An Improved Lightweight RFID Mutual-authentication Protocol

Liyun Luo[1, a*], Daowei Liu[1, b]

[1]Guangzhou Vocational College of Science and Technology, Guangzhou 510000, China

[a]kxhily@163.com, [b]daoweijun@126.com

Keywords: RFID, Light-weight, Mutual-authentication, Crossover, CRC.

Abstract. Aiming at the security problems and tag's cost problems of RFID, an improved light-weight RFID mutual-authentication protocol was proposed ,this protocol has proved to be save by BAN logic formal analysis method. Besides, Security analysis shows that the protocol possesses robust security as well as defending against malicious attacks such as disclosure attack, desynchronization attacks ,impersonation attack .It has better security and less consumption resource of computing and storage, etc.

Introduction

Radio Frequency Identification, RFID is a kind of non - contact technology to automatically identify people or objects. This recognition requires no physical contact or any other visible contact [1, 2]. RFID tags because of its small size, easy to carry, low cost, easy to use and so on, RFID system is widely used in supply chain management occasions, digital library management occasions, anti fake electronic passport system, build intelligent network environment [3 ,4], etc.

The RFID system includes three parts, the back-end database, the reader and the tag. The communication channel between the back-end database and the reader is generally considered as safe and reliable; The channel between Reader device and the tag exposed to the air, easy to be monitored, further more, the reader or tag can be forged or cheated, therefore, we need to design a reliable bidirectional authentication protocol for the communication between reader and tag, which is used to ensure the security of the whole RFID system [5, 6].

Many authentication protocols based on pseudo-random number generators have been proposed, which can achieve security and privacy protection, meanwhile, some lightweight RFID authentication protocols based on bit operations and HASH functions have been proposed, but these protocols are more or less exist safe and less efficient problems.

The authentication scheme proposed in the literature [7] can not resist the attack, the attacker can replay the message, so that the key between the reader and the tag is not consistent, thereby undermining the subsequent authentication between the two; The essence of the authentication scheme proposed in the literature [8] is a search protocol, which can not be considered as a two-way authentication protocol; The authentication scheme proposed in the literature [9] can not resist active attacks. The attacker can analyze the reply information of the tag by constantly asking the tags, and then all the key information stored in the tag can be deduced completely; The proposed authentication scheme proposed in the literature [10] cannot provide backward privacy security; The proposed scheme in the literature [11] can not resist brute force attacks, because R1 and R2 use cleartext, so an attacker can easily access the R1 and R2, using the exhaustive method can derive the stored key information from the tag; The literature [12] proposed cross bit operation according to the knowledge of genetic algorithms Cro (X, Y) , with the combination of XOR and Rot algorithm CURAP is proposed, but CURAP is too complex in the operation, and do not make use of their own label information stored, at the same time, after each certification ended, the need to update the content too much, which will to increase the amount of calculation and the increase of storage space, and the analysis shows that the protocol security is insufficient. According to the existing research results, this paper combines CRC and Cro algorithm proposed an improved lightweight RFID mutual authentication protocol. In the premise of not increasing the cost and the amount of calculation of the label, improve the security authentication protocol, make full use of the label itself has stored information as to the double authentication token, thereby reducing the cost of tags target.

Improved Protocol

Implementation of Cross Bit Operation. Assuming that X and Y are two binary arrays with an even number of L bits, $X=x_1x_2x_3...x_L$, $Y=y_1y_2y_3...y_L$; Among them, the values range of x_i and y_i are {0, 1}, i=1, 2,..L; Cro (X, Y) is a new L bit array which is formed by the odd bit of X and the even bit of Y. Cross bit operations can be implemented in the tag as follows: define two pointers P1 and P2,P1 point to X and P2 point to Y, when P1 points to the odd bit of X, give the value of this position to the Even bit of the result, when P2 points to the even bit of Y, then give the value of this position to the odd bit of the result. For example, take the length L=12， set X=111000110110, Y=011001011100, then Cro(X, Y) =110110111001, The specific implementation process as shown in Fig. 1.

