Dynamic Security Authentication Protocol Based on Hash Function for RFID System

Baolong Liu, Bing Yang

Abstract—In order to ensure the information security of the RFID system, this paper proposes a dynamic security authentication protocol based on hash function to prevent asynchronous attack within RFID system. The proposed protocol uses the tag key and the tag ID updating method to ensure the two-way authentication between the tag and the reader to avoid asynchronous attack. The correctness of the protocol is proved by using BAN logic analysis. The experimental results show that the protocol proposed can satisfy the security requirement of RFID system. Compared to existing security protocols, the presented protocol has improved the security level of RFID system. The solution can be implemented in the hardware environment, which provides a reliable approach for RFID system application in practical.

***Keywords*—**RFID systems; authentication; asynchronous attack; hash function; BAN logic.

I. INTRODUCTION

RADIO Frequency Identification (RFID) is an automatic recognition technology that utilizes spatial coupling to realize wireless contact of two-way communication. It can automatically identify target objects and transmit information. Compared to the commonly used identification methods (such as bar code, two-dimensional code), RFID tags has advantages of moved recognition, fast read and written. RFID system has high precision [1], adapting to environmental capacity, strong anti-interference, traceability and positioning at any time. Based on the advantages of RIFD system, it is widely used in the retail, logistics and other fields.

However, RFID system has information security and privacy issues. Criminals using open wireless environment vulnerabilities carry out illegal attacks, which will cause the system disorders, and even confidential disclosure. There are five major security risks: data privacy, replay attacks, location tracking, forged attacks and asynchronous attack.

Two methods are deployed to solve the security and privacy problems of RFID including: 1) Physical methods of security mechanisms, such as inactivation operation, using Faraday net to shield the signal, active interference. 2) Logical methods based on information security mechanism, which mainly focuses on authentication technology [2]. Authentication technology can solve some security issues effectively relating to RFID system. Experts and scholars have put forward a lot of RFID security protocols [3]-[4] about the logic of authentication. As the RFID tag for the operation of the memory is very limited, it is necessary the protocol proposed has small space and high security.

In order to improve security, dynamic security authentication protocols and low cost authentication protocol (LCAP) [10] are often adopted in RFID system. The security authentication protocols based on dynamic refresh tag ID are hash-based protocol using varying identifiers. The dynamic refresh tag ID is similar to the hash chain security authentication protocol, but it synchronously updates the relevant authentication data. By adding the random number generator in the system so that the ID exchange information of each response is different. It can resist the retransmission attack. The hash-based protocol also uses varying identifiers, and the tag update ID after only receiving the verification message, so there is a potential security risk of database asynchronous, and the protocol cannot resist the attacker's blocking attack. In addition, the agreement also takes up a lot of storage space. The LCAP protocol is an interrogation-response protocol characterized by using the left and right portions of the hash encrypted value to authenticate. The protocol dynamically refreshes the tag to ensure that the tag responds randomness after each end of the authentication process. It can effectively prevent replay attacks, fake attacks. Similar to the hash-based ID protocol, the tag also updates the ID after receiving the message and the authentication of the reader, and the database receives the message. Therefore, if the attacker at this time initiates into the camouflage or signal shielding attacks, the authentication data is asynchronous.

In order to overcome problem of authentication information asynchronous, several solutions have been proposed. Huang and Shieh [11] proposed a secret search protocol to solve privacy problems by providing a search mechanism for encrypted data. The protocol directly searches the password which does not need to be decrypted to improve performance. The main drawback of this protocol is that it uses a one-way hash function and therefore it does not conform to the EPC standard. Mtita et al. [12] have developed two mutual authentication and tag searching protocols, which the authors claimed that their agreement requires low computational resources, and readers and tags does not share any secrets.

This work is partially supported by Science & Technology Program of Shaanxi Province with project "2017GY-196", and the Opening Fund of State and Local Engineering Laboratory of Advanced Network and Monitoring Control with project "GSYSJ2016001".

Baolong Liu is with the Department of computing Science & Engineering, Xi'an Technological University, Xi'an 710021, Shanxi, China (corresponding author; e-mail: liu.bao.long@xatu.edu.cn.).

