International Journal of Security and Its Applications
Vol. 10, No. 9 (2016), pp.185-192
http://dx.doi.org/10.14257/ijsia.2016.10.9.19

RFID Tag Dynamic Ownership Transfer Protocol based on Lagrange of Multi-owner with Different Weights

GAN Yong, YANG Zong-qin, HE Lei, DU Chao

College of Computer and Communication Engineering, Zhengzhou University of Light Industry, Zhengzhou 450002, Henan, China
997811740@qq.com

Abstract

In practice, the tag may have multiple owners with different weights, and there are some owners who may sell their more or less weights to other owners. Therefore, the weights of all the owners may vary in life cycle of the tag, so the ownership needs to be dynamically updated and the key value needs to be changed in a timely manner. To solve this problem, the paper proposes a dynamic ownership transfer protocol of RFID tag based on Lagrange to implement the transfer of multi-owner with different weights. When there is a change on the weights of the owners, the agreement will recover the original secret key under certain conditions that the sum of the weights on the owners involved in the restoration of the key is equal to or greater than t and verify the legitimacy of the original owners. The new key is divided into n parts by secret sharing scheme, and then the owner gets the corresponding sub secret key according to the weight. Thereby it enhances the security and flexibility in the practical application of the ownership transformation.

Keywords*: RFID; dynamic ownership transfer; Lagrange; shared secret key*

1. Introduction

RFID (Radio Frequency Identification), an automatic identification technology which emerged in the 1990s, obtains specific information about a goal through non-contact radio frequency communications. In recent years, since RFID has many advantages, the technology has been widely used in various fields, such as management of supply chain, retail, transportation and the like. However, because the RFID storage capacity and computing power are very limited, traditional security elements [1-3] cannot be applied directly on the tag so that security and privacy of the RFID cannot be guaranteed. The most important is that most RFID tags need to do the transfer of ownership in its life cycle in practice, which makes security and privacy of a tag become more difficult.

Then, in practical application, the tags may be more than one owner, and owners may occupy different weights. And there may be some owners sell their holding weights to other owners so that the weights of the owners will vary in the life cycle of a tag. For example, a company is controlled by the chairman and some shareholders in real life who may hold different shares due to different identities or functions. Some decisions may be done by the chairman himself at the beginning, he sold some of the shares because of some reasons to make it below a certain value as a result. So when there is a decision to be done, he may need to join the other one or more than one shareholders to determine the decision because the shares of shareholders supported the decision must be more than a certain value. That is to say that a few shareholders who hold small shares may not decide a decision and it is not required for each shareholder to consent to it. Similarly, secret key given such a management also have more security and flexibility. In this case, RFID dynamic ownership transfer of owners with different weights has important research value.

ISSN: 1738-9976 IJSIA

2. Related Work

The ownership transfer of RFID tag has been done a lot of researches at home and abroad. Saito et al proposed a key update scheme [4], which could prevent the original owners to continue to read data of RFID tag after the ownership transfer. In the agreement, unique identification (ID) of RFID tag was encrypted by symmetric cryptography to prevent information about ID to be disclosed. When the new owner obtained the ID, the agreement encrypted the new key through a trusted third party (TTP). But the defect of the program is necessary to introduce a trusted third party to increase the complexity. Duc et al proposed the security agreement with a low complexity by using a random number generator (PRNG) and cyclic redundancy check (CRC) methods [5], but the protocol cannot prevent denial of service attacks, detect illegal tag, and provide forward security function. Osaka et al proposed a new RFID security mechanisms based on Hash functions and symmetric cryptosystem that could meet the security features of RFID system [6], in which privacy of the original owner and the new owner could be protected by changing the symmetry private key in the process of the transfer of ownership. Similarly, the program also has some shortcomings, such as protocol cannot resist denial of service attack and the attacker can track the tag. Kulseng proposed lightweight RFID ownership transfer protocol which required a third-party involvement [7]. The efficiency of the protocol is higher than the agreement based on Hash function, but the application of the protocol was limited because of the third-party involvement, and there was not a detailed analysis for resisting aggression. He Lei, Gan Yong et al proposed an ownership transfer protocol based on random permutation function to solve the safety problems of RFID tag system encountered during the transfer of ownership [8]. Gan Yong, Li Tianbao et al proposed a new RFID tag ownership transfer protocol [9]. The lightweight operations were adopted in the communication process of protocol, and the tag anonym which was processed by Pseudo-random Encryption Function was transmitted in wireless channel. Besides, it used a shared key recovery mechanism for authentication and authorization between the tag and the owner to ensure the robustness of the agreement.