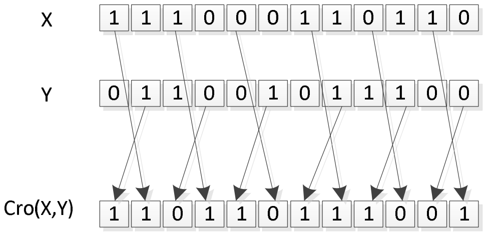

Fig. 1 Crossover operation calculation process.

Symbol Description. Firstly, give the description of each symbol in this protocol:

R: reader
T: tag
ID: The unique identifier of the tag (2L bit length);
ID_L: Identifier of the first half (L bits length of the front);
ID_R: Identifier of the second half (L bits length at the back);
K: The shared key between the tag and the reader (L bits length);
K_{new}: The shared key between the tag and the reader of current round (L bits length);
K_{old}: The shared key between the tag and the reader the last round (L bits length);
r: Random number generated by the reader (L bit length) ;
Cro(X, Y): Crossover bit operation;
CRC(X): Cyclic check function (used to encrypt the value of X) ;
$\oplus$: XOR operation;
||: Connection operation.

Certification Process. The improved RFID protocol authentication process is shown in Fig. 2.

The interpretation of A, B, D, E in the improved protocol:

$A = ID\_R \oplus r$;

$B = CRC(Cro(K \| ID\_R , ID) \oplus (K \| r))$;

$D = CRC(Cro(K , r) \| ID\_R \oplus ID)$;

$E = K_{new} \oplus r$;

$K_{new} = CRC(Cro(r , ID\_R) \oplus K)$.

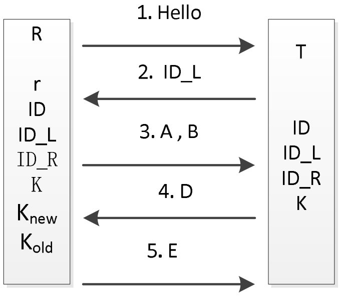

Fig. 2 The improved protocol.

The certification procedure for the entire protocol is described as follows:

(1) The reader sends a "Hello" signal to the tag, and initiates a request for authentication;

(2) After receiving the authentication request which is sent by the reader, the tag will be sent to the reader ID_L stored by itself as a response;

(3) After the reader receives the ID_L sent by the tag, it start to check whether there is a ID_L in the stored information. If does not exist, the label is forged, the certification immediately stopped; If there is, then the reader generates a random number r of length of L bits; and then with the ID_R corresponding to the ID_L to calculate the value of A, using K, ID_R, ID and R to calculate the value of B, and finally pass the value of A and B to the tag;

(4) After receiving the value of A and B sent by the reader, The tag first to calculate A⊕ID_R with ID_L stored by itself, so you can get a random number r, the using the r that has been calculated and the K, ID_R, ID stored by itself to verify the correctness of the B, that is: B`= CRC(Cro(K || ID_R, ID) ⊕(K || (A⊕ID_R))).

If B` and B are not equal, that the reader is a forgery, authentication immediately stop; if B` and B are equal, that the reader is legitimate, then the tag uses the r that generated by itself and the K, ID_R, ID stored by itself to calculate the value of D, and finally sent the value of D to reader;

(5) After the reader receives the value of D sent by the tag, the reader first uses the R which are generated by itself and the K, ID_R, ID stored by itself to verify the correctness of the D, that is:

D`= CRC(Cro(K, r) || ID_R ⊕ ID). If D` and D are not equal, implement step (6); If D` is equal to D, the tag is legitimate, then the reader uses the r that generated by itself and the K, ID_R stored by itself to calculate the value of $K_{new,}$ And start updating the secret key $K_{old} = K_{new}$, K_{new} = CRC(Cro(r , ID_R) ⊕ K) , Then use r to calculate the value of E, and finally sent the value of E to the tag;

(6) The reader uses the r that generated by itself and the K_{old}, ID_R, ID stored by itself to verify the correctness of the D, that is: D``= CRC(Cro(K_{old} , r) || ID_R ⊕ ID).

