

Secure group ownership transfer protocol with independence of old owner for RFID tags

Lei He, Yong Gan*, Yifeng Yin

School of Computer and Communication Engineering, Zhengzhou University of Light Industry, Dongfeng Road 5, Zhengzhou, China

Received 1 October 2014, www.cmnt.lv

Abstract

It is important to transfer the ownership of multiple tags efficiently. We proposed a secure group ownership transfer protocol with independence of old owner. It can transfer multiple tags ownership simultaneously. Moreover, the protocol runs regardless of the location of old owner. We analyzed the protocol by using GNY logic. The result indicates that the protocol provides mutual authentication, independence of old owner, forward security and backward security. It resists replay attack, man-in-the-middle attack, desynchronization attack and tracking attack. We implemented and simulated our protocol and other protocols and obtain experimental data. The performance comparison infers that our protocol is efficient and suitable for low-cost tag.

Keywords: RFID, tag, group ownership transfer, independence of old owner, GNY logic

1 Introduction

RFID (Radio Frequency Identification) is an automatic identification technology. It can identify lots of objects in a short time. Now it has been used in many fields, such as access control, tracking of objects, logistics management, etc. A typical RFID system is composed of three components, tag, reader and backend database. A tag is attached to the object which needs to be identified. The owner of the object stores the related information in the tag, such as manufacturer, production date, place of origin, etc. A reader is responsible for communicating with tag and backend database. Generally, it does not modify the messages received. It only forwards the messages to tag or backend database. Hence, reader and backend database are combined in some papers. A backend database stores the information about the tag and the object. It identifies the tag, further, the object, depending on the messages which are received from the tag.

In a RFID system, it is considered that reader and backend database have sufficient computation resource. They can implement some complicated cryptography algorithms. Hence, there are many methods to protect the security of the channel between reader and backend database. Generally, the channel is known as a secure channel. In contrast, tag has too limited computation resource to implement complicated cryptographic algorithms, such as symmetric and asymmetric key encryption algorithms. It is difficult to protect the security of messages which are exchanged by tag and reader. Hence, the channel between tag and reader is considered to be insecure. Now most of protection schemes or protocols use lightweight function, such as XOR, hash function, rotation left, etc., to protect the channel.

The object attached by tag may experience multiple owners in its lifetime. If an entity has access to the tag, we consider the entity has ownership of the tag. When the object is delivered to a new owner, it needs to securely transfer the access to new owner, namely, ownership transfer. Some researchers have proposed some ownership transfer protocols. Nevertheless, most of the protocols focus on single tag ownership transfer. It will transfer ownership one by one if there are many tags which need to transfer their ownership to new owner. The ownership transfer protocol that can transfer multiple tags ownership simultaneously is few. However, there are many scenarios which need to transfer multiple tags ownership. If it transfers the ownership one by one, it will be inefficient. We proposed a secure group ownership transfer protocol which can transfer multiple tags ownership simultaneously. It is more efficient than single tag ownership transfer protocol. It is assumed that there are m tags in a group. The computation time of tag is ts during the ownership transfer procedure. It takes $m*ts$ to transfer the ownership of m tags in single tag ownership transfer protocol at least, while it takes approximately ts in a group ownership transfer protocol. Therefore, it is important to design a secure group ownership transfer protocol.

The rest of the paper is organized as follows. Section 2 describes the ownership transfer model and its security requirements. Section 3 discusses related works. Section 4 presents the proposed protocol. In section 5, we analyze the protocol by using GNY logic. We implement and simulate the protocol and obtain experimental data in the section 6. Section 7 concludes the paper.

* Corresponding author's e-mail: yongg@zzuli.edu.cn

2 Problem statement

2.1 OWNERSHIP TRANSFER MODEL

RFID technology is often used in logistic management. The object will be attached a tag when it is transported. The tag stores the information about itself and the object. If an entity has access to the tag, we consider the entity has the ownership of the tag, namely, it is the owner. During the logistic process, the tag will experience multiple such entities, such as producer, wholesaler, dealer, etc. Every entity has the access to tag within a certain period. It will transfer the access right of tag to another entity when the object is delivered, which is called ownership transfer. The previous entity is old owner (OO), the next entity is new owner (NO). Hence, a tag ownership transfer protocol contains three entities at least, tag, old owner and new owner, where the owner is the integration of corresponding reader and backend database.

The tag ownership depends on the secrets shared by tag and owner. A typical ownership transfer procedure contains the following steps at least.

