TELKOMNIKA Indonesian Journal of Electrical Engineering
Vol.12, No.3, March 2014, pp. 2320 ~ 2326
DOI: http://dx.doi.org/10.11591/telkomnika.v12i3.4517

A Strong RFID Mutual Authentication Protocol Based on a Lightweight Public-key Cryptosystem

Zhicai Shi*[1], Yongxiang Xia[2], Chaogang Yu[3]
[1,2,3]School of Electronic&Electrical Engineering, Shanghai University of Engineering Science, Shanghai 201620, P.R. China
Corresponding author, e-mail: szc1964@163.com[1], x-free@163.com[2], yuchaogang@163.com[3]

Abstract

RFID is a key technology that can be used to create the ubiquitous society. However, this technology may suffer from some serious threats such as privacy disclosure. In order to solve these secure problems we propose a strong mutual authentication protocol based on a lightweight public-key cryptosystem: NTRU. The protocol assures the confidentiality of the RFID system by encrypting the messages communicated between tags and readers and the freshness of the messages by using pseudorandom number generator. Otherwise, the protocol can also prevent replay attack, tracing, and eavesdropping effectively. This authentication protocol uses less computing and memory resources, and it is very suitable to some low-cost RFID systems.

Keywords: *RFID, authentication protocol, privacy, security, NTRU*

1. Introduction

With the quick development of the Internet of things and its wide application Radio Frequency IDentification(RFID) technique gets the broad attention and research. RFID facilitates automatic identification of items using radio-waves. This technology initially introduced in the 1940s and 1950s, has got a drastic increase in the number of applications and implementations in the recent years. Today, RFID systems have been successfully applied to manufacturing, supply chain, agriculture, transportation, healthcare, and other relative fields [1].

However, the wide applications of RFID systems into modern society may very much likely make the security and privacy of consumers exposed to threats and risks. For example, businesses may have malicious competitors to collect unprotected RFID information illegally, use forgery tags to provide some wrong information, or even launch denial of service (DOS) attacks against the RFID systems. On the other hand, as a consumer, it is naturally preferred that the information of his RFID-tagged products should be kept private from outsiders. However, a tag reader at an efficient location can read the content of an un-protected tag, tracing the RFID-tagged product and even identifying the person carrying the tagged product. To protect the private information on the RFID systems, some special measurements have to be taken here to deter the reader from accessing the tags. This function is usually finished by an RFID authentication protocol. An RFID authentication protocol is a cryptographic protocol that allows a reader and a tag to authenticate each other. The current mainstream tags targeted at the majority of consumers are some low-cost tags and can only support simple computations and very limited storage. Due to severe resource constraints the current strong authentication protocols are not suitable to protect this RFID system because they need a lot of computing and memory resource during authenticating. It is very necessary to design a lightweight even ultra lightweight authentication protocol for low-cost RFID systems.

2. Related Works

Authentication is the process of ensuring that the users are the persons whom they claim to be. Therefore, the goal of authentication is only for authorized readers to get the content of the valid tags, the tag authenticates the reader before it is accessed and permits to

Received August 26, 2013; Revised September 30, 2013; Accepted October 22, 2013

be accessed by the reader. Moreover, it is guaranteed that private information would not be leaked in the presence of unauthorized entities.

An RFID authentication protocol is a cryptographic protocol that allows a reader and a tag to authenticate each other, and the protocol is especially suitable for cases where resource-limited RFID tags are involved. And this kind of authentication protocol is also called as the lightweight authentication protocol. For this case, conventional authentication protocols that require symmetric key computations or even public key computations are not applicable directly [2].

According to the special cases for RFID systems, many related research works have been done since the advent of RFID techniques. Stephen et al. [3] proposed a lightweight authentication algorithm which can be embedded in the low cost RFID tags which has a Randomized Access Control. This scheme provides the mutual authentication between readers and tags. A reader contains a list of all tag keys and each tag only stores its own key. During authentication, a reader sends an inquiry message to the tag. Then, the tag will generate a random number R and sends it with the hash value of the tag key to the reader. When the reader receives the tag message it will start to compute the hash value for every key in the list and compare it with the received tag message. Finally, after finding the corresponding key the reader will send a response message with the tag identifier to the tag so the tag will make sure that the reader is a valid one. This scheme is efficient, but it is a heavy weight solution if the key list is long.