Based on the above analysis, these agreements are for a single owner. Ownership transfer of RFID tag with multiple owners has not been solved perfectly, so the insecurity still exists and needs to be expended further discussion and study in the transfer process. To ensure the security and flexibility of the label, the paper from another angle proposes an ownership dynamic transfer protocol, which uses the secret sharing scheme [10] in which at least t or more participants pool their secrets shadows and reconstruct the secret key at the same time to manage a key, and recovers and distributes the secret key of a tag based on the Lagrange according to the weights of the owners.

3. Program Description

3.1. The Main Idea

In the life cycle of a tag, the weights of different owners may vary, because some owners will sell their weights, and some entity can become the new owners by buying weight of a tag. When there is a change on weights of owners, the paper designs a dynamic ownership transfer scheme based on Lagrange to complete the transfer of multiple owners with different weights. In the program the secret key will be divided into several sub secret key, and then the owners can get the corresponding the sub secret keys via a secure channel. When the key needs to be recovered, firstly to judge whether the sum of the weights about the owners participated in the restoration of the secret key is equal to or greater than t, if the condition can be met, the secret key can be got or not. Therefore, enhancing security and improving the flexibility in the practical application both are achieved in the dynamic ownership transfer. Once the secret key is recovered, it needs to be updated immediately to ensure the failure of original secret key, and the new

key needs to be divided to several parts and distributed to the owners according to the new weights.

3.2. System Initialization

Let $P = \{P_1, P_2, ..., P_n\}$ for n owners of a tag, w_i is the corresponding weight of owner P_i (on the border of m), w_{ni} means corresponding weight value of owner of P_i in a new round after the weights varying, $w_{ij}$is the weight which owner P_i purchases from owner P_j, Tag is the representative of a label, TID is the unique identify of tag, S represents the original key for communication with the original owner, and S_{ij} ($1 \leq j \leq w_i$) represents the owners with different weights to get different number of sub secret keys, S_{new} represents the secret key to communicate with the owners after the weights have a change .

3.3. Weights Sale Process

Now suppose a tag has three owners named P_1, P_2, and P_3, and respectively the weights of them are one, one as well as two, and the communication channel between the owner and the tag is safe. When the owner P_1 whose weight is one purchases a part of shares from the owner P_3 whose weight is two and the owner P_2whose weight is one also purchases a part of shares from the owner P_3 as well as a part of shares from the owner P_1, the weights among the owners will change completely. The process is shown as Figure1:

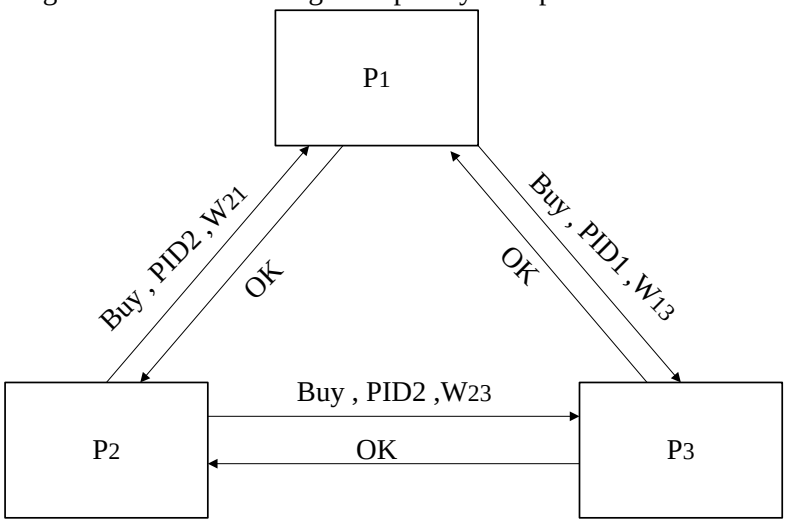


Figure 1. The Process of Purchasing Weights among Owners

From the figure l, we can clearly see that when there is an owner who want to purchase weights from other owners, it will send a request of buy, with its identity and the weights that it want to purchase. And when the owner agrees to sell its weights, it will send an OK to the buyer.

