The Research on Mutual authentication Protocol for RFID System Based on Combined Symmetric Key

Jiya Jiang [1] Tong Liu [2] Yanqing Shi[1] Jianwei Guo[1]

[1] Beijing Science and Technology Information Institute, Beijing, China 100044
[2]Beijing Academy of Science and Technology, Beijing, China 100089

Abstract

This paper analyzed the security problem existed in the low cost RFID system, and proposed a new security authentication protocol for RFID system by use the Combined Symmetric Key and SMS4 algorithm, then the management of large-scale keys can be simplified to the management of small-scale key seeds. It effectively resolves the security problem and reduces the requirement of tags as well.

Keywords: RFID Mutual authentication Combined Symmetric Key

1. Introduction

The Internet of Things refers to the various sensing devices, such as radio frequency identification devices, infrared sensors, global positioning systems, laser scanners, and other short-range wireless self-organizing network based on the barter communication mode, through a variety of access network and the Internet combine to form a huge intelligence network[1] . The aim is to get all the items connected to the network, in order to realize inter-connection of people and objects, as well as between objects, so that the system can realize the object identification, location tracking, monitoring and trigger corresponding events. Internet of things is called the third wave of the world information industry [2][3] following the computer, the Internet. Currently, the United States, European Union, Japan and South Korea and so on invested heavily in depth study and exploration of Things, China also attaches great importance to the study of the Internet of Things.

RFID technology is one of the key technologies of the Internet of Things in recent years, RFID technology is highly development at home and abroad, and has been widely used in various fields. However, because based on the openness of the wireless communication between the tag and reader, so that the data between the tag and reader are susceptible to interception, thus unauthorized access to the system, tracking, eavesdropping, forgery, physical attacks and other security issues exist . For RFID security issues, domestic and foreign researchers launched a series of interactive authentication protocol studies [4-8].

2. The research of RFID system security mechanisms

RFID system includes three parts: the tags, readers and data processing system [9]. The electronic tag can be attached to the object. The tag and reader communicate through the wireless signal each other, the reader transmits specific frequency signal to the electronic tag, the tags obtain the energy by the induced current and

send the stored data in the chip to the reader, and the reader receives the data and transmits to the upper application.

The communication between the reader and the tag is by the unprotected wireless channel, so the security issues very serious.

RSA or other asymmetric algorithms due to the computational complexity of the device computing power, and cannot be applied to the low-cost RFID systems. Then the design of the authentication protocols for the RFID faces great challenges, especially the scale key management problem is difficult to obtain an effective solution.

This paper presents a protocol which uses the symmetric cryptographic algorithms such as SMS4 and Combined Symmetric Key to realize the RFID mutual authentication. In the key manage system, key "seed" technology is used to achieve symmetric key update free maintenance, and reduce the maintenance costs of the certification center, so as to resolve the key update problem of high maintenance costs.

3. Combined Symmetric Key

Combined Symmetric Key (CSK) [10-11] is proposed by Beijing Key Laboratory of Network Cryptography Authentication where I and my colleagues work for.

The core idea of CSK is: given a small size of key seeds subset, the large-scale key subset can be generated from small-scale key seeds selected by a random number sequence and mapping function.

Thus, the management of large-scale Symmetric key has been simplified to the management of small-scale key seeds.

The CSK-based algorithms need the following points:

Firstly, every user's key seeds matrix is different to others.

Secondly, give the same key seeds matrix and different random number, the different key can be generated.

Thirdly, give different key seeds and the same random number, and then the different key can be generated.

Fourthly, the key seeds matrixes are limited, but the amount of the encryption keys can be unlimited generated by some function.

Lastly, all the key seeds matrixes of the users are stored in the server.

In this paper, we get the encryption keys from the encryption keys seeds through the function F .

We denote the key seeds matrix for one user as:

$$K_{148\times16}(M,N)=\begin{bmatrix} A_{10\times16.} \\ B_{12\times16} \\ C_{31\times16} \\ D_{24\times16} \\ E_{60\times16} \\ Z_{11\times16)} \end{bmatrix} \tag{1}$$

When authentication, a temporary key seeds can be got by the time stamp as the following:

$$K'_{16\times16}=\begin{bmatrix} A'_{year,m} \\ B'_{month,m} \\ C'_{day,m} \\ D'_{hour,m} \\ E'_{\min ute,m} \\ Z_{11\times16} \end{bmatrix} \tag{2}$$

Then, we can get the one-time key by the following function with a random number.

$$key = Em(\text{Key Seed} \parallel \text{R}_\text{i}) \tag{3}$$

4. Mutual Authentication Protocol in RFID System

Each electronic tag and reader has a unique device number identification information and key seeds matrix. In the Certification Center, the server stores the

cipher text of key seeds Matrixes and identification information of all equipments.