Bing Yang is with the Department of computing Science & Engineering, Xi'an Technological University, Xi'an 710021, Shanxi, China.

However, the server shares the temporary identifier, key and the access rights of the tag with the reader. These protocols are also susceptible to DoS and asynchronous attacks [13] because opponents can block the last messages individually and perform key updates through tags and readers in mutual authentication and tag searching protocols. The tag searching protocols was presented by Zheng and Li using Bloom filter and hash function to identify the 'wanted' tags among a set of tags that are in the field of the reader [14]. Chen et al [15] also adopted the Bloom filter, but with an iterative way identifies the desired tag in the field of readers without querying tags. In both solution, the reader and the tag use hash function to determine which bit is checked to select the candidate. Portions of the framework of the slotted Aloha protocol also are adopted in other approaches. For example Shahzad and Liu [16] use a standardized framework to estimate the number size of a given tag group readers in the Aloha protocol. Readers broadcast available numbers of slots, and each tag selects a time slot to respond. When the number of tags is estimated in the reader field, it would begin with initial step rather than searching for a particular tag. Gong et al. [17] used the framework of the Aloha method. The method focuses on the probability, which means a tag participates and generates a hash value during the authentication process, and it determine the number of slots used in response to the reader rather than an index that focuses on time efficiency. However, the research above cannot determine whether the Aloha protocol is valid and safe.

This paper presents RFID security authentication protocol based on dynamic ID [18] and index value updating. Compared to other protocols, the proposed protocol uses the ID information and index value updated simultaneously [19]. All the tag's related key information is not directly exposed as well as the index value in the entire process of identification. The protocol can ensure the reliability of identity authentication to a certain extent. The tag only needs to generate once a random number, reducing the computational redundancy of the tag. The protocol proposed can not only effectively protect the security of RFID systems but also reduce storage capacity, communication and the computational load between the two sides. The correctness and security of presented method is proved by using BAN logic. The experimental results show that the protocol proposed can satisfy the security requirement of RFID system.

II. The Proposed Security Protocol

The assumptions of this protocol are as follows.

1. The server and the reader is a wired transmission, which means they are connected physically [20]. It can be seen as a secure channel. The reader and the tag is a wireless transmission channel. Because of non-physical connected, it can be seen as an unsecure channel, which means that the attacker can intercept and control the channel data.

2. The tags referred to the protocol are low-cost passive tags, and the resources of each tag are strictly limited. Each tag in the protocol needs to have the capabilities of unidirectional hash function operation, random number generation, XOR operation and connection operation.

3. The tag will not be easily cracked by the attacker [21], which means the attacker cannot obtain the internal information of the tag, and one-way hash function is safe enough for violent crack from the attacker.

A. Initial conditions and related instruction

For the security authentication protocol with dynamic ID, the random number generators are the same to ensure mutual authentication for the tag, the reader and the server. The backend database stores the data pair (RID, θ) of the legal reader and the data of the legal tag (I_{jold} , I_{jnew} , ID_{old} , ID_{new} , K_{i} , S_{i}) and data table to store the random number of the reader. The database needs to read the current time and has the capabilities of hash function operation, random number generation operation, XOR operation and connection operations. An index value is used to verify the identity of the tag in the first step, which consist of 8-bit binary numbers such as '11111110'. The ID information is used to verify the identity of tag again to ensure its freshness, which consists of 16-bit numbers.

The reader stores data pair (RID, θ) and the tag also stores data tuple ($I_j, ID, K_{\text{i}}, S_{\text{i}}$), and its data is always fresh in the authentication process. K_{i} and S_{i} also consist of 16-bit number to make the calculation complex. The attacker is not easy to eavesdrop the key data of the tag. For the initial state, there are two conditions as follows: $I_{jnew} = I_{jold}$ and $ID_{\text{new}} = ID_{old}$

The symbols adopted in the protocol are described in Table 1.