P. Peris-Lopez et al. [4] proposed a lightweight mutual authentication protocol based on the idea of Minimalist and index-pseudonyms. Each tag stores a key divided into four parts of 96 bits (K=K1||K2||K3||K4) and these parts are updated after each successful authentication. This protocol consists of four steps, Tag Identification, Mutual Authentication, Pseudonym Index Updating, and Key Updating. However, this protocol is vulnerable to Desynchronization Attack [5].

B. Song and C.J. Mitchell [6] proposed a protocol which consists of three exchanges between readers and tags. Each tag stores a hash value of string μ[t=h(μ)] unique to each tag. Also, each server stores [new(μ,t), old(μ,t), D], where new(μ,t) is the new values of the string μ and corresponding h(μ)=t, and old (μ,t) is the previous stored data, and D is the data of the tag such as price. After a successful authentication both the server and the tag will update their values. However, if the updated message does not reach the tag, then the tag will use its old identifier. This can be utilized easily by hackers. If they are successfully able to prevent the tag updating, tag anonymity will be lost and they can track the tag easily.

Molnar and Wagner [7] proposed a private authentication protocol for library RFID which uses a shared secret and a pseudorandom number function to protect the messages communicated between tags and readers. This scheme cannot provide backward untraceability. Once a tag is compromised, the attacker can trace past communications from this tag [8], because a tag's identifier and secret key are static. They also built a new tree-based protocol to provide scalable private authentication. However, this approach requires that each tag stores many secrets corresponding to the path from the root to the tag, and privacy is weakened when an adversary is able to tamper with one tag [9].

T. Dimitriou [10] proposed an RFID authentication protocol that enforces user's privacy and protects against tag cloning. This protocol uses a challenge-response approach, where a tag uses a hash of its identifier as a response to a reader query, and the backend server sends a message using the updated identifier to the tag after receiving the tag response. Between valid sessions, the tag identifier remains the same, thereby making the scheme vulnerable to tracking. Additionally, the scheme is prone to DoS attacks.

The family of ultra-lightweight protocols, LMAP, M^{2}AP and EMAP [11, 12], are highly efficient due to their usage of only bitwise XOR, OR, AND and addition mod 2^m operations. Some costly operations such as multiplications and hash functions are not required at all, and random number generating operation is only done by the reader. In all these protocols, a dynamic index-pseudonym (IDS) (m-bit length) is used as the index to a table (a row) where all the information about a tag is stored. Each tag is associated with a key, which is divided in four parts each with 96 bits. As the IDS and the key (K) must be updated after each successful authentication, they need 480 bits of rewritable memory (EEPROM) in total. A ROM memory to store the 96-bit static identification number(ID) is also required. Peris-Lopez presented some security analysis and claimed that their protocols are secure against the man-in-the-middle

attack, replay attack and forgery attack. But other researchers pointed the family of ultra-lightweight protocols are not robust and these protocols are weak on countering the “bit manipulation” attack on the messages [11].

In this paper, we propose a strong authentication scheme for RFID systems that can reduce the necessary storage and computation resource in a tag by comparison with the schemes described above, as well as prevent the attacks mentioned above.

3. The RFID System and Its Classification

An RFID system consists of three components: radio frequency(RF) tags, RF readers, and a backend database server [2], as shown in Figure 1. A tag is basically a silicon chip with antenna and a small memory that stores a unique identifier known as EPC (Electronic Product Code). This EPC code acts as a key uniquely to identify a record in a database and some identification information of the tag is stored in this record. A reader is a device capable of sending and receiving data in the form of radio frequency electromagnetic waves. This device is basically used to read the unique EPC from the tag. Backend database server is used to store the information related to the objects being tagged with the help of RFID tags and cooperates with readers to finish some complicated functions.

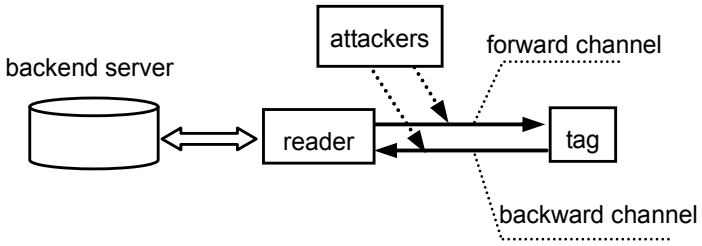

Figure 1. The Components of an RFID System

The basic setup for an RFID System is that the objects are tagged by some tags. These tags store some related data about the objects. They receive and respond to the queries sent by the RFID readers and transmit data stored in them to the readers. These readers transfer the received data to the backend server through wired or wireless networks. The readers could be fixed as well as mobile. The server processes the request and data from the reader and sends the related information about the object which is tagged to the reader.