This pre- distribution scheme does not require pre-establish a secure channel between the authentication server and the terminal. It can safely achieve mutual authentication between the authentication server and terminal as follows:

(1) The reader (device identification RID) puts forward a certification request, and then the electronic tag (device identification TID) generates a random number Nt and timestamp Tt. Based on CSK protocol and Symmetric algorithm such as SMS4, the authentication code SLT1 is generated from the key seeds matrix. And then send the code to the reader. The reader will send the RID, TID, SLT1, Nt and Tt to the authentication server.

(2) According to the TID, RID, the Server can get the respective key seeds matrixes KeyT for tag and KeyR for reader. And then calculates authentication code SLT2 by Nt, Tt KeyT, and then compares with SLT1. If the same, the server can confirm the electronic tag is Lawful. Then the server generates server timestamp Tb and a random number Nb, and calculates server-side authentication code SLR1 according to KeyR got from the reader's key seeds matrix. At last, SLR1 will be sent to the reader with Tb, Nb.

(3) The reader calculates SLR2 with Tb, Nb, and the key matrix, compares with SLR1, if the same, the reader completes the authentication to the server and electronic tags. Then it generates authentication code SLR3 with a new random number Na, parameters Tb, key seeds matrix, and then sends the SLR3 and Na to the server.

(4) The server confirms if the replay attack exist. If not, calculates SLR4 by Tb, Na and key seeds matrix. Compared with the SLR3, if exactly the same, the server completes the certification to the reader, otherwise interrupt certification. The server then calculates the authentication code SLT3 by KeyT, Tb, Na, and sends to the reader.

(5) The reader gets SLT3, Na, Tb, and sends to the electronic tags. The electronic tags calculate the authentication code SLT4, compare with SLT3, if the same, then electronic tags complete the authentication to the server and reader. Now, the electronic tag, the reader and the server complete mutual authentication each other.

5. Summary and Outlook

In this paper, the encryption algorithm used SMS4 algorithm, which is a block cipher algorithm published for the first time in China in 2006. And the problem of key management can be solved by Combined Symmetric Key technology. Based on this technology, the management of large-scale keys can be simplified to the management of small-scale key seeds. It effectively resolves the security problem and reduces the requirement of tags as well, thus this technology can be applied to low-cost mutual authentication RFID system.

6. Acknowledgements

This work was financially supported by the program of Large-scale Network Authentication Center affiliated to Beijing Municipal Institute of Science and Technology Information (No. PXM2012_178214_000005), the program of Innovation Group for Internet Real-name System (No. IG 201003C2) and the program of Beijing Talent Training Plan (No. 2012D 0020 2200 0002). Thanks for them very much.

In addition, I want to thank all our colleagues, both past and present, for their assistance during the progression of this research.

7. References

[1] LIU Qiang CUI Li CHEN Haiming. Key Technologies and Applications of Internet of Things [J]. Computer Science, 2010, Vol.37 No.6.

[2] SHEN Su-bin; FAN Qu-li; ZONG Ping; MAO Yan-qin; HUANG Wei. Study on the Architecture and Associated Technologies for Internet of Things [J]. Journal of Nanjing University of Posts and Telecommunications(Natural Science), 2009, 29(6) : 1-13.

[3] SARMA A, GIRAO J. Identities in the future Internet of things [J].Wireless Peers Communication, 2009, 49(3) : 353-363. .

[4] Lim C H, Kwon T. Strong and robust RFID authentication enabling perfect ownership transfer. Proceedings of the 8th international Conference on Information and communications security. Raleigh, NC,USA,2006:1-20.

[5] Le T V, Burmester M, de Medeiros B. Universally composable and forward-secure RFID authentication and authenticated key exchange. Proceedings of the 2007 ACM Symposium on Information, Computer and Communications Security. Singapore,2007:242-252.

[6] Ouafi K, Phan R C W. Traceable privacy of recent provably secure RFID Protocols. Proceedings of the 6th International Conference on Applied Cryptography and network Security. New York, NY, USA,2008:479-489.

[7] Phan R C W, Wu J, Ouafi K,Stinson D R. Privacy analysis of forward and backward untraceable RFID authentication schemes. Wireless Personal Communications, Springer, Netherlands, 2010:1-13.

[8] Song B, Mitchell C J. Scalable RFID security protocols supporting tag ownership transfer. Computer Communications, 2011, 34(4):556-566.

[9] ZHANG Zhong XU Qiu-Liang. Universal Composable Grouping-Proof Protocol for RFID Tags in the Internet of Things [J]. Chinese Journal of Computers,2011,Vol 34 No.7.

[10] Liu Tong, Jiang Jiya. Research on Large-scale Authentication Architecture and Key Management Protocol Based on Combine Symmetric Key. International Symposium on Computer Network and Multimedia Technology. Wuhan. 2009. 368-371.

[11] Jiya Jiang , Tong Liu.A Two-way Authentication Based on One-time SMS4 Algorithm and Combined Symmetric Key. International Conference on Computer Science and Software Engineering, Wuhan, 2008. 1024-1027.