International Journal of Security and Its Applications
Vol. 10, No. 10 (2016) pp.147-154
http://dx.doi.org/10.14257/ijsia.2016.10.10.14

RFID Tag Ownership Transfer Protocol of Multi-owner with Different Weights Based on Lagrange Algorithm

Gan Yong, Yang Zong-qin, He Lei and Du Chao

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

Abstract

As it is known, the researches on ownership transfer issues of RFID tag have focused on a single owner. However in practice, RFID tag may have multiple owners who occupy different weights. To solve the problem, the ownership transfer protocol of multi-owner with different weights based on Lagrange has been proposed. Assuming the key is divided into n parts in this paper, and the owner gets the corresponding sub secret key according to the weight. Then, If and only if the sum of the weights of the owners involved in the restoration of the secret key is equal to or greater than t, the secret key can be obtained, or not. Therefore, security of ownership transition and flexibility in the practical application are enhanced.

Keywords*: RFID tag, ownership transfer, Lagrange algorithm*

1. Introduction

RFID (Radio Frequency Identification) [1] is a non-contact automatic sensing technology, which can automatically obtain specific information about goals by electronic magnetic field, without establishing physical contact. With its small size, large capacity, long life, reusable and so on, in recent years, RFID technology has been widely used in various aspects of life, such as supply chain management, retail, health care, anti-counterfeiting security, transportation and other fields [2]. However, some disadvantages of wireless communication [3] and RFID system itself make that RFID security privacy cannot be guaranteed. And in practice most of the RFID tag may carry on the transfer of ownership in their life cycle, which makes security and privacy of tags become more difficult.

Then currently, the application about ownership transfer of a single owner has been unable to meet the needs of the majority market. Because In practice, tags may have more than an owner, and different owners may have different weights. For example, there is a company charged by the chairman and members of senior directors who may hold different shares due to different identities or functions. So, only when the shares of the shareholders who supports the decision more than a certain value, the decision can be determined, or not. That is to say, several shareholders who hold small shares may not decide a decision, but there is no need to get the consent of each shareholder. Similarly, the secret key given such a management also have more security and flexibility. In this case, the RFID tag ownership transfer between owners with different weights has important research value.

2. Related Work

Ownership transfer issues of RFID tags have carried out extensive researches at home and abroad. In 2005, Molnar, who first proposed the label ownership transfer issue, designed a pseudonym protocol based on secret key tree to achieve ownership transfer [4].

ISSN: 1738-9976 IJSIA

Although there were two methods proposed in the protocol to achieve the ownership transfer of RFID tags, the two methods essentially are only temporary authorization, in which new owner just got part of the information not safely gained control of the tags. Accordingly, the agreement did not achieve fully transfer of ownership. Then Lim and others proposed a two-way authentication protocol in which transfer of ownership can be achieved completely [5]. While this protocol needed higher computing power of label, and there was no specific description of the new owner is how to securely get the tag information. Besides, Fouladgar and Afifi proposed a simple and effective ownership transfer protocol which could protect the privacy of the new owner, but the tag would easily be tracked and impersonated [6]. Additionally, GAN Yong and Yang Jia-jia proposed RFID tag ownership transfer protocol based on an optional model [7] which used the password of reader to encrypt information and the original owner could choose whether to apply for reinstate authorization after releasing the ownership to protect the security of privacy. What is more, He Lei *et. al.*, proposed an ownership transfer protocol with transfer switch to protect the information security in the ownership transfer procedure [8]. In the protocol, tags and owners share two keys which are respectively used for mutual authentication and ownership transfer, and ownership transfer switches are set to allow ownership transfer and resist desynchronization attacks.

Based on the above analysis, it can be seen that they are for a single owner. So ownership transfer issues of RFID tag have not been perfectly resolved and there are some questions need to expend further discussion and study, such as insecurity and the protocol of multi-owner with different weights in the transfer process. To ensure the security and flexibility of using the tag, the paper puts forward an ownership transfer protocol of multi-owner with different weights from another point of view, which uses secret sharing scheme [9-10] to manage secret key, and utilizes Lagrange algorithm to restore and distribute secret key according to the weight of owners.