Table 1. The description of symbols adopted in protocol

Signs	Description
R_{r}	Random number generated by reader
R_t	Random number generated by tag
$I_{\text{j}old}$	The old index value of the jth tag
$I_{\text{j}new}$	The new index value of the jth tag
ID_{old}	The old ID information of the tag
ID_{new}	The new ID information of the tag
K_{i}	Secret value shared by the tag and the database
S_i	The secret value of the tag
$H(\cdot)$	Hash function
$\oplus$	XOR operator
$\|\|$	Connection operator
θ	Excepted communication delay
$PRNG(\cdot)$	Random number operator
RID	The ID information of the reader

B. Authentication process

The statement of authentication protocol is divided into eight steps. The implementation of the authentication process is shown in Figure 1.

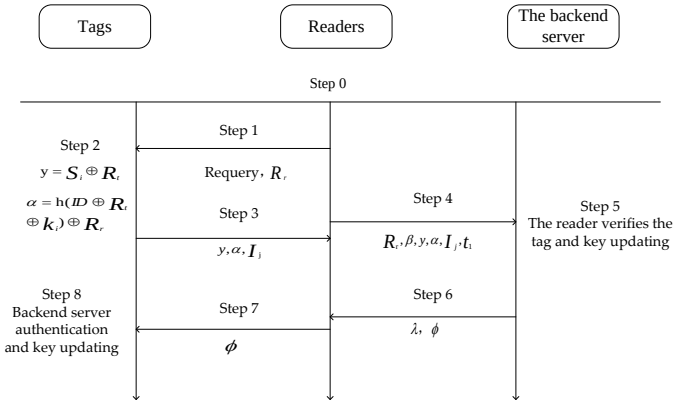

Fig 1. The detailed authentication process

The specific authentication process is as follows.

1. The reader generates a random number R_r and sends query and R_r to the tag as an authentication request, and record the current time t and R_r.

2. After receiving the reader request, the tag generates a random number R_t and records the random number into its memory area. Using ID, K_i and S_i calculates the following operation as: $y = S_i \oplus R_t$, $\alpha = h(ID \oplus R_t \oplus K_i) \oplus R_r$

3. Tag sends y, α and I_j to the reader.

4. The reader using current time t_1 checks whether the inequality $t_1 - t \le \theta$ is satisfied. If the inequality is satisfied, the formula $\beta = h(RID \| R_r)$ is computed, and the results of α, β, y, R_r, I_j, t_1 are sent to the backend database, otherwise the authentication is ended up.

5. After receiving the message from the reader, the back server performs the following operations.

• The server obtains current time t_2 and checks whether the inequality $t_2 - t_1 \le \theta$ is satisfied. If it is satisfied then continue with the next step, otherwise authentication process is stopped.

• The server queries random number table T. If R_r is found, the database may be attacked by default or a system error occurred, otherwise, the process continues next step and stores this random number into the table for the next authentication.

• In order to authenticate the reader, the server calculates $\beta' = h(RID \| R_r)$. If $\beta = \beta'$, the identity of the reader is authenticated successfully, otherwise, the process is terminated.

• In order to authenticate the tag, the server queries the tag index value I_j in the list. If matched item is found, the process continues to next step, otherwise, the authentication process is stopped.

• The generated random number R_t by tag can be calculated using the secret value S_i and y in tag's list. With the tag's data ID_{new}, the server calculates $\alpha' = h(ID_{new} \oplus R_t \oplus K_i) \oplus R_r$. If $\alpha = \alpha'$, the server updates the tag's ID value and does following operations: $ID_{new} = ID \oplus h(ID \| R_t)$, $ID_{old} = ID_{new}$. If $\alpha \ne \alpha'$, the server computes the value $\alpha' = h(ID_{old} \oplus R_t \oplus K_i) \oplus R_r$. If $\alpha = \alpha'$, the tag's ID keeps unchanged, otherwise, the authentication process stopped.

• For the next round authentication process, the data updated are as follows: $I_{jnew} = PRNG(I_j \oplus K_i)$, $I_{jold} = I_{jnew}$.

