Research on Security Protocol of RFID System Based on Public Key Cryptography

Song Wang¹, Bo Zhang²,*
School of Computer Science, Wuhan Donghu University, Wuhan 430212, China
*Corresponding author's e-mail: bob.cheung@ovspark.com

Abstract. As one of the key technologies of the Internet of Things, RFID technology has increasingly become a part of people's daily life. Because of the openness of the RFID system, its security problem becomes more and more serious. This paper improves the public key encryption authentication protocol and proposes a new protocol scheme. This scheme can provide better security authentication for the RFID system by using random number and session key, and it can satisfy the requirements of the RFID system in performance.

1. Introduction

With the continuous development of Internet of Things technology, as one of the critical technologies of Internet of Things, RFID (Radio Frequency Identification) technology has gradually become a part of people's daily life. As a non-contact automatic identification technology, RFID can automatically identify target objects and acquire relevant data information through radio frequency signals. Compared with other information identification technologies, RFID technology has greater advantages such as fast scanning, multiple-tag recognition and large data storage capacity. At present, RFID technology has been applied in various fields such as logistics, retail, manufacturing, medical treatment, identity recognition, intelligent transportation, food, anti-counterfeiting, animal identification, library, automobile, aviation and military, etc. However, with the various applications of RFID system, the computing power of commonly used RFID system is limited, and there is no effective protection measure. Therefore, the security problems of RFID becomes increasingly serious, especially the privacy of users. Because the RFID tag can directly respond to the reader's query without the permission of its owner, it will be read away by the nearby reader without the user's perception that the user's data will be illegally embezzled or the personal sensitive information will be leaked.

The methods which are used to implement the security mechanism of RFID system can be divided into three types: physical security mechanism, cryptography and tag authentication mechanism. The computing and storage resources of RFID tags are very limited, so the security protocols in general computer networks can not be simply used. In the research of security strategy based on cryptography, the design of RFID security protocol based on Hash function is mostly adopted, but this design can not resist replay and counterfeit attacks. What’s more, there are potential security risks of database synchronization. Recently a lot of work in the field of RFID security has been devoted to the design and analysis of lightweight authentication protocols which aim at the efficient realization of unilateral or bilateral authentication between tags and card readers with minimal computing power. Therefore, the purpose of this paper is to design a low-cost public key cryptosystem protocol with confidentiality and authentication.
2. Analysis of Security Authentication of RFID System

The prospect of RFID technology is vast, but due to the cost, security risks and other reasons, the application of RFID is still restrictive. Therefore, a number of security problems must be carefully analyzed which are encountered in the application of RFID. They should be classified scientifically and studied deeply. The existing security mechanisms and solutions would be analyzed in details and then the advantages, disadvantages and existing problems of each scheme in accordance with the security requirements of the RFID system could be accurately evaluated.

In the RFID system, tags have extremely strict cost constraints. The hardware resources, computing power and storage space are restrictive. Therefore, symmetric cryptosystem algorithm is widely used for information encryption in the RFID system. Symmetric cryptosystem will share a key between the reader and the electronic tag in applications. When the key of an electronic tag is leaked, it will affect the whole RFID system [1]. Compared with symmetric cryptosystems, public key cryptosystems use paired keys to complete encryption and decryption operations respectively. The key management mechanism is flexible and does not need to transfer keys in the transmission channel, which greatly reduces the possibility of key theft. Gaubatz and other researchers have compared Rabin encryption algorithm, elliptic curve encryption algorithm and Ntru encryption algorithm, and they have proposed that these public key cryptographic algorithms can be applied in wireless sensor networks with low power consumption [2]. Batina et al. have discussed the feasibility of the identification protocol based on elliptic curve cryptography and proved the feasibility of the protocol on RFID tags [3].

Public key cryptosystem requires high storage space and computing power, thus it is difficult for RFID system to use the existing mature cryptographic mechanism to achieve the communication security between the tag and the reader. Therefore, it is an important way to realize the security of RFID system with low cost to design efficient and concise encryption algorithm and improve the security authentication protocol which can protect users' data and privacy.