For an RFID system, a tag is its special device. Its computing and memory resource is very limited. There are two types of tags: active tags and passive tags. Active tags include miniature batteries used to power the tag and they are capable to transmit and obtain data over longer distances. The other one is a passive tag that does not have any battery in it, so it will need to be activated by the signal beamed from the reader. Passive tags are smaller, less expensive and used for a shorter range. Because of their priority this kind of tags are applied widely. Our researches mainly focus on security problems on these low-cost RFID Tags. During researching we also note that since well-designed conventional cryptographic protocols can be effectively implemented on resource-abundant backend servers and readers, it is usually assumed that the channels between backend servers and readers are secure. However, because of the limited resource in tags it has to assume that the channel between tags and readers is insecure. Readers have electric power enough to transmit signals over longer distances and tags only have limited electric energy to transmit signals over shorter distances. So the communication channels between readers and tags are asymmetric. We call the channel from readers to tags as forward channel and the channel from tags to readers as backward channel. These two channels are open and insecure. Most secure problems of RFID systems are resulted from these insecure channels.

4. A Strong RFID Mutual Authentication Protocol

The RFID authentication protocol based on Public-key Cryptography has been proved to have the most strong security and privacy [13, 14]. Among all Public-key Cryptography algorithms, NTRU (Number Theory Research Unit) is a lightweight Cryptography algorithm and it needs less memory and computing resources, runs faster than RSA, Elliptic and other public key encryption systems. Its encryption calculation only needs about 6000 logic gates and it can satisfy the requirement of the low-cost RFID fast authentication [15]. Then we use NTRU to design a strong mutual authentication protocol based on NTRU to solve the secure authentication problems for RFID systems.

4.1. The Strong RFID Mutual Authentication Protocol Based on NTRU

In the following parts, we use NTRU to encrypt and decrypt the messages exchanged between the backend server/reader and the tag so as to assure the privacy and confidentiality of the RFID system. The used notations for the authentication protocol are listed in Table 1.

Table 1. The Related Notations for the RFID Authentication Protocol

Notations	The meaning of each notation
ID	the unique identification of a tag
k_{pu}	the public key of NTRU
k_{pr}	the private key of NTRU
$E()$	the encryption function of NTRU
$D()$	the decryption function of NTRU
R_r	a pseudorandom number generated by a reader
R_t	a pseudorandom number generated by a tag
PRNG( )	a pseudorandom number generator

Supposed a tag is uniquely identified by its ID, $H(ID)$ is the hash value of the tag ID. Under the initial state of the RFID system, the tuple (ID, $H(ID)$, k_{pu}) is stored in each tag, the tuple (ID, $H(ID)$) for each tag, and k_{pr} is stored in the backend server. The tag has two functions. One is the NTRU encryption function $E_{k_{pu}}()$, and another is the pseudorandom number generator PRNG(). The backend server has the NTRU decryption function $D_{k_{pr}}()$, and the reader has the pseudorandom number generator PRNG().

The mutual authentication procedure between the backend server/reader and the tag is depicted in Figure 2, and the authentication protocol is described as follows:

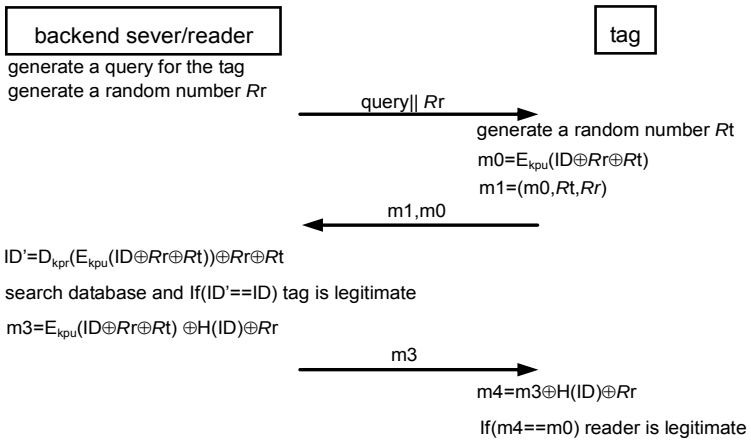

Figure 2. The RFID Authentication Protocol Based on NTRU

Step1: reader→tag

The reader generates a query for the tag and calls PRNG() to get a pseudorandom number R_r, the reader sends query|| R_r to the tag.