• Finally, the server calculates the data for the reader and the tag to authenticate the identity of the backend server in the next step: $\lambda = RID \oplus ID \oplus R_r$, $\phi = h(ID \| R_t)$.

6. The server returns λ, ϕ to the reader side.

7. The reader obtains the ID value of the tag according to its own RID and the random number R_r by the exclusive OR operation with λ, and sends the value ϕ to the tag.

8. The tag authenticates identity of the backend server and updates the key of the tag itself. The tag calculates the formula $\phi' = h(ID \| R_t)$. If $\phi = \phi'$, the tag updates the value of ID and the index value of itself: $I_{jnew} = PRNG(I_j \oplus K_i)$ and $ID_{new} = ID \oplus h(ID \| R_t)$, otherwise, the authentication process is terminated.

III. Security Analysis

The presented protocol can resist most of attacks for RFID system. The detailed analysis is as follows.

• Data privacy. The messages sent in the solution are encrypted using the hash function and the XOR operation. Because the hash function is the one-way, the attacker is difficult to obtain *ID*, *RID* and other confidential information. As for the confidentiality of message $y = S_i \oplus R_t$, the tag produces different random number, even if the attacker intercepts the response message in a few rounds of certification process, each response value is not the same, and the attacker cannot obtain the secret value of the tag.

• Replay attack. In the protocol proposed, the reader and the server need to check whether expected communication delay is satisfied when they receives a response message. If attacker repeats the request of the reader in the authentication process, the server side will check it using expected communication delay θ, and the attack will be filtered out in the first time by the server. If the tag request is reordered, it is

also possible to determine whether the communication delay is satisfied at the reader side. With solution above, the replay attack is avoided totally.

• Fake attack. If the attacker intercepts the reader's requested information and impersonates the reader to send message, the tag responds the attacker to send the message. Since the reader and the backend server are physically connected, the attacker cannot obtain the message transferred between reader and backend server. When the attacker counterfeits reader, with the identifier of the *RID*, the identity authentication will be failed. If the attacker intercepts the tag's responded message and sends the counterfeit tag to the reader, the first time each authentication process, the reader and the tag will generate a random number, which means that each of the authentication responses of the tag is not the same, and the attack can be prevented. In addition, the backend server and the reader must determine whether the expected communication delay is satisfied once received the response message. The fake attack cannot be established.

• Position tracking. Theoretically, an attacker can attack [22] the tag by intercepting the status information. Since the information in this protocol is encrypted using hash function and the XOR operation, and the ID of each communication tag is dynamically updated. In this way, the information for each response is different, so the attacker is difficult to intercept the information with a particular tag, and cannot track the tag location [23].

• Asynchronous attack. The tag and the backend server only update the corresponding index value and the tag identifier after the mutual authentication is finished successfully. Assuming the tag does not update the message in the current round due to some reasons, it cannot affect the next step of authentication because the server store two pairs of necessary data. In the next round authentication process, if the server side cannot obtain the corresponding message I_{jnew} and ID_{new} in the list, the server queries the list for I_{jold} and ID_{old}, and the corresponding index value and *ID* value are temporarily not updated. By this method, the generation of the asynchronous attack is prevented effectively.

Table 2 shows the security comparison of protocol proposed with existing solutions. It can be seen clearly that the proposed protocol has the best security performance compared to existing protocols, and it can resist the asynchronous attack.

Table 2. Security comparison with other protocols

Attacks	[11]	[14]	[15]	[16]	[17]	ours
Data privacy	√	√	√	√	√	√
Replay attack	×	×	×	×	×	√
Fake attack	√	×	×	×	×	√
Position tracking	√	√	√	√	√	√
Asynchronous attack	√	×	×	×	×	√

Notation: '√' indicates that the solution can prevent attack, and '×' indicates that the solution cannot resistant attack.

IV. BAN Logical Analysis and Proof of Security

The BAN logic provides an effective way for the formal analysis of the protocol. Logic only discusses the security of the authentication protocol at the abstraction level. It does not take into account the security flaws caused by the concrete implementation of the protocol and the flaws caused by the shortcomings of the encryption system. In general BAN logic reasoning is about to infer the specified protocol whether achieve the desired effect using the relevant rules in the BAN logic and the idealized protocol assumptions to.

