International Journal of Grid and Distributed Computing
Vol. 9, No. 11 (2016), pp.199-208
http://dx.doi.org/10.14257/ijgdc.2016.9.11.17

Multi-owner RFID Tag Ownership Transfer Protocol based on the Chinese Remainder Theorem

Yong Gan, YunQian Xu, Lei He and Feng Xue

School of Computer and Communication Engineering, Zhengzhou University of Light Industry, 450002, Zhengzhou, China
ganyong@zzuli.edu.cn , xyq_fighting@sina.com

Abstract

For the security issue of the single tag ownership transfer, this paper proposes a multi-owner RFID Tag ownership transfer protocol based on the Chinese remainder theorem. By using secret sharing scheme, this protocol divides the sharing key into n parts, which then are distributed to n owners. Only when t owners cooperate together, the sharing key will be recovered. Thus, it ensures the tag's security during the authentication and transformation of the ownership. Under the Linux environment, this protocol was achieved through simulationtest and the experiment data about the calculate time of the tag was got. Then with the number of owners increasing gradually, different results were compared. The result shows that in the protocol, when increasing the owners' number, the calculate time of tag is in the acceptable range, which is also apply to the low cost tag.

Keywords*: RFID; ownership transfer; Chinese remainder theorem; secret sharing*

1. Introduction

Radio Frequency Identification [1] is a kind of wireless communication technology, which mainly identifies specific targets and reads and writes the data through the radio signal, without establishing a mechanical or optical contact between recognition system and specific objectives. In recent years, RFID is the technique of identification and data collection that discussed by people most frequently. It is applied to almost every aspect of life such as supply chain management, identification and trace, logistics management, anti-terrorism technology, import and export trade and libraries. In most of these applications RFID tag's ownership should be transferred between different entities during its life cycle, which makes the tag's security and privacy risks become more complex[2].

With the development of information technology, the application of single owner in tag's ownership transfer can't meet the demand of market now. It is a common thing for multiple RFID to share one object's ownership.

For instance, electronic communication has been more and more depended into day's life, and many important files also need stored in electronic equipment. Therefore, the key management has become a very thorny problem. We suppose there is a large bank client system, which contains the important information of each customer. According to the different levels of customers, the system will use different keys to protect them .Meanwhile, these keys are also protected by a master key. Then it will exist the following problems:

Firstly, to get the master key, it needs an administrator present every time;

Secondly, if the master key administrator had an accident, the key will lose, and customers' information will unable to restore, also the losses will be serious.

Thirdly, if this key administrator betrayed the key to someone else, the entire system security and customer information will be in danger. In this situation, the secret sharing

ISSN: 2005-4262 IJGDC

technology should be used, which means more than one person share this master key and that only a certain number of people get together can people open the system. It can solve the problems such as leak and loss in the process of key management and prove the system's security[3-5].

2. Related Work

Scholars at home and abroad have done many researches in the security issue of tag's ownership transfer. Molnar *et al*[6]. designed a pseudonym protocol based on the key tree, which can realize the ownership transfer of tags by two methods. However, it is just a temporary authorization essentially without realizing full ownership transfer. On the contrary, Lim *et al*[7]. Put forwards the two-way authentication protocol which can achieve full ownership transformation.

But this scheme have high requirement for tag's computing power, and it does not illustrate the way to acquire the tag's related information safely for the new owner. Osaka *et al*[8].put forward a new RFID security mechanism based on Hash function and symmetric password. The shortcomings of the protocol are it cannot against denial of service attacks and does not meet the untractability. By using the method of random number generation (PRNG) and cyclic redundancy check (CRC), Duc *et al*[9]. proposed a low complexity security protocol. But it cannot prevent denial of service attracts and detect illegal tag, also cannot provide the forward security function. Thus, the current RFID tag ownership transfer problem has not been solved very well. Tag ownership transfer system still exist many vulnerable spots, which needs further research.

