Research of an Improved RFID Authentication Protocol

W.J. Yu
College of Automation
Hangzhou DianZi University
Zhejiang Hangzhou, China

Y.W. Zhang, Z.Y. Tu
Advanced manufacturing Institute Zhejiang Sci-Tech University Zhejiang
Hangzhou, China

***Abstract*--As a new automatic diagnosis technology, RFID is gradually widely used. But the characteristics of the RFID system and the limitations of RFID equipment have brought many security problems. For these problems, this paper discusses and explains system composition and security problems of RFID, analyzes features and deficiency of the existing typical RFID security protocols, and then puts forward a RFID security protocol based on key matrix. This protocol uses the key matrix to encrypt the data transferred between Reader and Tag, and after authentication it can renew the secret value of Tag to resist various attacks. Linux test has proved that this protocol has the features of high efficiency, low cost and high security.**

Keywords-RFID; key matrix; security protocol; access control

I INTRODUCTION

The access control system is an important tool in security measures. In recent years, the emergence of new technologies has transformed from traditional access control system to intelligent access control system. RFID(Radio Frequency Identification) Access control systems, an intelligent access control system, has extensively used in schools , residential areas , business units , research institutes and other institutions of security and attendance management.

As shown in Fig.1, the RFID access control system is mainly composed by three major components: the electronic tags (Tag), RFID reader (Reader), and back-end database (Backend Database). Transmission data between the RFID Reader and Tag is used by the radio channel. A channel from RFID Reader to Tag is called the forward channel, while a channel from Tag to Reader is called reverse channel. Information is exposed in the process of transferring information in the wireless channel. So transmitting information by the wireless channel between Tag and Reader is very dangerous. In view of the different parts of the system, the RFID system's security threats are from a variety of means of attack. The methods of attack the system mainly include [1]: On the air Attacks, Manipulating Data on the Tag, Manipulating Middleware Data, Attack the Data at the Backend, etc.

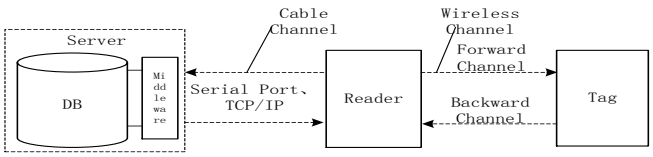

FIGURE I. BASIC COMPONENTS OF RFID ACCESS CONTROL SYSTEM.

Because of the disadvantage of wireless channel transmission of information, many security attacks on RFID systems are the process of information transmission in the front wireless channel. At present, many software security based on cryptography is also based on this communication process. Therefore, it has very high research value for the safety of this procedure [3].

II ANALYSIS ON THE SECURITY STRATEGY AND COST REQUIREMENTS OF RFID ACCESS CONTROL SYSTEM

For RFID, privacy protection and cost are regarded as two inter-constraint measures. Now there are two solutions of the security attacks to RFID system: physical security mechanism and software security mechanism based on encryption technology. As implementing physical security mechanism is troublesome and of high cost, software security mechanism based on encryption technology is becoming a hot research area. And many software security mechanism based on encryption technology has been created. These security protocols mainly include Hash - Lock protocol, random Hash - Lock protocol, Hash chain, distributed RFID asked - response authentication protocols, etc.

However, Hash - Lock protocol and random Hash-Lock protocol have the quality of less computation and lower-cost tags. However, the others need so large amount of calculation and the high cost of tags, that they also have greater security. So, How to balance the security requirements and low cost is a problem that we must consider when we are going to design a kind of RFID authentication protocol.

III THE EXISTING RFID SECURITY PROTOCOLS

Recently, Hash-Lock protocol came up by Weis et al has been widely recognized by the industry, which uses a random number inquiry - answer mode [2].

The protocol to solve the problem of information about the use of Tag response signal source tracking, but this protocol has two major weaknesses: ID is transmitted in plaintext, so attackers can easily intercept the transmission ID. In addition, we sent the data returned to the back-end databases for calculation matches without checking it, so the protocol also can't resist the retransmission attack.