- 1) Old owner updates the secrets shared with tag.
- 2) Old owner sends the updated secrets to new owner through a secure channel.
- 3) New owner negotiates new secrets with tag depending on the secrets which are received from old owner.

Afterwards, the new owner obtains the ownership of tag. Old owner can't access the tag any more. Note that there is an assumption that the negotiation procedure should be executed beyond the interrogate scope of old owner. Otherwise, old owner can eavesdrop on the messages exchanged by tag and new owner. It is possible for old owner to infer the new secrets negotiated by new owner and tag further because it has the old secrets. However, it is difficult to guarantee the tag beyond the interrogate scope of old owner. The RFID tag ownership transfer model is illustrated as Figure 1.

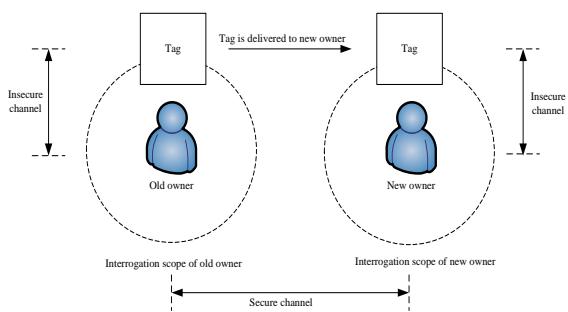


FIGURE 1 RFID tag ownership transfer model.

2.2 SECURITY REQUIREMENTS OF OWNERSHIP TRANSFER PROTOCOL

A tag ownership transfer protocol should meet the following security requirement:

1) Authentication.

It is necessary to execute authentication (AU) when tag communicates with owner. Owner verifies the tag to ensure the tag isn't counterfeited. If the tag also verifies the owner, it is two-way authentication or mutual authentication. Otherwise, it is one-way authentication. Most of services provided by owner are based on authentication. Hence, the authentication procedure is essential.

2) Resistance to some attacks.

There are some attacks in the RFID system, such as replay attack (RA), man-in-the-middle attack (MITMA), de-synchronization attack (DA) and tracking attack (TA). Replay attack and man-in-the-middle attack are two kinds of attack which widely exist in wire and wireless communication. The former means an adversary replays the messages eavesdropped to achieve certain goals, for example, counterfeiting another tag. The latter refers an adversary which locates in the middle of tag and owner communicates with tag and makes the tag believe that it is the owner and vice versa. De-synchronization attack is a specific attack in the RFID system. It refers that the secrets stored in the tag are updated, while the secrets stored in the owner aren't updated and vice versa. If a communication procedure suffers de-synchronization attack, owner won't be able to verify the tag any more. The tag can't authenticate the owner, too. Such attack is implemented by interference with the communication between tag and owner. Hence, it is also considered a kind of denial of service attack. Tracking attack is also a specific attack of RFID system. It is possible for an adversary to track the tag, further, the object attached by tag, by interrogating tag and checking the messages received. It can achieve the goal without authenticating the tag.

3) Forward security and backward security.

Forward security (FS) and backward security (BS) are two important security properties of ownership transfer protocol in the RFID system. Old owner and tag should update the secrets in a unidirectional manner before old owner sends them to new owner. New owner can't infer the previous secrets shared by old owner and tag even if it obtains the secrets sent by old owner, which provides forward security. New owner and tag also update the secrets. Old owner can't obtain the new secrets shared by new owner and tag, which provides backward security.

4) Independence of old owner.

In most of ownership transfer protocols, it is assumed that new owner and tag update the secrets beyond the interrogation scope of old owner. The assumption is important. If the new owner and tag update the secrets in the interrogation scope of old owner, the old owner will eavesdrop on the messages exchanged by new owner and tag. It can obtain the new secrets shared by new owner and tag because it has the current secrets shared by new owner and tag, which are used by new owner and tag to negotiate the new secrets. In this paper, we propose a new security property, that is, independence of old owner (IOO). It means that new owner and tag can negotiate new secrets

securely regardless of the location of old owner. Even if old owner eavesdrops on the messages exchanged by new owner and tag, it can't infer the new secrets.

3 Related works

Now most of ownership transfer protocols are for single tag. The protocol which can transfer multiple tags ownership is few. We introduce some ownership transfer protocols in this section.

The ownership transfer protocols proposed by Saito et al [1] are one of the early research results. They proposed an owner change scheme on three party models and an owner change scheme on two party models. The former contains TTP (Trusted third party), while the latter doesn't contain TTP. The protocol with TTP doesn't resist desynchronization attack. The protocol without TTP is vulnerable to be intercepted which reveals the keys shared by owners and tag. Hence, we consider the protocol has weakness in its security.