The security requirements of RFID authentication system mainly consider the following aspects. The first one is privacy protection: 1) bidirectional authentication between tags and card readers; 2) privacy of data. It means that secret data in tags can only be read by authorized card readers, and unauthorized card readers can not identify a specific tag; 3) authentication should prevent common attacks such as counterfeiting, replay, intermediaries, and also prevent attacks that fails to successfully authenticate a device by bringing it into a specific state. Second one is untraceability: an attacker cannot distinguish a tag from other tags based on protocol messages for tracing. The third one is distinguishability: in a system with a large number of tags, the output of different tags at the same time should be distinguishable for card readers; however, this distinguishability can only be recognized by legitimate card readers and not by attackers. Then it is anonymity: in some applications, the information of label users must be maintain secrecy in communication because the communication between tag and card reader belongs to wireless communication and tag identity information is vulnerable to interception, eavesdropping and other attacks. Thus effective means must be adopted to achieve anonymous authentication. The last one is forward security: an attacker cannot discover the information currently transmitted from the previously obtained information.

RFID systems are usually attacked in the process of wireless data transmission as shown in Figure 1. These attacks are mainly divided into passive attacks and active attacks. Data is firstly converted into cipher-text by the key and encryption algorithm before transmission. Without the attacker's understanding of the key and encryption algorithm used in encryption, the ciphertext transmitted can not be deciphered. The legitimate reader can use the private key and encryption algorithm to convert the obtained cipher-text into the original data. Stream cipher can also be used in the RFID system to encrypt each character separately. Because of the low computational complexity and easy hardware implementation, the current RFID system mainly uses stream cipher. However, with the development of technology, the simple encryption method in RFID system can not meet the system's requirements for authentication and privacy.
The public key cryptography system has solved the problem of key distribution in conventional key cryptosystem and the requirement of digital signature. From the initial research and development of public key cryptography, there are only two types of public key systems that are safe and practical, namely, cryptosystem based on Large Integer Decomposition Problem and cryptosystem based on discrete logarithm problem.

3. Improvement of Security Protocol about RFID System

One of the key problems in the encryption and authentication technology of public key-based RFID system is how to manage and distribute the public keys of each user. Because the resources and processing capacity of RFID tags are very limited, effective key management methods must be designed to satisfy the actual needs. In addition, there are two kinds of entities in the RFID system, one of which is the limited computing power entities such as RFID tags and another of that is the entities with strong computing power such as reader and writer. In the design of certificates for RFID tags, the characteristics of tags need to be considered. The key does not need to be replaced frequently and the cryptographic algorithm supported by RFID can be determined. This kind of certificate structure can be greatly simplified. Certificate can contain version number, serial number, unified identification, public key of RFID tag and other information. The authentication method of the reader's certificate includes any entity including the RFID tag. After receiving the certificate, the tag checks the contents, authorization information and signature to verify the validity of the certificate. This paper improves the public key encryption and authentication system and designs a secure protocol with confidentiality and authentication. The specific steps are as follows:

**Fig.2 Public key cryptography based Authentication protocol**

| Authentication Server(A) | Reader(A) | Tag(B) |
|--------------------------|-----------|--------|
| Send identity ID_{A}     | E_{PK_{A}}[N_{A}||ID_{A}] | Send random number N_{1}, N_{2} |
| One-off random number N_{1} | E_{PK_{A}}[N_{A}] | |
| ID_{A}||ID_{B}[N_{1}||N_{2}] | Send identity and random number |
| AS issue Ticket | E_{PK_{A}}[N_{A}||ID_{B}||PK_{B}||T] | |
| | E_{PK_{A}}[N_{A}||ID_{B}][T] | |
| Send session key | E_{PK_{A}}[E_{PK_{B}}[K_{A}||T][N_{2}]] | |
| Send enciphered message | E_{PK_{A}}[K_{A}][E_{x_{A}}[M]] | |
(1) Reader A encrypts identity ID_A with public key PK_B of tag B and sends one-off random number N_1 as the unique identification of this business to tag B.