If D`` and D are not equal, that the tag is a forgery, authentication immediately stop; if D`` and D are equal , that the tag is legitimate, then the reader uses the r that generated by itself and the K, ID_R stored by itself to calculate the value of $K_{new,}$ And start updating the secret key $K_{old} = K_{new}$, K_{new} = CRC(Cro(r , ID_R) ⊕ K), Then use r to calculate the value of E, and finally sent the value of E to the tag;

(7) After receiving the value of E from the reader, firstly the tag uses the K, ID_R stored by itself and the value received from A to verify the correctness of the E, that is: E`= CRC(Cro(A⊕ID_R , ID_R) ⊕ K) ⊕(A⊕ID_R).

If E` and E are not equal, that the reader is a forgery, authentication immediately stop; if E` and E are equal , that the reader is legitimate, Then the tag uses the received r to calculate the value of r ⊕E, then can get Knew, and the tag begins to update the key K = Knew.

BAN Logic Formal Analysis

In this protocol, BAN logic analysis method is used to formalize the protocol. The relevant knowledge of BAN is described in detail in the literature [13], including its syntax, inference rules and steps. Using BAN logic formalized analysis was carried out on the protocol, the procedure is as follows.

(1) Idealized model of protocol

Message ① R→T: Hello;

Message ② T→R: ID_L;

Message ③ R→T: A, B;

Message ④ T→R: D;

Message ⑤ R→T: E.

(2) Anticipated target of the agreement

The validity proved target of this protocol are the four main objectives: G1, G2, G3, G4, that is, the trust between two-way authentication between entities and mutual information.

G1: $R \models D$, R believes D.

G2: $T \models A$, T believes A.

G3: $T \models B$, T believes B.

G4: $T \models E$, T believes E.

(3) Initial assumption of protocol

P1: $R \models R \overset{K}{\leftrightarrow} T$, R believes shared secret key between R and T.

P2: $T \models R \overset{K}{\leftrightarrow} T$, T believes shared secret key between R and T.

P3: $R \models R \overset{ID}{\Leftrightarrow} T$, R believes the ID Shared secret information between R and T.

P4: $T \models R \overset{ID}{\Leftrightarrow} T$, T believes the ID Shared secret information between R and T.

P5: $R \models R \overset{ID\_L}{\Leftrightarrow} T$, R believes the ID_L Shared secret information between R and T.

P6: $T \models R \overset{ID\_L}{\Leftrightarrow} T$, T believes the ID_L Shared secret information between R and T.

P7: $R \models R \overset{ID\_R}{\Leftrightarrow} T$, R believes the ID_R Shared secret information between R and T.

P8: $T \models R \overset{ID\_R}{\Leftrightarrow} T$, T believes the ID_R Shared secret information between R and T.

P9: $R \models \#(r)$, R believes the freshness of random number r.

P10: $T \models \#(r)$, T believes the freshness of random number r.

P11: $T \models R \mid\Rightarrow A$, T believes R's jurisdiction of A.

P12: $T \models R \mid\Rightarrow B$, T believes R's jurisdiction of B.

P13: $R \models T \mid\Rightarrow D$, R believes T's jurisdiction of D.

P14: $T \models R \mid\Rightarrow E$, T believes R's jurisdiction of E.

(4) The reasoning process of the protocol

From the message ④, we can get $R \triangleleft \{D\}$ (R Once received message D) , and from the initial hypothesis P1 and message meaning rules $\frac{P \models P \overset{K}{\leftrightarrow} Q, P \triangleleft \{X\}_K}{P \models Q \mid\sim X}$ (If the main body of the P believes the Shared key between the main body of P and Q, and P has received the encrypted X, which Encrypted with K, Then P believes the message X sent from the main body of Q), then we can get $R \models T \mid\sim D$

By the assumption of P9 and message freshness rules $\frac{P \models \#(X)}{P \models \#(X,Y)}$, (If a part of a message is fresh, then the whole message is fresh) then we can get $R \models \#(D)$.

According to the formula $R \models T \mid\sim D$ and $R \models \#(D)$ which had been derived, and random number verification rules $\frac{P \models \#(X), P \models Q \mid\sim X}{P \models Q \models X}$, we can get $R \models T \models D$

Based on $R \models T \models D$, Initialization hypothesis P13 and Jurisdiction rule $\frac{P \models Q \Rightarrow X, P \models Q \models X}{P \models X}$, we can get $R \models D$. Therefore, the target G1 is proved.