Fouladgar and Afifi proposed two ownership transfer protocols [2]. One is based on Hash function and requires old owner and new owner believe the same online database, the other is based on symmetric key encryption algorithm and doesn't need trusted database.

Dimitriou proposed a tag ownership transfer protocol[3]. It mainly uses a pseudo-random function with key to protect the messages exchanged by tag and owner. Owner and tag will update the key when they implement authentication successfully. It is necessary for old owner and new owner to update the key to protect forward security and backward security.

Kulseng et al proposed two ownership transfer protocols [4]. The first protocol assumes that tag and owners believe the same TTP. Tag and TTP share a secret PIN in the protocol. Both of them update PIN at the end of the protocol, but it doesn't explain how to resist desynchronization attack. The second protocol doesn't involve TTP. It is vulnerable to tracking attack.

Zhou et al proposed an ownership transfer scheme in supply chains [5]. Besides tag, old owner, new owner and TTP, it contains a new entity, the third party logistics. It is possible for the protocol to suffer de-synchronization attack.

Song and Mitchell proposed a scalable security scheme which contains a tag ownership transfer protocol [6]. If the protocol completes successfully, new owner and tag will share new secrets. Moreover, old owner can't identify the tag any longer. The ownership transfer protocol needs to be executed beyond the interrogation of old owner.

Fernandez-Mir et al proposed a scalable authentication protocol supporting ownership transfer [7]. Tag is assigned two keys, ik and uk. The former is identification key, which is used to verify identification. The latter is update key. The protocol is mainly divided into synchronized identification phase, update phase, desynchronized identification phase, and controlled delegation phase and owner transfer phase. The desynchronized identification

phase can be executed continuously MAX times. If it is executed consecutively more than MAX times, the database won't verify the tag any more.

Kapoor and Piramuthu proposed two ownership transfer protocols [8]. One needs TTP, the other doesn't need. Both of them use symmetric key encryption algorithm to protect the messages exchanged among tag and owners. Hence, tag has a large amount of computation.

4 Protocol descriptions

It is necessary to design a group ownership transfer protocol to transfer the ownership of a group of objects simultaneously. Now the related research result is few. In this paper, we propose a secure group ownership transfer protocol with independence of old owner. It is assumed that the channels between tag and owners, including old owner and new owner, are insecure, while other channels are secure for the convenience of research. There are m tags in a group. The notations in Table 1 are used in the paper.

A tag and owner store not only the key and group key, but also the key and group key last used. The tag stores secret and group secret shared with TTP. The owner stores a status bit which infers whether the tag is ready for transfer ownership, etc. The key and secret are unique among the tags in the group. The group key and group secret of all tags in the group are same. Our protocol transfers the ownership of m tags to new owner simultaneously. The protocol is illustrated as Figure 2.

TABLE 1 Notation

Notations	Meaning
a, b	concatenation of message a and b
r_i	i -th random number
ID _{OO}	the identification of old owner
ID _{NO}	the identification of new owner
k_{i-p}	p -th key of i -th tag in the group
GK_q	q -th group key
GS	the group secret shared by a group of tags and TTP
s_{q-i}	the secret shared by i -th tag in the q -th group and TTP
H(a)	one way hash function of message a
GOTROO	a flag, which is short for group ownership transfer request with independence of old owner
GOTAIOO	a flag, which is short for group ownership transfer allowance with independence of old owner
RGOTROO	a flag, which is short for Re-GOTROO
GOTAC	a flag, which is short for group ownership transfer allowance completion
GOTCTTP	a flag, which is short for group ownership transfer command from TTP
GOTA	a flag, which is short for group ownership transfer accomplish
RGOTCTTP	a flag, which is short for Re-GOTCTTP

- A8: $T| \equiv \# GK_2$
A9: $TTP \in (GK_2, k_{i-2}, GK_3, k_{i-3}, GS, s_{q-i})$
A10: $TTP| \equiv T \xleftarrow{GS, s_{q-i}} TTP$
A11: $TTP| \equiv \# k_{i-3}$