3. Program Description

This part is the core idea of this paper, because it not only describes the agreement in which multiple owners with different weights sell their ownership to a new entity, but also displays the process of RFID tag ownership transfer graphically to prove the feasibility of the protocol.

3.1. The Main Idea

For a complete ownership transfer protocol of RFID tag, firstly, we must ensure that the new owner can get all the relevant information, including control of the tag. And secondly the original owner can no longer make any operation to ensure the privacy of a new owner. Finally other requirements of security and privacy of RFID systems must be met. According to the above conditions, the paper designs an ownership transfer protocol based on a secret key sharing scheme of Lagrange to achieve transfer among several owners with different weights. The key of a tag will be divided into several sub secret keys which will be distributed to the owners who can get corresponding parts according to their weights via a secure channel in the program. When the sum of the weights about the owners participated in the restoration of the secret key is equal to or greater than t, the shared secret key can be recovered according to the Lagrange algorithm

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

to ensure security of ownership transfer and flexibility in the practical application. And when the key is recovered, it is necessary to update the key immediately for a new owner to ensure the failure of the secret key of the original owner.

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 the owner P_i, T means the tag, TID is the unique identify of tag, S represents the key to communicate with the original owner, S_{ij} $(1 \leq j \leq w_i)$ means that the owner gets different number of sub secret keys according to the weights, and S_{new} represents a new key that can achieve the communication between the tag and the new owner.

3.3. Key Recovery Process

When there is a new owner to apply for the ownership transfer of the RFID tag, the original owners are required to complete the certification between the original owners and the tag to restore the original's secret key. Now suppose a tag has three owners, the weights of each owner respectively are 1, 1, 2, and the communication channels between the original owners and the new owner is safe. The specific process is shown in Figure 1:

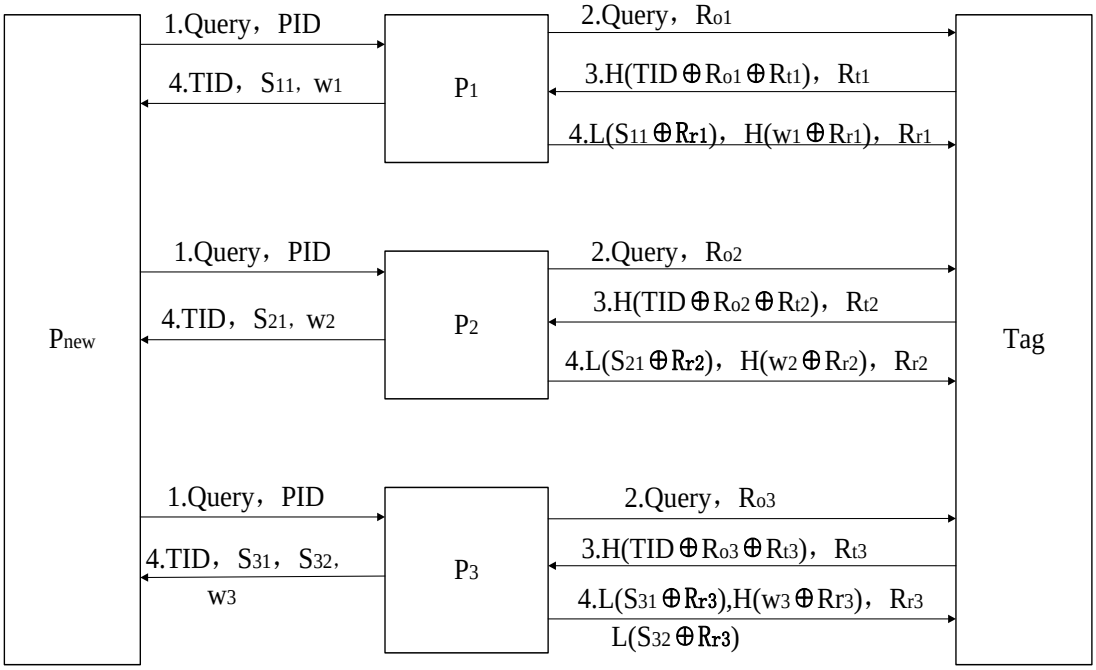

Figure 1. The Process of Recovery Key and Certification

1. When P_{new}, the new owner asks for ownership transfer to the original owners respectively named P_1, P_2, P_3, the identity PID of the new owner is passed to the original owners.