By using the above conditions and rules, the same, in the same way, we can get $T \models A$, $T \models B$ and $T \models E$. That is to say, target G2, G3 and G4 have been proved, not repeat them here.

Security Analysis

Fake Attack. When the attacker disguised as a legitimate reader, you can obtain the values of ID_L and D, but the attacker cannot get the values of ID and ID_R, therefore unable to verify correctness of D, so that the identity of the attacker will be exposed; When the attacker disguised as a legitimate tag, you can obtain the values of A, B and E , but the attacker can not get the values of ID, ID_R and the key shared between ID and ID_R, Therefore, the attacker can not obtain the value of random number r by calculating, so the attacker is unable to calculate the correct D, at last, the attacker can't calculate the correct shared key K because of the lack of the values of ID , ID_R and other necessary information. Based on the above analysis, we can know that this authentication protocol can resist the fake attack.

Tracking Attack. The attacker disguised as a legitimate reader to send information to the tag, he can get the tag response information: ID_L and D, in an attempt to track the activities of the tag according to the response information. Although the whole certification process ID_L is expressly sent, but the protocols used in the calculation process is ID_R, but there is no relationship between ID_R and ID_L, at the same time in the authentication process no transmission related with ID_R information, so the attacker can not intercept the ID_R, even if the attacker gets D, there is no other role; And because the whole process of transmission of information, information is encrypted by the cyclic redundancy check function and then transmitted, even if the attacker can get information, there is still no way to get the shared key K, so the authentication protocol in this paper can resist the attack.

Replay Attack. In the process of the whole protocol authentication, the reader can ensure the freshness of the information by means of random number r. Even if the attacker disguised as a legitimate reader, generate a random number r, to deceive the tag to obtain privacy information, but the attacker unable to calculate the correct values of A and B, because of the lack values of ID_R and shared key K, the tag requires only a simple calculation can identify the authenticity of the reader, and after each authentication end, both the reader and the tag will be updated the key, at the same time, the reader will also be stored shared key K_{old} which was authenticated last time. Therefore, even if the attacker replay the message, the authentication will not cause any privacy leakage, so the authentication protocol can resist replay attack.

Brute Force Attack. All messages transmitted during the entire protocol authentication process. in addition to ID_L is transferred expressly, other messages are encrypted and then transmitted, and the attacker is unable to get ID_R, ID and shared key K in advance, so the attacker could not get any useful information, even if they intercept the ID_L; Meanwhile, each certification end between the reader and the tag, there will be a shared key update process, which makes the shared key used in each round of authentication process between the two are not the same, plus the attacker just can get the values of A, B and D, and these three values are the result of encryption, and there are ID_R, ID, K and R these four variables are unknown to the attacker, the attacker wants to use brute force method to brute force to get the shared key K is not realistic, so this authentication protocol can resist the violent crack attack.

Desynchronization Attack. In order to destroy the consistency of the key between the tag and the reader, the attacker can attack in the following ways: (1) the attacker makes the tag end to be updated, and the reader is not updated; (2) The attacker makes a key update between the tag and reader ends, but the parameters between the two update is not consistent.

In this protocol, the update of the shared key is first after the reader is calculated, and sent it to the tag after a simple encryption, after the tag received E, Firstly, according to the information stored in their own to verify the correctness of the E, only under the premise that E is correct, the tag will be updated for the key, otherwise, the update operation will not be carried out. Throughout the certification process, the attacker does not have the values of ID_R and ID, so the attacker can not calculate the shared key which is updated. At the same time the reader stored current round of the shared key K and the last round of authentication shared key K_{old}, therefore, even if using K couldn't calculate the right results, still we can use the $K_{old,}$ to calculate, so this authentication protocol can resist desynchronization attack.