Before using the BAN logic proves the protocol, the authentication body is usually represented by a concise reasoning symbol. The tag is denoted by *T*, the reader is denoted by *R*, and the ID of the tag is represented by *IDT*.

A. Establish and idealized protocol model

M1: $R \rightarrow T : Query, R_r$

M2: $T \rightarrow R : \alpha = h(ID \oplus R_t \oplus K_i) \oplus R_r$

$$y = S_i \oplus R_t \quad I_j$$

M3: $R \rightarrow T : \phi = h(ID \| R_t)$

where, M_1, y and I_j are expressly transmitted, and they have no effect on the logical attributes of the analysis protocol. Above model can be converted to the following BAN logical language.

M2: $R \lhd\!< h(IDT, R_t, K_i) >_{R_r}$

M3: $T \lhd h(IDT, R_t)$

B. Protocol initialization hypothesis

P1: $R \mid\equiv R \xleftrightarrow{R_r} T$

P2: $T \mid\equiv T \xleftrightarrow{R_r} R$

P3: $R \mid\equiv R \xleftrightarrow{IDT} T$

P4: $T \mid\equiv T \xleftrightarrow{IDT} R$

The above four initial assumptions are obvious. For assumption P1, because R_r (random number generated by the reader) is always fresh, it is believed that it sent R_r is fresh. *IDT* is the tag itself identifier, and it is certainly believed that *IDT* is fresh.

C. The expectations of the protocol

The expected objective of this protocol is to achieve:

(1) $R \mid\equiv T \mid\sim IDT$

(2) $T \mid\equiv R \mid\sim \mathrm{IDT}$

D. Proof of the authentication process

The proving process is as follows.

(1) Proof evidence for objective: $R|\equiv T|\sim IDT$

With M2:

$$R \lhd\!< h(IDT, R_t, K_i) >_{R_r},$$

and the initial hypothesis P1:

$$R|\equiv R \xleftrightarrow{R_r} T$$

Using the message meaning rule

$$\frac{P|\equiv P \xleftrightarrow{Y} Q \wedge P \lhd (X)_Y}{P|\equiv Q|\sim X},$$

We can obtain result:

$$R|\equiv T|\sim h(IDT, R_t, K_i).$$

With M2:

$$R \lhd\!< h(IDT, R_t, K_i) >_{R_r},$$

using the receive message rule

$$\frac{P \lhd (X.Y)}{P \lhd X}$$

We can obtain result:

$$\frac{R \lhd\!< \mathrm{h}(IDT, R_t, K_\mathrm{i}) >_{R_r}}{R \lhd (IDT, R_t, K_i)}.$$

It indicates that

$$\mathrm{R} \lhd (IDT, R_\mathrm{t}, K_\mathrm{i}).$$

From the message

$$R|\equiv T|\sim h(IDT, R_t, K_i)$$

and

$$\mathrm{R} \lhd (IDT, R_\mathrm{t}, K_\mathrm{i}).$$

Using logical community rule

$$\frac{P|\equiv Q|\sim H(X_1, X_2, \cdots\cdots X_\mathrm{n}) \wedge P \lhd X_1, X_2, \cdots\cdots, X_n}{P|\equiv Q|\sim (X_1, X_2, \cdots\cdots, X_n)}$$

We can learn that

$$\frac{R|\equiv T|\sim \mathrm{h}(IDT, R_t, K_i) \wedge R \lhd (IDT, R_t, K_i)}{R|\equiv T|\sim (IDT, R_t, K_i)}$$

The following conclusion can be achieved.