2. When the original owner P_1 agrees to the application, it will send a request to the tag with generating a random number R_{o1}.

3. When the tag gets the request from P_1, it will generate a random number R_{t1}, and calculate $M = H(TID \oplus R_{o1} \oplus R_{t1})$, which will be sent to the original owner P_1 simultaneously.

4. When the message from the tag is received by P_1, it will use TID ' stored in back-end database to calculate the result with R_{t1} and R_{o1}, and then if the result of $H(TID' \oplus R_{o1} \oplus R_{t1})$ is equal with M, the label is certified. The back-end database will generate random numbers R_{r1}, then $L(S_{11} \oplus R_{r1})$, $H(_{w1} \oplus R_{r1})$ and R_{r1} are sent to the tag. At the same time, the identify TID of the label, the weight w_1 of the original owner P_1 , as well as the sub secret key S_{11} will be sent to the new owner through a secure channel.

5. Similarly, if the original owner P_2 and P_3 also agree to the application, they will respectively send $L(S_{21} \oplus R_{r2})$, $H(w_2 \oplus R_{r2})$, R_{r2}, $L(S_{31} \oplus R_{r3})$, $H(w_3 \oplus R_{r3})$, R_{r3} , L

($S_{32}\oplus R_{r3}$) to the label. The new owner will get identify TID of the tag, the weights w_2, w_3 of the original owners and their respective sub secret key S_{21}, S_{31}, S_{32} through a secure channel.

6. When the label Tag receives a message sent by the original owners, it will calculate the sum of weights of original owners who agree to convert the ownership. If the condition that the sum is equal to or greater than t is satisfied, the key S' can be recovered according to Lagrange algorithm. And then the key S and key S' recovered by Lagrange are compared, if there is S = S', the original owners are lawful so that the two-way authentication is completed, and the secret key S is recovered.

3.4. Ownership Transfer Process

After the new owner receiving the label information given by the original owners, it will send a request to the label, and then do the mutual authentication with the tag. When the authentication is passed, it is necessary to execute key agreement in order to communicate with each other. Specific implementation process is shown in Figure 2:

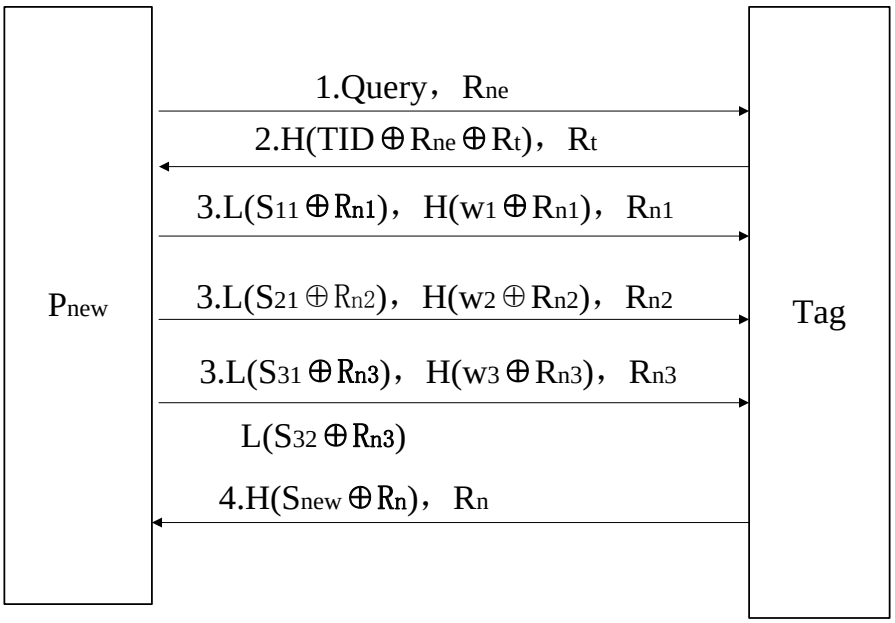

Figure 2. The Process of Ownership Transformation

1. The new owner P_{new} sends the request to the tag, with generating a random number R_{ne}.

2. After the label receiving a request from P_{new}, it will generate a random number R_t, and calculate M = H (TID⊕R_{n1}⊕R_t), which will be simultaneously sent to the new owner P_{new}.