3.4. Key Recovery Process

When the weights of the owners of the RFID tag change, the owners need to complete the authentication with the tag, and restore the original secret key S. The specific process of authentication and recovery is shown in Figure 2:

Figure 2. The Process of Recovery Key and Certification

1. The original owner P_1 of the tag sends a request, with generating a random number R_{o1} to the tag.

2. After the label receives the request from P_1, it will generate a random number R_{t1} and calculate M = H (TID ⊕ Ro1 ⊕ Rt1), which will simultaneously be sent to the owner P_1.

3. When the messages from the tag are received by the owner P_1, the result will be calculated with R_{t1}, $R_{o1}$and TID ' stored in back-end database. If there is H (TID' ⊕ Ro1 ⊕ Rt1) = M, the label is certified. And then the back-end database generates a random numbers R_{r1}, the owner P_1 will sent L (S_{11} ⊕ R_{r1}), H (w_1 ⊕ R_{r1}), H (w_{n1} ⊕ R_{r1})and R_{r1} to the Tag.

4.Similarly, the original owners P_2 and P_3 respectively send L (S_{21} ⊕ R_{r2}), H (w_2 ⊕ R_{r2}), H (w_{n2} ⊕ R_{r2}), R_{r2},L (S_{31} ⊕ R_{r3}), L (S_{32} ⊕ R_{r3}), H (w_3 ⊕ R_{r3}), H (w_{n3} ⊕ R_{r3}) and R_{r3} to the tag.

5. When the tag receives the messages sent by the owners, it needs to judge whether the condition is satisfied that the sum of the weights of the owners is equal to or greater than t, namely $\Sigma_{p\in A}w_i$> = t,in which A is a set of participants agreed to recover the key. If it is met, the key S' can be recovered according to Lagrange algorithm:

$$f(0) = \sum_{i=1}^{t} y_i \left\{ \prod_{1\le j\le t, i\ne j} \frac{(0 - x_j)}{(x_i - x_j)} \right\}$$

And then the key S and key S' recovered by Lagrange are compared, if there is S = S', the original owners is lawful. Therefore, the paper not only completes the two-way authentication but also recovers the secret key S.

3.5. Ownership Transfer Process

According to comparison of the old and new weights received from the owners to see whether the weight value is changed, when a change occurs, the secret key S needs to be updated to S_{new} which will be divided into several sub secret keys, and then the owners will be given the corresponding parts based on the new weights. At the first, the tag will arbitrarily select t-1 elements named a_1, a_2, ..., a_{t-1} in the finite field GF (q) (q is a large prime numbers) to construct t-1 degree polynomial:

$$f(x) = S_{new} + \sum_{i=1}^{t-1} a_i x^i$$

Secondly, the tag will assign the corresponding secret shares S_{ij} according to new weights w_{ni} of owners:

$$S_{ij} = f(x_{ij}), 1<=j<=w_{ni}$$

in which x_{ij} is equal with (i-1) m + j, and m is an upper bound for the weight of participants. And finally, S_{ij} will be sent to each participant through a secure channel.

4. Security Analysis

Firstly, from the perspective of security requirements [11-12] in the field of RFID, security refers to one or more of the following elements: 1) the confidentiality of the Security 2) the integrity of the contents of the message 3) the sender and recipient authentication 4) effectiveness (availability). Specific security problems faced by a RFID system mainly include the following: spoofing attack, replay attack, tracking, man-in-the-middle attack. So this paper will analyze the security of the protocol from the aspects.

1) Spoofing attack

If there is an attacker masquerading as a legitimate owner to send Query and a random number R_{o1} to a tag, the attacker will fetch a response from tag: M = H (TID $\oplus R_{o1} \oplus R_{t1}$), R_{t1}. When the real legitimate owner sends Query and R'_{o1} , the attacker will send M = H (TID $\oplus R_{o1} \oplus R_{t1}$) and R_{t1} to the owner. Since the owner generates a new random number each time in the authentication session, that is to say R_{o1} is not equal to R'_{o1}, an attacker cannot spoof a legitimate label to conduct spoofing attacks. Therefore, the protocol is safe for spoofing attacks.

2) Replay attack

After the owner sends Query and R_{o1} to the label, the attacker gets the response from the tag: M = H (TID $\oplus R_{o1} \oplus R_{t1}$), R_{t1} and then repeatedly sends the information to owners in order to do replay attack. But the Query from owners and the response from label are different each time, so repeatedly sending the same message cannot be certified. Therefore, the protocol is safe for replay attack.