On this basis, this paper will present a kind of scene that many owners share the tag's ownership. It uses the secret sharing scheme to manage the key, and distributes and recovers the shared key based on the Chinese remainder theorem. It solved the problem of authority cheat in the traditional cryptosystem and improved the security in the process of the tag ownership transformation.

3. Scheme Description

This paper uses the secret sharing scheme based on Chinese remainder theorem to realize multi-owners tag ownership transformation. The tag's shared secret key is divided into several sub-keys (secret share) which then are distributed to multiple owners through the security channel. Only when the owners' secret shares achieve a certain number, it can restore the shared secret of tags according to the Chinese remainder theorem. Thereby it improves the security in the process of tag ownership transform.

3.1. Protocol Design

Initialization Phase

In the phase of the RFID system initialization there is a tag T, which contains the unique identifier (TID) and the key k communicating with the original owners. It also has n original owners, which contain the tag's identification (TID) and the share of their own secret key k_i.The background database storage the identification of tags, n original owners' information and key.

The following notations are used throughout the paper:

Tag: Tag

TID: Unique identifier

R_i: The i^{th} owners , $i = 1, 2.....n$

DB：Back-end database

k: Old key

k_i: The sub-key of the original owner R_i ; $i = 1, 2.....n$

k_{new}: New key

Roo_i: random numbers generated by original owner

Rod_i: random numbers generated by back-end database

Rno: random numbers generated by current owner

H(.):One-way hash function

f: encryption functions

$\oplus$:XOR

3.2 Certification Phase

The certification stage of the protocol is in order to complete the mutual authentication between the tag and the three owners. Specific certification process is shown in Figure. 1

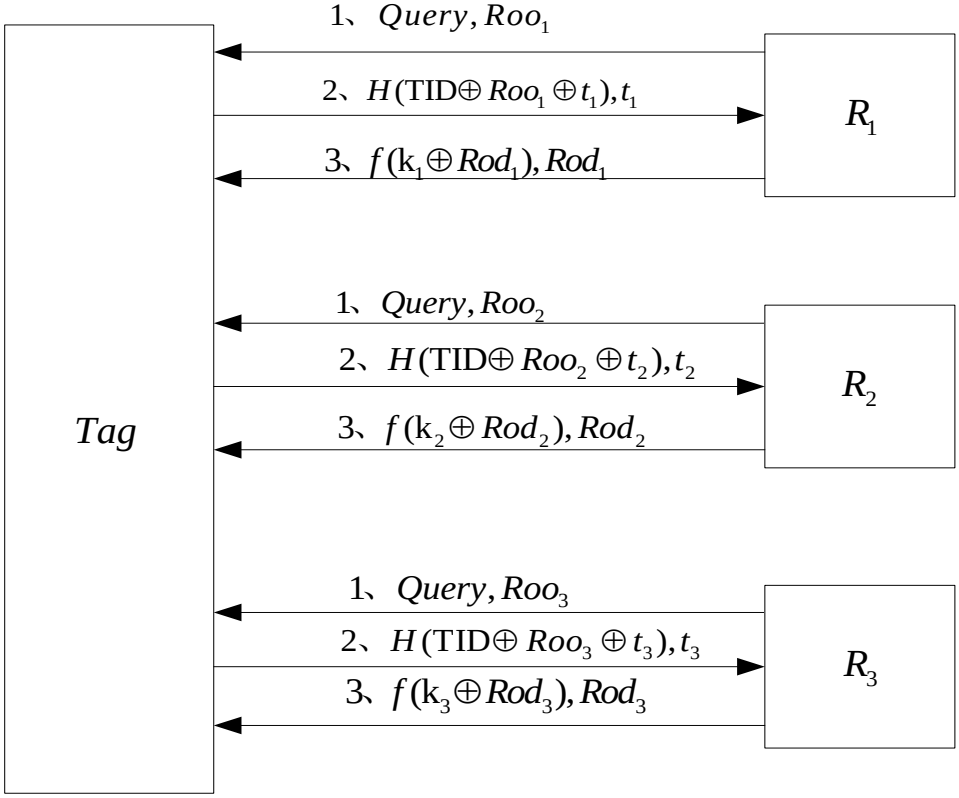

Figure 1. Authentication Phase

Step 1:

Original owner broadcasts query to tag and generate random number Roo_1.