3. When the new owner P_{new} receives the message from the tag, it will calculate H (TID⊕Rn1⊕Rt) with R_{n1}, R_t and TID sent by the original owner. If the result of calculation is equal with M, the label is certified.

4. The new owner P_{new} respectively computes L ($S_{11}\oplus R_{n1}$), H ($w_1\oplus R_{n1}$), L ($S_{21}\oplus R_{n2}$) , H ($w_2\oplus R_{n2}$), L ($S_{31}\oplus R_{n3}$), H ($w_3\oplus R_{n3}$),L ($S_{32}\oplus R_{n3}$) with the information from the original owners and generating the random number Rn1, Rn2, Rn3, and then send them to the label.

5. After the tag receiving the message sent by the new owner, it will calculate the sum of weights sent by the new owner to see whether the sum is equal to or greater than t. If the condition is satisfied, the key S' can be recovered according to Lagrange algorithm. And then if there is S = S', the new owner is verified.

6. The tag will update the new key S_{new} for the new owner, as well as generating a random number R_n, which will be send to the new owner. So the new owner can start communication with the tag.

4. Security Analysis

The agreement firstly does not allow the original owners do any operation to the tag to achieve a complete transfer of ownership, and then meets other security requirements of RFID system, and finally achieve the security transfer.

Fully transfer ownership: When the owner varies, the program updates the secret key so timely that the original owners can no longer carry out any operation to the tag. The new owner obtains all the information of the label to get the ownership of the tag. And the new owner will not know the original secret key of the tag, so it cannot review all the information before. Thus, the program guarantees forward and backward safety at the same time.

Non-tracking: There will be a random number in each response message between the tag and the owners. Even if the attacker continues to send the same message to the tag, but each response of the tag is different, so the attacker cannot distinguish respond information from a tag and cannot do track.

Anti-middle attacks: the two-way authentication is added to ensure security throughout the ownership transformation process, so an attacker cannot get the message to achieve attack through disguising the identity.

Anti-replay attack: During the messages delivery, a random number is added to each session and the messages have been hashed. An attacker posing as a legitimate owner or legitimate tag cannot get any useful information because the query and the response is different each time. There repeating the same message cannot get the certification.

5. Simulation

For the protocol set forth above, the simulation experiment has been done to prove the availability of this protocol in the Linux system whose CPU is 3.60GHz and the memory is 4GB. There are three sets of data obtained by the experiment respectively when the threshold of restoring the key is equal with two, equal with five and equal with nine. And each set of data consists of three parts which respectively are the number of the 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.