3) Tracking

When an attacker disguised as a legitimate owner sends Query and R_{o1} to the label, he will get the response from tag: M = H (TID $\oplus R_{o1} \oplus R_{t1}$), R_{t1} and then track the label by analyzing the response. But the label will produce a new random number R'_{t1} in each authentication session, and Hash with a one-way operation is safe, so the attacker will not know the response received from which label. Therefore, the protocol is safe for tracking.

4) Man-in-the-middle attack

Throughout the process of RFID tag ownership transfer, the two-way authentication has been joined, so an attacker cannot get the message by identity disguised to achieve attack. Therefore, the protocol is safe for man-in-the middle attack.

Last but not least, the protocol also ensures that the owners cannot do any operation with original weights to achieve a full ownership transfer of RFID tag, that is to say that it ensures forward and backward security.

5. Simulation

For the dynamic ownership transfer protocol set forth above, the paper has done a simulation experiment to prove the availability of this protocol under the Linux system where CPU is 3.60GHz and the memory is 4GB. Three sets of data are obtained by doing the experiment which respectively are the results when the sum of the weights is equal with two or greater two, equal with five or greater five and equal with nine or greater nine. And each set of data consists of three parts which respectively are the number of owners, the sum of the weights involved in recovery and the time consumed by the tag to implement the protocol. The result is shown in Figure 3, in which microseconds is the time unit and the horizontal axis represents a set of data, the vertical axis represents the specific situation of each data.

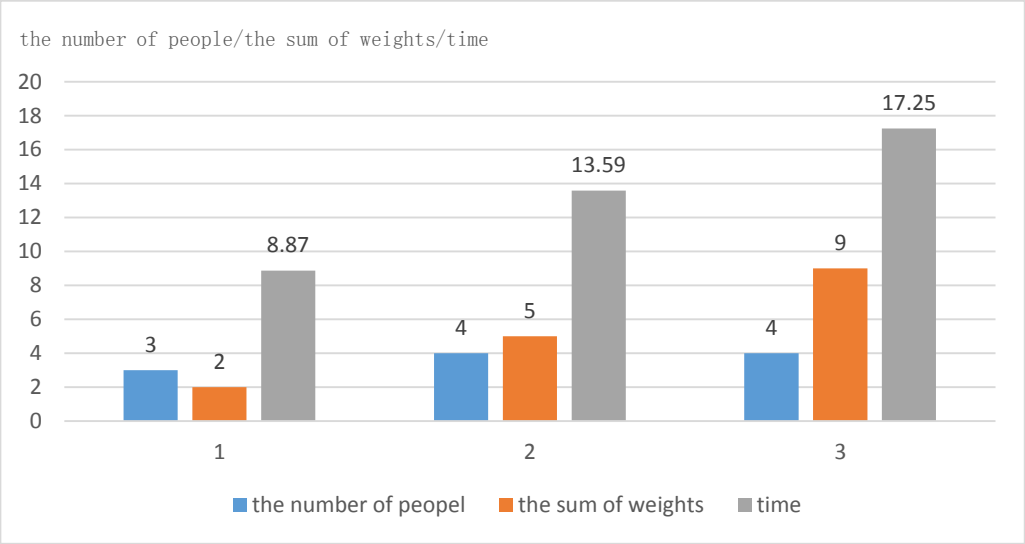


Figure 3. Time-consuming of the Tag

As can be seen from the figure, when there are four owners for a tag, and requiring the sum of weights is equal with five, it needs 13.59/us to achieve the goal. But when there are also four owners for a tag, and requiring the sum of weights is equal with nine, it needs 17.25/us to achieve the goal. Therefore, the execution time of a tag is independent of the number of owners, but about the sum of weights. And the more weights it requires, the more time it will consume. What is more, it also can be seen that it is a suitable to apply the protocol for low-cost tags, because the calculation can be completed in a short period of time.