Aiming at this problem, we have written an article named < Study of Random Hash-Lock Protocol for RFID Access Control System >. But in practice we have found some

shortcomings that database will send the identifications of Tag to Reader so that Tag will calculate each of identifications which increase Tag's cost in each authentication. But for large applications, this is obviously inefficient. So we propose a kind of RFID security authentication protocol based on key matrix.

IV AN IMPROVED RFID AUTHENTICATION PROTOCOL

A. The Improved Protocol Process

The authentication process is shown in Fig.2 of the protocol.

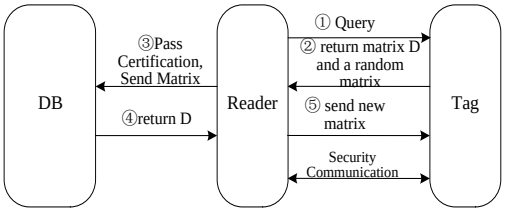

FIGURE II. AN IMPROVED KEY MATRIX PROTOCOL.

We call random invertible matrix KT generated by Tag，and call random invertible matrix KR generated by Reader. In each process, authentication process of the protocol can be listed as follows:

1. Tag receives the Query authenticated requests and Random invertible matrix KR from Reader, and records the matrix.

2. Tag saves the ID as matrix and calculates D = K-1TSID, and then sends this D and KR to Reader. The role of KR is mainly for the convenience of Reader checking.

3. Reader compares KR with its own storage. If they are not equal, Authentication will fail. If equal, Reader will send D = K-1TSID to the background database. The background database uses D stored in itself to multiply by KT coming from Reader, and then finds the existence of ID' which is equal to ID. If there is such an ID, we can get the corresponding matrix key values S, and DB will send S to Reader, or Authentication will fail.

4. If the background database passes the authentication, it will return the key SID to Reader. Reader uses it and KR stored in itself to multiply by D' = KR SID, and sends D' to Tag.

5. After receiving D', Tag will use it and K-1R stored in itself to multiply by S'ID. If S'ID is equal to SID, Reader passes the identity authentication. The process of this authentication process ends. Reader still sends the Query authenticated request and Random invertible matrix to prepare the next authentication.

B. Characteristics of the Improved Protocol

Improvement of RFID security protocol is proposed in this paper has three important characteristics: Firstly, compared with the random Hash-Lock protocol, the data that this protocol send to Tag in the certification replaces the original ID plaintext transmission, which obviously improves the security of transmission process. Secondly, Tag can retrieve the corresponding key by verifying from the back-end database. What's more, different Tags own different keys, which will prevent the drawback that if one card is cracked causing that all cards will not be able to use. These two characteristics above can achieve by many ways. In other paper, we once have come up with an idea that we can use Hash function to solve this problem. But there is still some deficiency. Why we choose a matrix based way? The main concern is the problem of the protocol cost. In this protocol, Tag only needs simple matrix operations and only needs few gate circuits, which greatly reduces the cost of Tag. In low-cost tag, only 200~3000 logic gates can be used in security-related tasks. Hash algorithm, AES algorithm and ECC algorithm need the number of the gate circuits is much more than that of Tag can support. The matrix algorithm of the protocol is equivalent to Exclusive OR, Modular 2 arithmetic, or pseudo Random Number Generation. But this algorithm only needs no more than 1000 gate circuits.

TABLE I. COMPARISON OF VARIOUS ALGORITHMS' COMPLEXITY.

Algorithm	Equivalent Gate circuits	Algorithm	Equivalent Gate circuits
SHA-1	8120	MD5	8001
the method in this paper	several hundred	AES-128	3400
SHA-256	10868	ECC-192	23600

Therefore, no matter from the view of security or cost, this protocol is much better than Hash-Lock protocol and random Hash-Lock protocol.