Step2: tag→reader

The tag calls PRNG( ) to generate a pseudorandom number R_t, the tag calls the encryption function $E_{k_{pu}}()$ to encrypt $ID \oplus R_t \oplus R_r$ and generates the message m0= $E_{k_{pu}}(ID \oplus R_t \oplus R_r)$. Then the tag forms the message m1=(m0, R_t) and sends m1 to the reader.

Step3: reader→backend server

The reader uses the received message m1 to form the message m2=($E_{k_{pu}}(ID \oplus R_t \oplus R_r)$, R_t, R_r), and sends m2 to the backend server by the secure channel between them.

Step4: backend server→reader

The backend server uses its private key k_{pr} and the decryption function $D_{k_{pr}}()$ to decrypt $E_{k_{pu}}(ID \oplus R_t \oplus R_r)$, and abstract ID by XOR operation with R_t and R_r. The backend server searches its database with ID. If the backend server finds the corresponding item in its database it notifies the reader that the tag is a legitimate one. Then the backend server uses $H(ID)$ to form the message m3= $E_{k_{pu}}(ID \oplus R_t \oplus R_r) \oplus H(ID) \oplus R_r$ and sends m3 to the reader. If the backend server does not find out the corresponding item with ID, and it notifies the reader that the tag is illegal. This step finishes the authentication of the reader to the tag.

Step5: reader→tag

The reader sends m3 to the tag. The tag calculates m3 with $H(ID)$ and R_r by XOR operation and it gets m4= $m3 \oplus H(ID) \oplus R_r$. Then the tag compares m4 with m0. If m4 equals with m0 the tag knows this reader is legitimate, otherwise the tag refuse to be accessed by this reader. This finishes the authentication of the tag to the reader.

4.2. The Analysis of the Strong RFID Mutual Authentication Protocol Based on NTRU

During the authentication procedure described above, the tag finishes one encryption operation and one pseudorandom generating operation, the backend server and reader finish one decryption operation and one pseudorandom generating operation. Otherwise, they need to finish several simple bitwise XOR operations. Now we analyze the security of the proposed authentication protocol.

a) Data confidentiality. During the whole authentication procedure, all messages between the tag and the reader are encrypted by NTRU. Although attackers can get the messages they can not decrypt the messages. So attackers can not understand the real meanings from the messages which they got. The use of NTRU guarantees the proposed authentication protocol has the strong confidentiality.

b) Eavesdropping. During the whole authentication duration, all messages about the tag ID are encrypted and attackers do not know anything about the tag from their acquired data. Eavesdropping to the communication channel between tag and reader is invalid. The privacy of the RFID system is protected.

c) Position detection or tracing. One of the most serious privacy problems for the RFID system is that if a fixed value is exposed during each session, the privacy of the user's position may be encroached upon. To prevent this type of attack, a pseudorandom generator is used to assure each session between tags and readers is fresh so as to make attackers not to know where their received data is sent from. All messages exchanged between readers and tags are encrypted and attackers can not infer any useful information about tags or their owners from these messages.

d) Replay attacks. This type of attack means to re-send data acquired through eavesdropping to compromise the RFID system. When some identical or fixed values are exposed from the tag during the authentication procedure, tracking problems may arise and privacy may be encroached upon. In order to prevent replay attacks the content of each authentication between tags and readers should be different by pseudorandom generating and encrypting. If an attacker re-sends its received message later this message has not any

meanings because each new authentication generates a new pseudorandom number and the corresponding fresh messages.

e) Forward security. Forward security is the property that guarantees the security of the past communications even when a tag is compromised at a later stage. Because for each authentication the reader and the tag generate a pair of new random numbers which there does not exist any relationship with the last authentication. Attackers can not infer the detail information of the last authentication from the current received messages and they cannot guess the tag's or reader's past behaviors.

f) Tag anonymity. The tag performs XOR and encryption calculations to ensure user anonymity. Further, the encrypted ID or its hashing value cannot be used to find which tag it has come from. The tag encrypts its ID and variable random number to make its ID impossible to be exploited.