6. Conclusion

This paper proposes a RFID tag dynamic transfer protocol to support the key negotiation between the tag and multi-owner who have different weights. When weights of the owners have a change, it is necessary to dynamically update the secret key. So the owners need to conduct two-way mutual authentication with the tag, recovering the original secret key of the label based on Lagrange according to the sum of the weights and the various sub-key. And then the tag will update the key which later will be divided into several parts according to the sum of new weights. Finally, each owner can get the corresponding amounts of sub secret key which are equal with the values of the weight. Since a single owner or multiple owners whose weights are not satisfied with the conditions cannot communicate with the tag, the security of RFID tag ownership transfer is improved. The agreement not only achieves fully ownership transfer of RFID tag but

also ensures the forward security and backward security of information, and at the same time other security requirements of RFID tag system can met such as not tracking, anti-middle attacks, anti-replay attacks and so on. Simulation results show that the time-consuming of calculation is acceptable for low-cost tags in this paper. In ensuring the safety of ownership transfer, how to shorten the time-consuming and computation of tag is the next problem needed to be solved. Importantly, when there is a new owner to join or the ownership of a tag fully is received by other new owners, it is necessary to design a new RFID ownership transfer protocol to achieve the transfer.

Acknowledgements

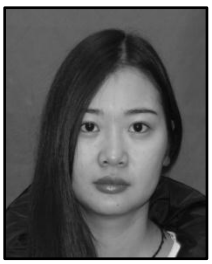
This paper is sponsored by National Natural Science Foundation of China, No. 61572445 and the key scientific research projects of colleges and universities in Henan province, NO.16A520075.

References

[1] Zhou Yongbin, Feng Dengguo. Design and analysis of RFID security protocols [J].computer, **(2006)**, 29 (4): 581-589).
[2] Ding Zhenhua, Li Jintao, Feng Bo. RFID-based security authentication Hash Functions Protocols [J]. Computer Research and Development, **(2009)**, 46 (4): 583-592).
[3] Song B, Mitchell C J. RFID authentication protocol for low-cost tags [J]. Development & Change, **(1971)**, 2(2):98-106.
[4] Saito J, Imamoto K, Sakurai K. Reassignment Scheme of an RFID Tag's Key for Owner Transfer [M]. Embedded and Ubiquitous Computing – EUC 2005 Workshops. Springer Berlin Heidelberg, **(2005)**, 1303-1312.
[5] 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, **(2006)**.
[6] Osaka K, Takagi T, Yamazaki K. An Efficient and Secure RFID Security Method with Ownership Transfer [C].Computational Intelligence and Security, 2006 International Conference on. IEEE, **(2006)**, 1090 - 1095.
[7] Kulseng L, Yu Z, Wei Y, et al. Lightweight Mutual Authentication and Ownership Transfer for RFID Systems[C].INFOCOM, 2010 Proceedings IEEE. IEEE, **(2010)**, 1-5.
[8] He Lei, Gan Yong, Yin Yifeng. RFID tags ownership transfer protocol based on random permutation function [J] Zhengzhou University: Engineering Science, **(2013)**, 34 (6): 24-27.
[9] Gan Yong, LI Tianbao, Xu Yunqian. Research on lightweight anonymous secure ownership transfer protocol of RFID tag [J] Zhengzhou University of Light Industry: Natural Science Edition, **(2015)**, (2): 52-55.
[10] Yang C C, Chang T Y, Hwang M S.A (t, n) multi-secret sharing scheme [J].Applied Mathematics & Computation, **(2004)**, 151(2):483-490.
[11] Ranasinghe C, Engels D W, Cole P H. Low-cost RFID systems: Confronting security and privacy [J]. In: Auto-ID Labs Research Workshop, **(2005)**, 17(5):12 - 21.
[12] Stajano F, Anderson R. The Resurrecting Duckling: Security Issues for Ad-hoc Wireless Networks [M] Security Protocols. Springer Berlin Heidelberg, **(2000)**, 172-182.

Authors

Gan Yong, He got his Ph.D. in Computer Science and Technology from Xi'an Jiaotong University. He is a professor in the School of Computer and Communication Engineering, Zhengzhou University of Light Industry and dedicated to research computer network and its security. He has published more than 50 research papers in journals and conferences.



Yang Zong-qin, She received the B.S. degree in network engineering from Zhengzhou University of Light Industry, Zhengzhou, China, in 2014. She is currently pursuing the master's degree at the School of Computer and Communication Engineering, Zhengzhou University of Light Industry. Her current research interests include RFID tag ownership transfer among multiple owners with different weights.

He Lei, He received his Master Degree in Cryptography from Southwest Jiaotong University in 2006. He is now an associate professor 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 30 research papers in journals and conferences.

Du Chao, He received the B.S. degree in Software Engineering from Zhengzhou University, Zhengzhou, China, in 2010. He is currently pursuing the master's degree at the School of Computer and Communication Engineering, Zhengzhou University of Light Industry. His current research interests include authentication scheme under Internet of Things.