$$R|\equiv T|\sim (IDT, R_t, K_i)$$

With the belief rule

$$\frac{P|\equiv Q|\sim (X,Y)}{P|\equiv Q|\sim X}$$

We can get

$$\frac{R|\equiv T|\sim (IDT, R_t, K_i)}{R|\equiv T|\sim IDT}$$

And objective (1) is derived as

$$R|\equiv T|\sim IDT.$$

(2) Proof evidence for objective: $T|\equiv R|\sim \mathrm{IDT}$

With M3:

$$T \lhd h(IDT, R_t)$$

and the initial hypothesis P2:

$$T|\equiv T \xleftrightarrow{R_\mathrm{t}} R$$

Using the message meaning rule

$$\frac{P|\equiv P \xleftrightarrow{K} Q \wedge P \lhd (X)_K}{P|\equiv Q|\sim X}$$

We can get

$$\frac{T|\equiv T \xleftrightarrow{R_\mathrm{t}} R \wedge T \lhd h(IDT, R_t)}{T|\equiv R|\sim h(IDT, R_t)}$$

And the result can be obtained.

$$T|\equiv R|\sim h(IDT, R_t).$$

With the message M3:

$$T \lhd h(IDT, R_t)$$

Using receive message rule

$$\frac{P \lhd (X,Y)}{P \lhd X}$$

We can obtain

$$\frac{T \lhd h(IDT, R_t)}{T \lhd IDT, R_t},$$

and that is to say

$$T \lhd IDT, R_\mathrm{t}.$$

With the message

$$T|\equiv R|\sim h(IDT, R_t)$$

and

$$T \lhd IDT, R_\mathrm{t}.$$

Using logical community rule

$$\frac{P|\equiv Q|\sim H(X_1, X_2, \cdots\cdots X_\mathrm{n}) \wedge P \lhd X_1, X_2, \cdots\cdots, X_n}{P|\equiv Q|\sim (X_1, X_2, \cdots\cdots, X_n)}$$

We can deduce the result

$$\frac{T|\equiv R|\sim h(IDT, R_t) \wedge P \lhd IDT, R_t}{T|\equiv R|\sim (IDT, R_t)}.$$

This means that

$$T|\equiv R|\sim (IDT, R_t).$$

From the belief rule

$$\frac{P|\equiv Q|\sim (X,Y)}{P|\equiv Q|\sim X}$$

we can obtain

$$\frac{T|\equiv R|\sim (IDT, R_t)}{T|\equiv R|\sim IDT}$$

Finally, the objective (2) can be derived as

$$T|\equiv R|\sim IDT.$$

The protocol proposed in the paper can be deduced by the formal analysis of the BAN logic, so the protocol can effectively achieve the security objectives of the two-way legal authentication of tags and readers in the RFID sensor network.

V. Experimental Results

A. Experimental environment

All the experimental is performed on a PC with a 3.3GHz, 2GB of RAM, and the Windows 7 32 bits operating system. The algorithms are coded in Java, and the backend database is deployed with MySQL. Readers are wired connect to backend server, and communication of readers and tags are wireless. In simulation process, all calculation, verification and updated operations in the backend server are completed by the computer, and the read/write device for tags is accomplished using MCU-51 and RF module. The tag uses the passive MIFARE Plus IC card. The hardware for simulation is shown in Figure 2.

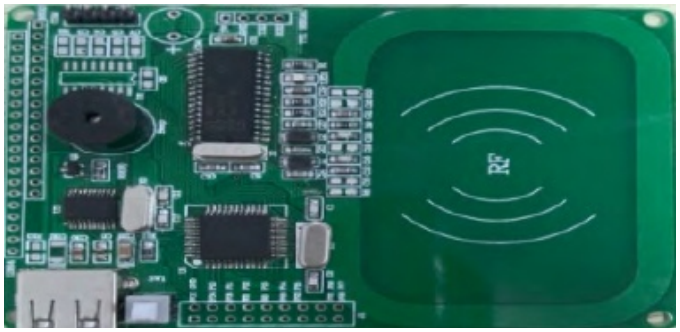

Figure 2. Hardware used for simulation

B. Experimental flowchart

According to authentication process, the flowchart used to simulate the experimental is shown in Figure 3.

