RFID Tag Dynamic Ownership Transfer Protocol for Multiple Owners

Yong Gan, Zongqin Yang, Lei He, Chao Du

School of Computer and Communication Engineering, Zhengzhou University of Light Industry, Zhengzhou 450002, China

Abstract

Existing research, the protocols about ownership transfer of RFID tag are all for a single owner. However, in practice, a tag may have multiple owners and the owners may have different weights. Besides, the owners may sell their weights to other entities to make the entities become new owners. So when a change in ownership, the key value needs to be dynamically updated in a timely manner. Therefore, this paper proposes a simple protocol based on Lagrange algorithm to achieve the dynamic ownership transfer of RFID tag for multi-owner with different weights. In the protocol, the new owners will get the weights and the original sub-key from the original owners by buying them. What is more, the protocol verifies the legitimacy of the original owners and the new owners by recovering the original secret key, and uses secret sharing algorithm to distribute sub-key according to the weights of the new owners. So it has more practical value as well as using value and enhances the security of the ownership transfer, and the simulation shows that the calculation and time consuming are not high in the protocol.

Keywords: multi-owner, shared secret key, dynamic ownership transfer.

1. INTRODUCTION

With the rapid development of the theory and technology about Internet of Things, RFID (Radio Frequency Identification), an automatic target recognition technology through the electronic magnetic field, has been widely used in the Internet of Things such as supply chain management, retail, security, transportation and so on, but with the emergence of new security and privacy issues. When there is a change in ownership transfer, because of the low-cost of RFID tag, storage capacity and computing power are very limited, traditional security technologies cannot be applied directly on the tag to make owners privacy and RFID security cannot be guaranteed. Therefore, privacy and security have become a major obstacle to the promotion of RFID, so it is the common goal of academia and industry to design the ownership transfer protocol of RFID tag.

Nowadays, the existing researches of domestic and foreign scholars are mostly for a single owner. That is to say, there is only an owner for a tag. But in practice, the tag may have more than one owner, the owners jointly possess the ownership of the tag, and different owners may have different weights. In life cycle of the tag, some owners may sell their weights to make ownership of a tag change. Just as when shareholders of a company whose shares are greater than a certain value agree to sell their shares to others, others will get the right of control. Similarly, when the ownership of the tag needs to be converted, the sum of weights of owners who agree to the ownership transfer is greater than the predefined threshold. If the condition is met, the ownership of RFID tag will be converted to other entities, namely, ownership transfer of the tag. Managing key like this is also more security and flexibility, so the dynamic ownership transfer for multiple owners with different weights has important research value.

2. RELATED WORK

RFID as an automatic identification technology, its main function is to be recognized by the system, which not only have common security problems with other systems, also face the problem — the personality privacy, including the privacy and position information of attachment, as well as the privacy problems during ownership transfer between in the original and new owners (Zhou and Feng, 2006).
At present, the scholars of domestic and foreign have carried out extensive research on the security and privacy issues about the ownership transfer, but their main researches have focused on the ownership transfer of a single owner. Saito et al., (2005) proposed two ownership transfer protocols, the one with a trusted third party, the other one without a trusted third party. And both protocols are used by the encryption function of key control, but it still cannot guarantee the forward security of the tag information. In 2007, Osaka et al., (2006) also proposed an ownership transfer protocol with a trusted third party and using the Hash function, but the protocol still cannot resist the desynchronization attack, and the tag can easily be tracked by the attacker. Since then, a number of other researchers tried to improve the Osaka protocol, such as in 2008, Yoon and Yoo (2008) proposed the improvement program, which modified the last message that the back-end database send to reader as well as reader send to the tag. Later, Zhou et al., (2011) believed the tag requires different types of ownership in the supply chain, and proposed a new certification ownership transfer plan of tag in order to achieve a seamless transition between them. Chen et al., (2009) also proposed improvement program based on the Osaka protocols, in the program a message was added to send to a tag by reader. Then Chen et al., (2013) proposed an ownership transfer mechanism of low-cost tag in line with EPCC1G2, which uses biological fingerprint to provide authentication two-way to ensure the security during the ownership transfer of RFID tag. Besides, He and Gan et al., (2014) proposed an ownership transfer protocol with retrospective ability and analyzed its security level by using GNY logic and a secure group ownership transfer protocol for tags in RFID system to transfer the ownership of multiple tags simultaneously. The two protocol all provide an authentication between the tag and owners and enable to resist the attacks. Moreover, the results of the empirical study show that the cost time of a tag is less than some other protocols and suitable for low-cost tags. Xu et al., (2016) put forward two kinds of multi-owners tag ownership security transfer protocol. These two protocols are based on the Chinese remainder theorem and the Lagrange interpolation algorithm, but the status of multi-owners is the same, so the actual situation may be not met.

