. GNY logic proved the correctness of the protocol. Compared with common protocols, the new protocol has good performance in anonymity, anti-tracking and synchronization, etc. The new protocol also has many advantages, such as high security, strong flexibility and wide range of application. There will be a practical value.

REFERENCES

[1] ZHANG Lin-he.Construction of Military Logistics System Based on RFID Technology[D].PACKAGING ENGINEERING,2010,31（5）:134-137

[2] International organization for Standardization.ISO/IEC 18000-3. Information Technology AIDC Techniques-RFID for Item Management, March 2003

[3] ZHOU Yong-bin,FENG Deng-guo.Design and Analysis of

Cryptographic Protocols for RFID[J].CHINESE JOURNAL OF COMPUTERS,2006,29（4）：581-589

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

[5] Ohkubo M.,Suzuki K.,Kinoshita S.A cryptographic approach to privacy-friendly tag. In: RFID Privacy Workshop,2003,13（7）：218-227

[6] Rhee K.,Kwak J.,Kim S.,Won D. Challenge-response based RFID authentication protocol for distributed database environment. In: Hutter D. ,Ullmann M. Proceeding of the 2nd International Conference on Security in Pervasive Computing(SPC 2005). Lectures Notes in Computer Science 3450.Berlin:Springer-Verlag,2005,70-84

[7] Lee S. M.,H wang Y. J.,Lee D. H.,Lim J. I. Efficient authentication for low-cost RFID systems. In: Gervasi O.Gavrilova M. L.,Kumar V.,Laganh A.,Lee H. P.,Mun Y.,Taniar D.,Tan C. J. K. eds. Proceedings of international Conference on Computational Science and Its Applications (ICCSA 2005). Lectures Notes in Computer Science3480. Berlin: Springer-Verlag,2005,619-627

[8] Molnar D.,Wagner D..Privacy and security in library RFID: issues,practices,and architectures. In: ACM CCS,2004,11（4）：210-219

[9] ZHANG Heng-shan,GUAN Hui-sheng,HAN Hai-qiang.Public key based mutual authentication protocol for RFID system[J].Computer Engineering and Applications,2010,46（5）：69-72

[10] C. C .Tan, B .Sheng,Q. Li.Severless search and authentication protocols for RFID[C].5th Annual IEEE International Conference on Pervasive Computing and Communications. New York:IEEE Press, 2007:24-29

[11] DENG Miao-lei,WANG Yu-lei,QIU Gang,et al.Authentication Protocol for RFID without Back-End Database[J]. Journal of Beijing University of Posts and Telecommuniations,2009,32（4）：59-62

[12] F. Feng and L. Liu,“ROAD：An RFID offline authentication，privacy preserving protocol with DOS resilience.”IFIP，pp.139-146，2008

[13] ZHAO Bin. Research on Secure and Serverless RFID Authentication and Search Protocols [D] . XIDIAN UNVERSITY, 2011.

[14] Gong L, Needham R, and Yahalom R. Reasoning about belief in cryptographic protocols[C]. Proceedings of the 1990 IEEE Symposium on Research in Security and Privacy, Oakland, California, 1990:234-248.