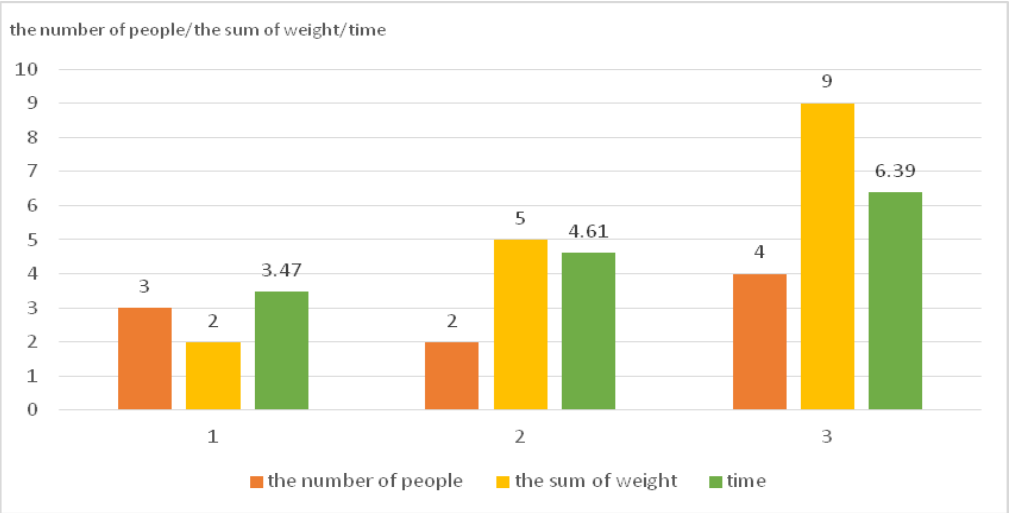

Figure 3. Time-consuming of the Tag

As can be seen from the figure, when there are three owners for a tag, and requiring the sum of weights is equal with two, it needs 3.47/us to achieve the goal. But when there are two owners for a tag, and requiring the sum of weights is equal with five, it needs 4.61/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 new ownership transfer protocol which supports the tag can make key negotiation with multiple owners who have different weights. Firstly, the new owner sends request to the original owners to apply for ownership transformation. And then when the former owners agree to the application, they will conduct a two-way mutual authentication with the tag. Finally depending on the sum of weights and the respective sub-key, the tag can recover the key and verify it based on Lagrange algorithm. Because a single owner or multiple owners who are not satisfied with the conditions can not communicate with the tag, the security is improved during the ownership transfer process. The agreement not only completes the full transfer of ownership but also ensures forward and backward security about the information of the tag, and it is the most important that security requirements of RFID system can be met, such as anti-middle attacks, replay attacks, and other anti-security. Simulation result shows that the computation time of the agreement is shorter, so it is suitable for low-cost tags. When the security is ensured, the next step need to solve the problem that how to shorten the computation time of the tag as well as safely distribute the secret key to the multiple owners whose weights change in the life cycle of a tag.

Acknowledgements

The authors would like to thank the editors and anonymous reviewers for their valuable comments. 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] Y. Zhanqing, “Radio Frequency Identification (RFID) Theory and Applications[M]”, Electronic Industry Press, **(2004)**.
[2] J. Yongming, S. Huiping and G. Zhi, “Transfer of ownership of RFID tag protocols [J]”, Computer Research and Development, vol. 48, no. 8, **(2011)**, pp. 1400-1405.
[3] H. Zheng-ming, “Talking about the security of wireless communication technology [J]”, Urban Construction Theory: Electronic Edition, **(2013)**.
[4] Molnar D., Soppera A. and Wagner D., “A Scalable, Delegatable Pseudonym Protocol Enabling Ownership Transfer of RFID Tags [J]”, Lecture Notes in Computer Science, vol. 3897, no. 2, **(2005)**, **pp.** 276-290.
[5] Lim C. H. and Kwon T., “Strong and Robust RFID Authentication Enabling Perfect Ownership Transfer [M]”, Information and Communications Security. Springer Berlin Heidelberg, **(2006)**, pp. 1-20.
[6] Fouladgar S. and Afifi H., “An efficient delegation and transfer of ownership protocol for RFID tags [J]”, The First International Eurasip Workshop on RFID Technology, **(2007)**.
[7] G. Yong, Y. Jia-jia and L. Tian-bao, “A new ownership transfer protocol with optional mode for RFID tags [J]”, Zhengzhou University of Light Industry: Natural Science Edition, **(2014)** May, pp. 52-55.
[8] H. Lei, G. Yong and Y. Yifeng, “RFID Tag Ownership Transfer Protocol with Transfer Switch [C]”, The "spike" group of computer science graduate student in Henan Province, **(2014)**.
[9] Pedersen T. P., “Non-Interactive and Information-Theoretic Secure Verifiable Secret Sharing [J]”, Lecture Notes in Computer Science, vol. 576, no. 12, **(1991)**, pp. 129-140.
[10] Shamir, “How to share a secret [J]”, Communications of the ACM, vol. 22, no. 11, **(1979)**, pp. 612-613.

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.