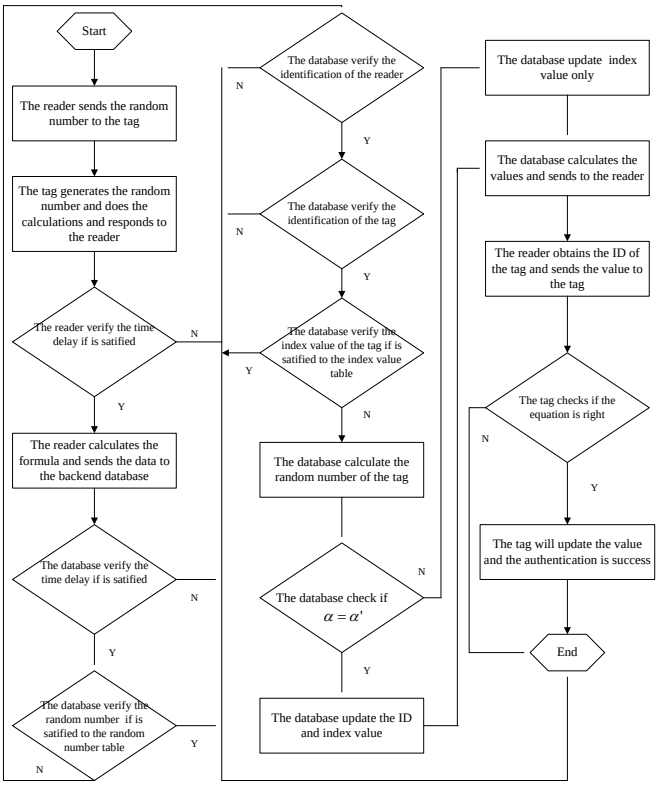

Figure 3. The flowchart for simulation

C. Experimental results

Figure 4 is the main interface for system testing. As shown in Figure 4, the menu "Reader" is used to complete the process of authentication between readers and tags. The menu "Database" is used to store information exchanged within the whole authentication process.

Figure 4. The main interface for testing

When click the menu "Reader", the detailed items to complete authentication is shown in Figure 5.

Figure 5. The detailed authentication processing

At the beginning state, the request signal is generated automatically by default with random number after clicked the button "Request authentication". The request signal is corresponding to the variable R_r as described above.

When request signal is generated, user inputs the tag index or generated by system, and clicks the button "Tag response" to get result as shown in Figure 6. The tag responses the random number calculated using $I_{jnew} = PRNG(I_j \oplus K_i)$. The backend server queries the database and returns $\phi = h(ID \| R_t)$.

Figure 6. Tag response

In order to authenticate the reader identity, user input reader's identifier used in simulation as shown in Figure 7.

After obtained reader's identifier, user click button "Reader authentication", and the results of $\beta = h(RID \| R_r)$ is shown.

Figure 7. Reader authentication

The backend server should also authenticate whether the tag is legitimate. When the button "Tag authentication" is clicked, the system returns the result of tag authentication as shown in Figure 8. To this stage, one round authentication is completed. Because the protocol proposed is a dynamic authentication process, the tag's ID and Key are changed after one round authentication. If previous tag's ID input, it will obtain a negative authentication results.

Figure 8. Tag authentication

Through a large number of testing, the experimental results indicate that the solution proposed can correctly distinguish legitimate and illegal tags, and it can prevent attacks mentioned above. The solution can be implemented in the hardware environment, which provides a reliable approach for RFID system application in practical.

VI. Conclusions

This paper introduces a dynamic RFID security protocol based on hash function in RFID sensor networks. A new scheme has been proposed to solve the shortcomings existing protocols. The protocol proposed can effectively solve various security and privacy problems faced in readers and tags in RFID sensor network. Finally, through establishment of the idealized model of the protocol, the BAN logic is used to prove correctness of the protocol. The security has been proved in theory. The experimental results show that the solution proposed can correctly distinguish legitimate and illegal tags, and it can prevent various attacks within RFID system.

References

[1] Z. Fu, X. Sun, Q. Liu, L. Zhou, J. Shu, "Achieving efficient cloud search services: Multi-keyword ranked search over encrypted cloud data supporting parallel computing", IEICE Transactions on Communications, vol.E98, no.B(1), pp.190-200, 2015.