C. The Protocol's Computation Analysis

Compared with the Hash-Lock protocol and the random Hash-Lock protocol, the protocol conversation between Reader and Tag calls for 3 times in the authentication process, that the number of conversation is not increased. What's more, we use key matrix to take place of Hash function, so that the amount of calculation has descended. Conversation between Reader and Tag calls for 2 times, that the amount of calculation and the conversation hasn't increased. Tag's amount of storage is Tag's ID, the key S and random invertible matrix, which have little amount of storage compared to other protocols. As with the random Hash-Lock protocol, this protocol needs to calculate all Tag's matrix. But it will not produce a large amount of calculation.

In a RFID access control system, Reader can share a part of the calculation pressure for the back-end database, so the calculation of authentication process can be transferred to Reader. Different access control system should update data setting different time as far as possible, which can avoid the problem that several access control systems require updating data at the same time, so that it brings the server to its knees.

In such a system, different access control systems authenticating information need different time. For example, there are two systems – a residential community access control system and a unit building access control system. The residential access control system stores the information of the entire district staff, which will led to have a large number of certification calculation, so that it needs a long time to do it. While personnel information stored in the unit building access

control system is less, and the time of certification is shorter. It also makes different cards to have different access permissions. One card is only for certain legal access control system. People who come from the different units of the same cell (different departments of the same company) can only access their own permissions areas.

D. The Simulation of Read Protocol

The system of Reader uses Linux platform. According to the algorithms above, part of the code simulating the protocol is listed as follows:

```
① Reader creates random number
void CreatRandom()
{
struct timeval tpstart;
gettimeofday(&tpstart,NULL);
srand(tpstart.tv_usec);
int **arr1, **arr2;
for(i = 0; i < ARow; i++)
{  //produce random number 1~1000 as an example
   arr1[i] = 1+(int) (1000.0*rand()/(RAND_MAX+1.0)); }
}
// allocate the memory space of one dimensional matrix
arr2 = (int *)malloc(sizeof(int) * ARow * ACol);
for(row = 0; row < ARow; row ++)      // convert to a one dimensional matrix based on row
{
for(column = 0; column < ACol; column ++)
{
loc = column + row*ACol;
  arr2[loc] = arr1[row][ column ];
}
}
SentRan();            // send random number
}
② Reader or backend server gets all IDs, and Check matrix values
void Check_ID_Matrix ()
{
int** list[MAX] = {\0};
list = GetAllIDs();                    // get all IDs from the database
int** random = GetRandom();            // get the random number from Tag
int** hashcode = GetEncryptionCode();  // get the encrypted matrix from Tag
for(int i = 0; i < MAX; i++)
{
if(MatrixEqual(EncryptionCode(list[i]), hashcode))
{
int** k = GetKey(ls);          // get the corresponding key
Key=key;                       // Key is a global variable
return;
}
}
}
```

Setting the byte length of the random number, we should note: if the length is too long , the stored random number will occupy too many resources of card hardware, while shorter, the probability of two adjacent generating the same random number is becoming larger, which may lead to judge wrongly as replay attacks and return an authentication failure . The calculation of the check random matrix value can be placed on the server-side, and also can be placed on Reader side. The laster will help to reduce the server's calculation pressure.

VSUMMARY

This paper introduces the security risks RFID will face when it is applied in access control system, and analyzes their advantages and disadvantages. In view of the design defect of the random Hash-Lock protocol, this paper comes up with a protocol of security authentication based on key matrix, analyzes the security of this protocol and calculation, and proves that this protocol can effectively resist common RFID access control system attacks. Under the condition of larger amount of data, reducing the pressure of the server calculation is an important aspect of building distributed access control system.

REFERENCES

[1] GONG L, NEEDHAM R, YAHALOM R. Reasoning about belief in cryptographic protocol. Proceedings of the 1990 IEEE Symposium on Research in Security and Privacy, California, 1990:234-248.

[2] Weis S A, Sarma S E, Rivest R L, et al. Security and Privacy Aspects of Low-cost Radio Frequency Identification Systems. Proc. of the 1st International Conference on Security in Pervasive Computing. Berlin, Germany: Springer-Verlag, 2004: 201-212.

[3] Boneh D, Franklin M. Identity-based encryption from the Weil pairing. In; Advances in Cryptology, CRYPTO 2001, Lecture Notes in Computer Science. 2001, 2139: 213-229.