3. PROGRAM DESCRIPTION

This part is the core content of this paper, it proposes a dynamic ownership transfer protocol for multi-owner with different weights. In the protocol, it firstly uses a secret sharing management scheme to manage the key, which means in a \((t, n)\)-threshold secret sharing (Shamir, 1979), a dealer first divides a secret into \(n\) shares to be distributed among \(n\) players. Subsequently, at least \(t\) players can collaborate to recover the secret. And the secret sharing based on the Lagrange polynomial interpolation system (Shamir, 1979) and vector system (Blakley, 1979) which respectively was proposed by Shamir and by Blakley has been widely studied and applied. This protocol also uses Lagrange formulation to recovery the original key and distributes the new sub secret key based on the weights of the owners. So when there is an ownership transfer of RFID tag, the key can dynamically be updated in time to ensure the security and flexibility.

3.1. The main idea

In the life cycle of a tag, the owners may sell their weights to other entities to make them become new owners. So when a change in ownership, the key value needs to be dynamically updated in a timely manner. When multiple owners of the tag change, that is to say, the ownership of the tag is transferred, this paper designs a dynamic ownership transfer protocol which uses secret key sharing scheme based on Lagrange formulation to achieve the transfer among multiple owners with different weights.

In the protocol, when the new entities get the weights and the original sub-key from the original owners by buying them to make themselves become the new owners, it is necessary to authenticate mutual legitimacy of the tag and the owners by restoring the original secret key. But only when the sum of weights of the owners involved in recovering the secret key is equal to or greater than \(t\), the shared secret key can be recovered based on the Lagrange formulation.

\[
f'(0) = \sum_{i=1}^{x} y_i \prod_{1 \leq j < i \text{ or } i \neq j} \frac{0 - x_j}{x_i - x_j}
\]  

(1)

Similarly, the new owners and the tag must be authenticated. When everything is completed, the new key will be divided into several sub secret key by secret sharing, and new owners will get corresponding sub-key according to the weights of the new owners.
3.2. System initialization

Let $P = \{P_1, P_2, \ldots, P_n\}$ for $n$ owners of a tag, $w_i$ is the corresponding weight of owner $P_i$, $Q = \{Q_1, Q_2, \ldots, Q_m\}$ for new owners of a tag, $w_{ni}$ means corresponding weight value of new owner $Q_i$ (on the border of $m$), $w_{ni}$ is the weight which owner $P_i$ purchases from owner $Q_i$. 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 sub secret keys of original owners with different weights, $S_{new}$ represents the new secret key to communicate with the new owners, and $S_{nj}$ $(1 \leq j \leq w_{ni})$ represents the owners with different weights to get different number of sub secret keys.

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 owners is safe. When the new owner $Q_1$ purchases shares from the original owner $P_1$, the new owner $Q_2$ purchases shares from the original owner $P_2$, and the new owner $Q_3$ purchases shares from the original owner $P_3$. The owners of RFID tag will change completely. The process is shown as Figure 1:

![Figure 1. The process of purchasing shares from original owners](image)

From the figure 1, we can clearly see that when there is a new owner who wants to purchase shares from an original owner, it will send a request of buy, with its identity. And when the original owner agrees to sell its shares, it will send the unique identification of tag (TID), the sub secret key and the weights to the buyer.

3.4 Original owner certification

When the owners of the RFID tag change, the secret key needs to be updated. So the owners need to complete the mutual authentication with the tag by restoring the original secret key $S$ to prevent normal communication from being damaged between the original owners and the tag due to the impersonation attack from attackers. The specific process of authentication and recovery is shown in Figure 2:

1. The original owner $P_1$ of the tag sends a request, with generating a random number $R_{p1}$ to the tag.
2. After the label receives the request from $P_1$, it will generate a random number $R_{t1}$ and calculate $M = H(\text{TID} \oplus R_{p1} \oplus R_{t1})$, 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 $R_{t1}$, $R_{p1}$ and TID stored in back-end database. If there is $H(\text{TID} \oplus R_{p1} \oplus R_{t1}) = M$, the label is certified. And then the back-end database generates a random numbers $R_{p1}$, the owner $P_1$ will sent $L(S_{11} \oplus R_{p1}), H(w_{1} \oplus R_{p1})$ and $R_{p1}$ to the Tag.
4. Similarly, when the tag is proved to be legitimate by the original owners $P_2$ and $P_3$, they respectively send $L(S_{21} \oplus R_{pt2}), H(w_2 \oplus R_{pt2}), R_{pt2}, L(S_{31} \oplus R_{pt3}), L(S_{32} \oplus R_{pt3}), H(w_3 \oplus R_{pt3})$ and $R_{pt3}$ to the tag.