Step 2:

Tag generates a random number t_1 and computes $M_1 = H(TID \oplus Roo_1 \oplus t_1)$ then transmits M_1, t_1 to original owner R_1.

Step 3:

After the original owner R_1 received the message, it use t_1 and Roo_1 to match TID' stored in their backend database. If there exists

$H(TID \oplus Roo_1 \oplus t_1) = H(TID' \oplus Roo_1 \oplus t_1)$ then the tag is authenticated. At the same time the DB generates a random number Rod_1 and forwards $f(k_1 \oplus Rod_1)$, Rod_1 to Tag

Step 4:

Similarly, original owner R_2 R_3 forwards $f(k_2 \oplus Rod_2)$ Rod_2, $f(k_3 \oplus Rod_3)$, Rod_3 to Tag

Step 5:

After receiving the message which original owner R_1, R_2, R_3 ,send, Tag T restores the key k' according to the algorithm of the Chinese remainder theorem. Meanwhile, compared the tag's key k with the key k' restored by using the Chinese remainder theorem, if $k = k'$,the original owner is legal. Then the two-way authentication is completed.

3.3 Ownership Transfer Phase

Ownership transform phase is the key design in this paper. First of all, the current owner should verify the identity of the original owners respectively. After verification, the original owner sends their own sub-key to the current owner respectively through a secure channel. Then, the current owner sends them to the tag, and does the mutual identity authentication with tag. After verification through executing key agreement, they can communicate with each other. The concrete implementation process is shown in Figure. 2.

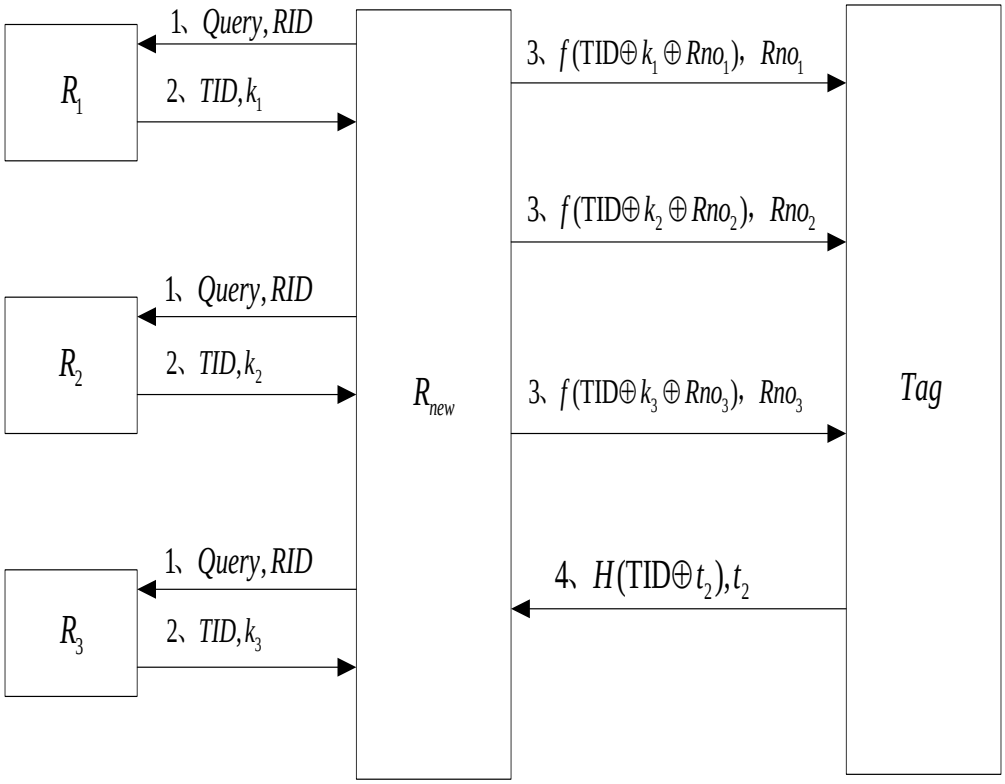

Figure 2. Ownership Transformation Phase

Step 1:

The new owner applies to the original owner of ownership transformation, and at the same time, the new owner sends the identifier (RID) to the original owner. We assume that the channel between the new owner and the original owner is secure. After the

original owner R_1 agreed to the application, it transmits tag's identity TID and the key of the original owner k_1, k_2, k_3 to the current owner via the secure channel.

Step 2:

Now, the current owner, after knowing three sub-keys k_1, k_2, k_3 and generating random number Rno_1, forwards Rno_1 and encrypted function $f(TID \oplus k_1 \oplus Rno_1)$ to the tag .

Step 3:

Similarly, the current owner generates two random numbers Rno_2, Rno_3 and then forwards Rno_2, Rno_3, $f(TID \oplus k_2 \oplus Rno_2)$, $f(TID \oplus k_3 \oplus Rno_3)$ to tag.

Step 4:

As for the sub-keys k_1, k_2, k_3 the tag uses two or more than two of them to restore the keys k' based on the Chinese remainder theorem. If k' is equal to the key k stored in the tag, the current owner is legal.

Step 5:

Tag generates random number t_2, and then sends it and $H(TID \oplus t_2)$ to the current owner. If the current owner exists TID' which can make $H(TID \oplus t_2) = H(TID' \oplus t_2)$ then the new owner is successful in tag certification.

Step 6:

The current owner updates key k_{new} as his new key, and generates random number Rno_4 .After sending this new key by encrypted function to tag,the tag and the current owner can start communication.

3.4 Arithmetic Statement

According to the Chinese remainder theorem algorithm resulting F

Find a constant p, and use the big prime number generator to generate three prime numbers d_1, d_2, d_3 which are mutual prime number with p, and satisfied $d_1 d_2 > p d_3$. Then chose arbitrary number a, satisfied $a < \left[\frac{M}{p} \right]$

So there have $k' = k + ap$

In the rang $[0, k']$ calculate

$$\begin{cases} k_1 = k' \bmod d_1 \\ k_2 = k' \bmod d_2 \\ k_3 = k' \bmod d_3 \end{cases}$$

When k_1, k_2 present, k' satisfied

$$\begin{cases} k' \equiv k_1 \bmod d_1 \\ k' \equiv k_2 \bmod d_2 \end{cases}$$

Solving congruence equations

$$\begin{cases} M = d_1 d_2 \\ M_1 = \dfrac{M}{d_1} \\ M_2 = \dfrac{M}{d_2} \end{cases}$$

Through $y_1 M_1 = 1 \bmod d_1$ find y_1

Similarly work out y_2

Get $k^{'} = k_1 M_1 y_1 + k_2 M_2 y_2$

Through $k = k^{'} - ap$ work out k

4. Security Analysis

In this section, we will give a brief analysis of the security of our protocol.

Untraceability: Every communication between tag and owners will use random numbers to change the tag's response information in each session. The attacker cannot distinguish the response information of each tag, so it is impossible to trace.

Anti-Middle Attack: Because the authentication phase and ownership transformation phase have joined the two-way authentication, the attacker cannot get messages to realize attack by identity in disguise.

Anti-replay Attack: During the process of message delivery, each transmission of the owner will add with random numbers and all of the messages are encrypted by Hash. Every time response messages are different. Thereby, the attacker cannot get the identity information of the tag from the transmission information, nor can he use the information to produce the new authentication information needed when passing the authentication process.