5. Conclusion

It is generally agreed that the security and privacy of the tag play an important role in determining the cost and performance of an RFID system. To solve this problem we have proposed a low complexity mutual authentication protocol based on NTRU public key encryption system. Different from other public key encryption systems, NTRU is simple and fast. For our proposed authentication protocol the tag only needs one encryption calculations and one pseudorandom generating operation. By analyzing the authentication protocol proposed by us, we has justified that the protocol has the strong data confidentiality and forward security, it can prevent Eavesdropping, Position detection or tracing, Replay attack effectively, and it completes the strong mutual authentication between readers and tags. The protocol only needs less computing and memory resources, and it can be used in low-cost RFID systems.

Acknowledgements

We are grateful for the anonymous reviewers who made constructive comments so that we can improve and refine our paper. The relative work about this paper is supported by National Natural Science Foundation of China (No. 61272097), the Science Research Project(No. 2011XY16) and the Discipline Developing Foundation(No. XKCZ1212) of Shanghai University of Engineering Science.

References

[1] Arun N Nambiar. *RFID Technology: A Review of its Applications*. Proceedings of the World Congress on Engineering and Computer Science. San Francisco, USA. 2009; 2:1-7.
[2] Soo-Young Kang, Deok-Gyu Lee, Im-Yeong Lee. A Study on Secure RFID Mutual Authentication Scheme in Pervasive Computing Environment. *Computer Communications*. 2008; 31(18): 4248-4254.
[3] Stephen A Weis, Sanjay E Sarma, Ronald L Rivest et al. Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems. Lecture *Notes in Computer Science*. 2004; 2802: 201–212.
[4] Pedro Peris-Lopez, Julio Cesar Hernandez-Castro, Juan M Estevez-Tapiador, Arturo Ribagordaet. *EMAP: An Efficient Mutual-Authentication Protocol for Low-Cost RFID Tags*. Lecture Notes in Computer Science. 2006; 4277: 352-361.
[5] T Li, G Wang. *Security Analysis of Two Ultra-Lightweight RFID Authentication Protocols.* Proceedings of the 22nd IFIP SEC 2007. Sandton, Gauteng, South Africa. 2007; 32: 109-120.
[6] B Song, CJ Mitchell. *RFID Authentication Protocol for Low-cost Tags*. Proceedings of the First ACM Conference on Wireless Network Security. Alexandria, USA. 2008: 140-147.
[7] D Molnar, D Wagner. *Privacy and security in library RFID: Issues, Practices, and Architectures*. Proceedings of the International Conference on Computer and Communications Security. Washington, USA. 2004: 210-219.
[8] H Chien, C Chen. Mutual Authentication Protocol for RFID Conforming to EPC Class 1 Generation 2 Standards. *Computer Standards & Interfaces*. 2007; 29(2): 254–259.
[9] RD Pietro, R Molva. *Information Confinement, Privacy, and Security in RFID Systems*. Lecture Notes in Computer Science. 2007; 4734: 187–202.
[10] T Dimitriou. *A lightweight RFID protocol to protect against traceability and cloning attacks.* Proceedings of the International Conference on Security and Privacy for Emerging Areas in Communication Networks. Athens, Greece. 2005: 59–66.

[11] Tieyan Li, Guilin Wang, Robert H Deng. Security Analysis on a Family of Ultra-lightweight RFID Authentication Protocols. *Chinese Journal of Software*. 2008; 3(3): 1-10.
[12] P Peris-Lopez, JC Hernandez-Castro, JM Estevez-Tapiador, A Ribagorda. *M^2AP: A Minimalist Mutual-Authentication Protocol for Low-cost RFID Tags*. Proceedings of the International Conference on Ubiquitous Intelligence and Computing. Wuhan, China. 2006: 912-923.
[13] RI Paise, S Vaudeney. *Mutual authentication in RFID: Security and Privacy*. Proceedings of the 2008 ACM Symposium on Information, Computer and Communications Security. Tokyo, Japan. 2008: 292-299.
[14] SV Kaya, E Sava. Public Key Cryptography Based Privacy Preserving Multi-context RFID Infrastructure. *Ad Hoc Networks.* 2009; 7(1):136-152.
[15] Jian Chen, Chun Zhang. The public key Cryptography for low power RFID. *Chinese Journal of Semiconductor Technology*. 2009; 9:890-894.