(2) Label B encrypts the one-time random number N_1 with the public key PK_A of reader A and the new one-time random number N_2 generated by tag B, which will be sent back to the reader.

(3) Reader A sends its identity information, random number N_1, identity information of tag B and random number N_2 to authentication server AS.

(4) The authentication server sends two messages encrypted by AS key to reader A as the public key certificate to both sides of the communication. In practical applications, random numbers can be saved to AS servers. If we find that random numbers have been used before in subsequent communications, it will be considered as replay attacks. The combination of random number and time-stamp makes it possible to save all random numbers in an extremely short period of time in communication, and the synchronization of time-stamps is not too precise.

(5) Reader A encrypts the selected session keys and time-stamps with its own secret keys encrypted by the public keys of random numbers N_2 and B, and sends them to tag B together with the public key certificate, identity information and random number N_1 of reader A, so that B confirms that the sender is reader A. Since the session key is encrypted by the key of the reader A, no third party including the authentication server can obtain the session key.

(6) Reader A sends information encrypted with one-time session key to label B. In this process, only label B can use its own public key to get the one-time session key, and then use the session key to get the information.

(7) Reader A destroys \{PK_A, SK_A, KS\} and label B destroys \{PK_A, KS\} after communication is completed.

4. Safety Performance Analysis

As an open system, RFID system is vulnerable to be eavesdropped, and suffer replay attacks, counterfeit attacks, location tracking, denial of service attack and other attacks. The main purpose of the security authentication protocol based on public key which is proposed in this paper is to protect the security of data transmission in RFID system. It has the following advantages:

(1) Effective prevention of replay attacks. In the form of random number and time-stamp, the random number is different each time in the communication process, and there is no regularity. If the random number used before is found in the message, it is considered as replay attack.

(2) Two-way authentication. The random number encrypted by public key can effectively authenticate the legitimacy of both sides of communication, which effectively prevents illegal reading and counterfeiting attacks.

(3) Data confidentiality. This protocol adds the way of encrypting information with one-time session key in the authentication protocol and ensure the security of communication data.

(4) Preventing surveillance. After each communication, the two parties involved in the communication will destroy the key of the communication, so the risk of key leakage is minimal.

(5) Forward safety. Because the session keys and random numbers used in each communication are different from those used before, it is difficult for illegal users to obtain the correlation of each data. Therefore, it is impossible to infer the previous output and track the previous session based on the information of the intercepted tag. The forward security of the protocol can be guaranteed.

5. Conclusion

This paper analyses the security protocol of the RFID system, and improves the public key encryption authentication system. It realizes two-way authentication between the reader and the tag, and resists all kinds of attack methods, which meets the security requirements of RFID system.

Acknowledgments

This paper was co-supported by the Foundation for Young Scholars in Wuhan Donghu University under grant 2018dhzk007. Thanks for the support of Wuhan Donghu University. Thank you for
providing the experimental platform in Wuhan Donghu University. We have completed the implementation of the algorithm on this platform and the experimental data is presented.

References:
[1] Kaya S V, Savas E, Levi A, et al. Public key cryptography based privacy preserving multi-context RFID infrastructure [J]. Ad Hoc Networks, 2009, 7(1):136-152.
[2] Gaubatz G, Kaps J P, Ozturk E, et al. State of the Art in Ultra-Low Power Public Key Cryptography for Wireless Sensor Networks[C] Pervasive Computing and Communications Workshops, 2005. PerCom 2005 Workshops. Third IEEE International Conference on. IEEE, 2005.
[3] Batina L, Guajardo J, Kerins T, et al. Public-key cryptography for RFID-tags[C] IEEE International Conference on Pervasive Computing & Communications Workshops. IEEE, 2007.
[4] ZHANG Heng-shan, GUAN Hui-sheng, HAN Hai-qiang. Public key based mutual authentication protocol for RFID system. Computer Engineering and Applications, 2010, 46 (5): 69-72.
[5] ZHANG Yuting, YAN Chenghua. Research on RFID Authentication Technology Based on Two-way Authentication Protocol[J]. Netinfo Security, 2016 (1): 64-69.