Forward Security: In ownership transformation phase, although the original owner sends his sub- key to the current owner, three sub-keys are not enough to restore the original key k according to the Chinese remainder theorem, which thus ensures the forward security.

Backward Security: After the mutual authentication between the current owner and tag, the current owner will update its key to k_{new} and send the new key to tag later. The current owner and tag will communicate with the new key which the original owner does not know. Consequently, it ensures the backward security.

5. Protocol Simulation

On Linux platform we implemented the proposed agreement first, and then got the consumed time for executing protocol respectively when the numbers of owners who have the tag ownership are three\five and seven. Then we compared the different results shown in Figure.3 (in microseconds).In this experiment2.13 GHz CPU and 2GBs of memory were used. What can be seen from the diagram is in the proposed protocol tag can complete the calculation in a short period of time, which means the low cost tag is suitable.

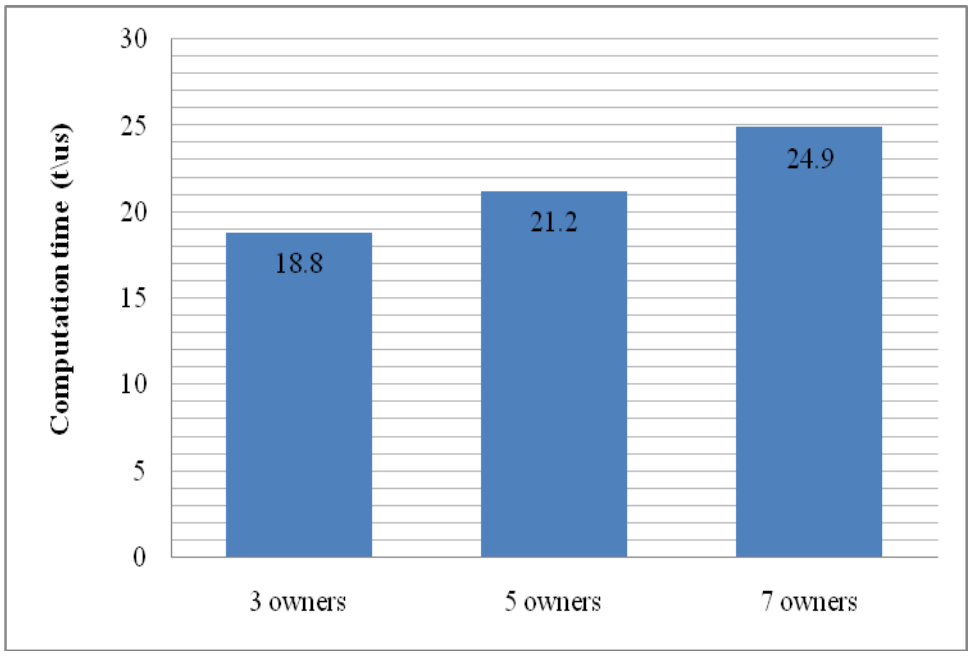

Figure 3. Comparison Chart of the Tag's Computation Time

6. Business Value

RFID has extensive application and has high commercial value, Such as the following areas:

Retail industry: Effective supply chain operations can ensure that when consumers to buy some goods they will arrival in time, beyond that the visibility potential benefits which produced by RFID include: reduce inventory, reduce the labor costs and increase sales.

Manufacturing industry: It can easily improve assembly efficiency, Identify and put an end to fake parts, enhance the accuracy of the production planning, reduce inventories bring down recall costs

Transportation and Logistics: Because of the logistics industry between suppliers and customers, therefore, in this trade RFID tags and basic requirements means in the side of extending services have the huge business opportunities such as Customs clearance faster, prevent counterfeited and so on.

The RFID protocol mentioned in this paper, if applied in business , it can not only make sure the security of trade secret ,but also guarantee the integrity and reliability of business information.