5. When the tag receives the messages sent by the owners, if the sum of the weights of the owners is equal to or greater than $t$, the key $S'$ can be recovered. And then the key $S$ and key $S'$ recovered by Lagrange are compared, if there is $S = S'$, the original owners are lawful. Therefore, the two-way authentication is completed.

$$\begin{align*}
\text{Tag} & \quad \text{P1} \\
1.\text{Query}, \quad R_{q1} & \quad 2.\text{H(TID} \oplus R_{q1} \oplus R_{nt1}), \quad R_{nt1} \\
3.\text{L(S}_{11} \oplus R_{nt1}), \quad H(w_{1} \oplus R_{nt1}), \quad R_{nt1} & \\
\text{P2} & \quad \text{P3} \\
1.\text{Query}, \quad R_{q2} & \quad 2.\text{H(TID} \oplus R_{q2} \oplus R_{nt2}), \quad R_{nt2} \\
3.\text{L(S}_{11} \oplus R_{nt2}), \quad H(w_{2} \oplus R_{nt2}), \quad R_{nt2} & \\
\text{Tag} & \\
1.\text{Query}, \quad R_{q3} & \quad 2.\text{H(TID} \oplus R_{q3} \oplus R_{nt3}), \quad R_{nt3} \\
3.\text{L(S}_{31} \oplus R_{nt3}), \quad L(S_{32} \oplus R_{nt3}), \quad H(w_{3} \oplus R_{nt3}), \quad R_{nt3} & \\
\end{align*}$$

**Figure 2.** The process of mutual authentication between the owner and the tag

### 3.5 Ownership transfer process

When the owners of the tag sell their weights, there will be some new entities to become the new owners of RFID tag. Not only the original owners need to complete the certification with the tag, the new owners also need to complete the certification. And then when the new owners are legal, the tag will distribute the new sub secret key to it according to their new weights. The specific ownership transfer process shown in Figure 3:

$$\begin{align*}
\text{Tag} & \quad \text{Q1} \\
1.\text{Query}, \quad R_{q1} & \quad 2.\text{H(TID} \oplus R_{q1} \oplus R_{nt1}), \quad R_{nt1} \\
3.\text{L(S}_{11} \oplus R_{nt1}), \quad H(w_{1} \oplus R_{nt1}), \quad H(w_{2} \oplus R_{nt1}), \quad R_{nt1} & \\
6.\text{H(S}_{n11} \oplus R_{nt1}), \quad R_{nt1} \\
\text{Q2} & \quad \text{Q3} \\
1.\text{Query}, \quad R_{q2} & \quad 2.\text{H(TID} \oplus R_{q2} \oplus R_{nt2}), \quad R_{nt2} \\
3.\text{L(S}_{21} \oplus R_{nt2}), \quad H(w_{2} \oplus R_{nt2}), \quad H(w_{2} \oplus R_{nt2}), \quad R_{nt2} & \\
6.\text{H(S}_{n21} \oplus R_{nt2}), \quad H(S_{n22} \oplus R_{nt2}), \quad R_{nt2} \\
\end{align*}$$

**Figure 3.** The process of RFID tag ownership transfer

483
1. The new owner $Q_1$ of the tag sends a request, with generating a random number $R_{q1}$ to the tag.

2. When the label receives the request from $Q_1$, it will generate a random number $R_{nt1}$ and calculate $M = H (TID \oplus R_{q1} \oplus R_{nt1})$, which will simultaneously be sent to the owner $Q_1$.

3. When the owner $Q_1$ receives the messages, it will calculate $M' = H (TID' \oplus R_{q1} \oplus R_{nt1})$ with $R_{nt1}$, $R_{q1}$ and $TID'$ received from $P_1$. If there is $M' = M$, the tag is legal. And then the back-end database generates a random numbers $R_{qt1}$, the owner $Q_1$ will sent $L (S_{11} \oplus R_{qt1})$, $H (w_{n1} \oplus R_{qt1})$, $H (w_1 \oplus R_{qt1})$ and $R_{qt1}$ to the Tag.

4. Similarly, the new owners $Q_2$ and $Q_3$ respectively send $L (S_{21} \oplus R_{qt2})$, $H (w_{n2} \oplus R_{qt2})$, $H (w_2 \oplus R_{qt2})$, $R_{qt2}$, $L (S_{31} \oplus R_{qt3})$, $L (S_{32} \oplus R_{qt3})$, $H (w_{n3} \oplus R_{qt3})$, $H (w_3 \oplus R_{qt3})$ and $R_{qt3}$ to the tag.