Performance Analysis

The performance of the lightweight RFID bidirectional authentication protocol is evaluated in terms of the amount of computation, storage space and so on. The performance comparison between this protocol and several other lightweight authentication protocols is shown in Table 1:

In Table 1: this agreement only need to store the ID, ID_L, ID_R, K of the four variables, so as to reduce the storage space of RFID tags; The reader generates a random number r, the tag does not generate random number, so the end tags do not need to install the random number generator, reducing the total number of gate circuit at the same time, appropriate to reduce the cost of tag; At the end of each certification between tag and reader, the complex calculation process of the shared key is calculated at the end of the reader, and then passed to the tag, the tag only need a simple XOR operation can be get the shared key, thereby reducing the amount of calculation of the end tag to a certain extent; This protocol the tag end is used method of connection, XOR, cross operation, less computation of cyclic redundancy check, so as to ensure the computation of the certification process does not increase significantly.

Table 1. Lightweight RFID authentication protocol performance comparison.

Protocol	Computational requirements	Storage space
LMAP	$\wedge$ $\vee$ $\oplus$ $+$	6L
SASI	$\wedge$ $\vee$ $\oplus$ $+$ Rot	7L
Gorssamer	$\oplus$ $+$ Rot MixBits	7L
This protocol	$\|\|$ $\oplus$ CRC Cro	4L

Summary

This paper presents an improved lightweight RFID bidirectional authentication protocol. Make full use of tag ID information stored by the reader and tag by themselves as the two certified messenger, by using a simple CRC operation and cross bit operation at the end of the tag to achieve mutual authentication between the tag and the reader, and under the premise of ensuring no increase in the amount of calculation, the protocol can effectively resist various denial of service attacks, desynchronization attacks, impersonation attacks and other malicious attacks, ensuring that the limited resources of low cost to complete the two-way authentication on the tag. The correctness and security of the protocol are verified by the formal analysis of BAN logic.

References

[1] Z. H. Ding, J. T. Li, B. Feng, Research on hash-based RFID security authentication protocol, J. Comp. Res. Develop. 46(4) (2009) 583-592.

[2] C. S. Ma, Low cost RFID authentication protocol with forward privacy, Chin. J. Comput. 34(8) (2011) 1388-1398.

[3] International Telecommunication Union, ITU Internet Reports 2005: The Internet of Things, Geneva: ITU, 2005.

[4] L. Gong, et al. Reasoning About Belief in Cryptographic Protocols. In Proceedings of the 1990 IEEE Computer Society Symposium on Research in Security and Privacy, IEEE Computer Society Press, Los Alamitos, California, 1990, 5 234-248.

[5] Y. M. Jin, Q. Y. Wu, et al. RFID Lightweight Authentication Protocol Based on PRF, J. Comp. Res. Develop. 51(7) (2014) 1506-1514.

[6] M. Ohkubo, K. Suzuki, S. Kinoshta, Hash-chain based for-ward-secure privacy protection scheme for low-cost RFID, Proceedings of the 2004 Symposium on Cryptography and Information Security, Berlin: Springer-Verlag, 2004, 719-724.

[7] G. Godor, S. Imre, Hash-based mutual authentication protocol for low-cost RFID systems, Proc of the 18th EUNICE Conf on Information and Communications Technologies. Berlin: Springer, 2012, 76-87.

[8] A. Miyaji, M. S. Rahman, KIMAP: Key-insulated mutual authentication protocol for RFID, Int. J. Autom. Identific. Technol. 3(2) (2011) 61-74.

[9] M. S. I. Mamun, A. Miyaji, M. S. Rahman, A secure and private RFID authentication protocol under SLPN problem, Proc of the 6th Int Conf on Network and System Security, Berlin: Springer, 2012: 476-489.

[10] B. Alomair, J. Cuellar, R. Poovendran, Scalable RFID systems: A privacy-preserving protocol with constant time identification, IEEE Trans on Parallel and Distributed Systems, 23(8) (2012) 1-10.

[11] S. H. Wang, S. J. Liu, D. W. Chen, Scalable RFID Mutual Authentication Protocol with Backward Privacy, J. Comp. Res. Develop. 50(6) (2013) 1276-1284.

[12] Z. Y. Du, G. A. Zhang, H. L. Yuan, Crossover Based Uitra-lightweight RFID Authentication Protocol, Comput. Sci. 40(11) (2013) 35-37.

[13] Y. Tian, G. L. Chen, J. H. Li, A new ultra-lightweight RFID authentication protocol with permutation, IEEE Commun. Lett. 16(5) (2012) 70.