7. Conclusion

This paper proposed a tag ownership transform protocol that support key agreement between tag and multiple owners. The original owner and tag do two-way mutual authentication at first. According to the sub-keys the tag restores the key based on the Chinese remainder theorem and then validates it. Because one single owner cannot communicate with tag, the security of the ownership transformation is improved. The current owner communicates with tag outside the range of original owner and updates the tag's key. It completes ownership transformation and ensures the forward security and backward security of the tag at the same time. This protocol can resist replay attack, middle attack and desynchronization attack. Also the tag is untraceable. The simulation experiment shows that in this protocol the computing time of tag is short, which is

suitable for low cost tag. Meanwhile, how to shorten the time consuming of tag and how to provide verifiability between multi-owners are the questions we need to solve in the next step.

Acknowledgement

This paper is sponsored by National Natural Science Foundation of China No. 61572445 and the key scientific research projects of colleges and universities in Henan province, No. 16A520075.

References

[1] Nath B, Reynolds F, Want R. RFID Technology and Applications. IEEE Pervasive Computing. **(2006)**;5(1):22-4.
[2] Zhang Y G, Fang Y S. A Research on Public Key Cryptographic Algorithms and Its Application Technology [J]. Journal of Hefei University, **(2008)**.
[3] Mamun M S I, Miyaji A. A Scalable and Secure RFID Ownership Transfer Protocol[C]//Advanced Information Networking and Applications (AINA), **(2014)**IEEE 28th International Conference on. IEEE, **(2014)**: 343-350.
[4] Feldman P. A practical scheme for non-interactive verifiable secret sharing[C]//Foundations of Computer Science, 1987. 28th Annual Symposium on. IEEE, **(1987)**: 427-438.
[5] Rabin T, Ben-Or M. Verifiable secret sharing and multiparty protocols with honest majority[C]//Proceedings of the twenty-first annual ACM symposium on Theory of computing. ACM, **(1989)**: 73-85.
[6] Molnar D, Soppera A, Wagner D. A scalable, delegatable pseudonym protocol enabling ownership transfer of RFID tags[C]//Selected Areas in Cryptography. Springer Berlin Heidelberg, **(2006)**: 276-290.
[7] Lim C H, Kwon T. Strong and robust RFID authentication enabling perfect ownership transfer[M]//Information and Communications Security. Springer Berlin Heidelberg, **(2006)**: 1-20.
[8] Osaka K, Takagi T, Yamazaki K, *et al*. An efficient and secure RFID security method with ownership transfer[M]//RFID security. Springer US, **(2008)**: 147-176.
[9] Duc D N, Lee H, Kim K. Enhancing security of EPCglobal Gen-2 RFID against traceability and cloning[J]. Auto-ID Labs Information and Communication University, White Paper, **(2006)**.

Authors

Yong Gan, He received the bachelor's degree in Semiconductor physics and device from Xi'an Jiao Tong University in 1986. He received Ph.D. Degree in computer science and technology from Xi'an Jiao Tong University in 2006. He is currently a Professor of computer science and technology in the department of computer and communication engineering, Zhengzhou University of Light Industry.His research interests include multimedia communications; image

Yunqian Xu, She received her bachelor's degree in Software engineering from Zhengzhou University of Light Industry in 2012. She is currently a Master Degree Candidate of software engineering in the department of computer and communication engineering, Zhengzhou University of Light Industry. Her research interests include Tag ownership transfer; information security;

Lei He, received his Master Degree in Cryptography from Southwest Jiao tong University in 2006. He is now a lecturer in the School of Computer and Communication Engineering, Zhengzhou University of Light Industry. His research interest mainly focuses on wireless network security and cryptography, especially, RFID security. He has published more than 20 research papers in journals and conferences

Feng Xue, He received his M.Sc. in computer science and technology from Zhongyuan University of Technology 2012.He is a postgraduate student in the School of Computer and Communication Engineering, Zhengzhou University of Light Industry. His research direction is information security and big data.