5. As to verify the original owners, the tag needs to recover the key $S'$ through the messages sent by the new owners, if there is $S = S'$, the new owners are lawful.

6. The tag will update key, and arbitrarily select t-1 elements named $a_1$, $a_2$, ..., $a_{t-1}$ to construct $t-1$ degree polynomial:

$$f(x) = S'_{new} + \sum_{j=1}^{t-1} a_j x^j$$ (2)

And then the tag will calculate the new sub secret key $S_{nij}$ according to new weight $w_m$ of the new owner:

$$S_{nij} = f(x_{ij}) (1 \leq j \leq w_m)$$ (3)

in which $x_{ij}=(i-1) m + j$, and $m$ is an upper bound for the weights of owners. That is to say, the tag will generate new sub keys $S_{n11}$, $S_{n21}$, $S_{n31}$ and $S_{n32}$, with generating random number $R_{nq1}$, $R_{nq2}$ as well as $R_{nq3}$, and respectively send the sub key encrypted by Hash function to the new owners, namely, $H(S_{n11} \oplus R_{nq1})$, $H(S_{n21} \oplus R_{nq2})$, $H(S_{n31} \oplus R_{nq3})$.

4. SECURITY ANALYSIS

The security and privacy issues of the RFID tag are the main reasons why it has not been widely applied. In the process of ownership transfer, three requirements need to be met: firstly, the original owners can continue to operate the tag to protect the privacy of the new owners after the ownership transfer. Secondly, when the new owners obtain the ownership of the tag, they cannot view previous data in order to protect the privacy of the original owners. Finally, it also needs to ensure to resist tracking attacks, replay attacks and so on in the process of ownership transfer. This paper will analyze and verify the protocol from the above aspects.

1) backward security

When there are new entities to be the new owners, the tag will timely update the key with the owners in the protocol to ensure that the original owners cannot do any operation to the tag to achieve a full ownership transfer of RFID tag, that is to say that it ensures backward security.

2) Forward security

When the two-way authentication is completed between the new owners and the tag, the tag will update the key to replace the original secret key to make that the original key is invalid.

3) Impersonation attack
If there is an attacker masquerading as a legitimate owner to send Query and a random number $R_{q1}$ to a tag, the attacker will fetch a response from tag: $M = H (TID \oplus R_{q1} \oplus R_{nt1})$, $R_{nt1}$. When the real legitimate owner sends Query and $R_{q1}$, the attacker will send $M = H (TID \oplus R_{q1} \oplus R_{nt1})$ and $R_{nt1}$ to the owner. The owner will find $R_{q1} \neq R_{q1}'$, so the messages achieved by the attacker are invalid. Therefore, the protocol is safe for impersonation attacks.

4) replay attack

After the owner sends Query and $R_{q1}$ to the label, the attacker gets the response from the tag: $M = H (TID \oplus R_{q1} \oplus R_{nt1})$, $R_{nt1}$ and then repeatedly sends the information to owners in order to do replay attack. But the random numbers generated from owners and the tag are different each time, so repeatedly sending the same message cannot be certified. Therefore, the protocol is safe for replay attack.

5) tracking

When an attacker disguised as a legitimate owner sends Query and $R_{q1}$ to the label, it will get the response from tag: $M = H (TID \oplus R_{q1} \oplus R_{nt1})$, $R_{nt1}$ and then track the label by analyzing the response. But in each authentication session, a new random number $R_{nt1}$ will be generated, and Hash function is a one-way operation, so the attacker will not distinguish the response from tags. Therefore, the protocol is safe for tracking.

5. SIMULATION

For the dynamic ownership transfer protocol among multiple owners with different weights 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 and each set of data consist of three parts which respectively are the total share of the secret key, key recovery threshold and the time consumed by the tag to implement the protocol. The result is shown in Figure 4, 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 4. Consuming calculation of RFID tag in the ownership transfer process](image)

As can be seen from the figure, the greater the key threshold value is required, the more time the tag consume to implement the protocol. Besides, 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

In this paper, a kind of dynamic transfer protocol which uses a key management scheme based on Lagrange formulation is proposed between the tag and multiple owners with different weights. When the new entities buy the weights to become the new owners, that is to say, the ownership of the tag has changed, the tag will update the secret key after original owners finishing two-way mutual authentication with the tag by recovering the original secret key of the label based on Lagrange. And then according to the sum of new weights, the new key will be divided into several parts which will be distributed to the new owners according to their weights after the
tag verifying the legitimacy of the new owners. Firstly, forward and backward security of the information about RFID tag can be ensured by updating the secret key. Secondly, because each session will generate a new random number, 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.

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