[2] Y. Liu, S.Feng, "Scalable Lightweight Authentication Protocol with Privacy Preservation", Tenth International Conference on Computational Intelligence and Security, IEEE Computer Society, 2014, pp. 474-478.

[3] 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 Cryptogra-phy and Information Security, Berlin: Springer-Verlag, 2004, pp.719-724.

[4] Z. Li, X. Zhong, X. Chen, J. Liu, "A Lightweight Hash-Based Mutual Authentication Protocol for RFID", International Workshop on Management of Information, Processes and Cooperation. Springer, Singapore, 2016, pp.87-98.

[5] S. Lee, Y. Hwang, D. Lee, J. Lim, "Efficient Authentication for Low-Cost RFID Systems", Computational Science and Its Applications – ICCSA 2005. Springer Berlin Heidelberg, 2005, pp. 619-627.

[6] S. Huang, S. Shieh, "Authentication and secret search mechanisms for RFID-aware wireless sensor networks", International Journal of Security and Networks, vol.5, no.1, pp.15–25, 2010.

[7] C. Mtita, M. Laurent, J. Delort, "Efficient serverless radio-frequency identification mutual authentication and secure tag search protocols with untrusted readers", IET Information Security, vol.10, no.5, pp. 262–271, 2016.

[8] S. Zhou, Z. Zhang, Z. Luo, E.Wong, "A Lightweight Anti-Desynchronization RFID Authentication Protocol", Information Systems Frontiers, vol.12, no.5, pp. 521-528, 2010.

[9] Y. Zheng, M. Li, "Fast tag searching protocol for large-scale rfid systems", IEEE/ACM Transactions on Networking, vol.21, no.3, pp. 924–934, 2013.

[10] M. Chen, W. Luo, Z. Mo, S. Chen, Y. Fang, "An efficient tag search protocol in largescale rfid systems with noisy channel", IEEE/ACM Transactions on Networking, vol.24, no.2, pp. 703–716, 2016.

[11] M. Shahzad, A. Liu, "Fast and accurate estimation of rfid tags", IEEE/ACM Transactions on Networking, vol.23, no.1, pp. 241–254, 2015.

[12] W. Gong, J. Liu, Z. Yang, "Fast and reliable unknown tag detection in large-scale rfid systems", in MobiHoc, 2016, pp. 141–150.

[13] J. Cho, Y. Jeong, O. Sang, "Consideration on the brute-force attack cost and retrieval cost: A hash-based radio-frequency identification (RFID) tag mutual authentication protocol", Computers & Mathematics with Applications, vol.69, no.1, pp. 58-65, 2015.

[14] A. Alqarni, M. Alabdulhafith, S. Sampalli, "A Proposed RFID Authentication Protocol based on Two Stages of Authentication", Procedia Computer Science, vol.37, pp. 503-510, 2014.

[15] C. Zhang, W. Zhang, H. Mu, "A Mutual Authentication Security RFID Protocol Based on Time Stamp", First International Conference on Computational Intelligence Theory, Systems and Applications, 2016, pp. 166-170.

[16] B. Wang, J. Zhang, X. Sun, N. Wang, Y. Zhao, F. Wang, "Research on authentication technology of agriculture products traceability system based on RFID", Guangdong Agricultural Sciences, vol.41, no.14, pp.172-179, 2015.

[17] D. Henrici, "Hash-based enhancement of location privacy for radio-frequency identification devices using varying identifiers", IEEE Conference on Pervasive Computing and Communications Workshops, IEEE Computer Society, 2014, pp.149.

[18] M.Uddin, S.Mekhilef, M.Rivera, "Experimen-tal validation of minimum cost function -based model pre-dictive converter control with efficient reference tracking", IET Power Electronics, vol.8, no.2, pp. 278-287, 2015.

Baolong Liu he is an associate professor, School of Computing Science & Engineering, Xi'an Technological University. His research interest is information processing.

Bing Yang she is a Master degree candidate, School of Computing Science & Engineering, Xi'an Technological University. His research interest is the security of RFID system.