5.3 REASONING PROCEDURE

- G1: $T| \equiv OO \sim GOTRIOO (M1, A1, A2, A3, I3, I7)$
G2: $T| \equiv OO \in GK_1 (M1, A1, A2, A3, I3, I6)$
G3: $OO| \equiv T \sim GOTAIOO (M2, A4, A5, A6, I3, I7)$
G4: $OO| \equiv T \in (k_{i-1}, k_{i-2}, GK_2) (M2, A4, A5, A6, I3, I6)$
G5: $T| \equiv TTP \sim GOTCTTP (M5, A1, A7, A8, I3, I7)$
G6: $T| \equiv TTP \in (GK_2, GS) (M5, A1, A7, A8, I3, I6)$
G7: $TTP| \equiv T \sim GOTA (M6, A9, A10, A11, I3, I7)$
G8: $TTP| \equiv T \in (GK_2, k_{i-2}, GK_3, k_{i-3}, GS, s_{q-i}) (M6, A9, A10, A11, I3, I6)$

From the analysis and reasoning procedure, it demonstrates that our protocol provides mutual authentication of tag with old owner and TTP. Tag believes that old owner wants to transfer the ownership to new owner. Old owner confirms that all tags have updated the key and group key. The update is irreversible, that is, an adversary can't infer the key and group key from the key and group key updated. Tag believes that old owner and TTP have approved the ownership because it receives the flag GOTCTTP which comes from TTP. TTP believes that all tags in the group have accomplished the ownership transfer. It confirms that the tags have updated the key and group key. Moreover, the update also is irreversible. Afterwards, TTP sends the keys and group key of tags in the group to new owner. New owner communicates with tags by using the keys and group key. Now new owner obtains the ownership of the group of tags, while old owner doesn't obtain the ownership any longer.

We find that our protocol can resist replay attack and man-in-the-middle attack according to the reasoning procedure. If it suffers de-synchronization attack, the tag and owner can resynchronize the key or group key because they store them last successfully used. Therefore, the protocol can resist de-synchronization attack. In addition, owner first demonstrates its identity to tag. The tag will communicate with the owner when it believes the owner is authentic. Moreover, the response of tag contains random number which protects the freshness of the message. An adversary can't track the tag by eavesdrop on the messages or counterfeit a valid owner.

In our protocol, old owner and tags update the confidential information in a unidirectional manner. New

owner or an adversary can't infer the initial confidential information shared by old owner and tags even if it obtains the confidential information updated or eavesdrops on the messages exchanged between old owner and tags. Hence, this protocol provides forward security. TTP and tags share a secret and group secret which aren't known by anyone else. The secret and group secret are used to protect the messages exchanged by TTP and tags and update the keys and group key. Old owner can't infer the keys and group key. Therefore, this protocol provides backward security.

Moreover, there is a new security property in the protocol. Even if old owner eavesdrops on the messages exchanged by tags and TTP, it wouldn't infer the keys and group keys because it doesn't obtain the secrets and group secret which are shared by tags and TTP. This protocol doesn't need the assumption which requires the tag is beyond the interrogation scope of old owner. Hence, our protocol provides the independence of old owner.

Table 2 summarizes the privacy and security of our protocol and compares it with the protocols introduced in Section 3. The symbol, “√”, means the security requirement is met or the protocol resists such an attack, while the symbol, “×”, is just the opposite. The symbol, “○”, means the security requirement is partially met.

6 Protocol implementing and simulation

Our protocol can execute ownership transfer of multiple tags simultaneously, while the ownership transfer protocol for single tag transfers ownership of multiple tags one by one. Hence, one of the important features of our protocol is the high efficiency. We implemented and simulated our protocol and some related protocols to obtain experimental data (Figure 3). We focus on the computation time cost by tag because we consider owners have sufficient computation resource. From the result we find that the time cost by tag of our protocol is less than some other protocols. Note that the time of our protocol is cost to transfer ownership of m tags simultaneously. It is less than the time of transfer ownership of one tag in some protocols. That is, its cost time of m tags ownership transfer is less than one tag ownership transfer. The time cost by m tags to transfer ownership approximately takes $1/m$ time of some other protocols cost. Therefore, this protocol is much more efficient than single tag ownership transfer protocol.

TABLE 2 Comparison with other protocols

	AU	RA	MITMA	DA	TA	FS	BS	IOO
[1] with TTP	√	√	√	×	√	√	√	√
[1] without TTP	×	√	×	×	×	√	√	×
[2] based on Hash	√	√	√	√	√	√	√	×
[2] based on symmetric key algorithm	√	√	√	√	√	√	√	×
[3]	√	√	√	√	√	√	√	×
[4] with TTP	√	√	√	×	√	√	√	√
[4] without TTP	√	√	√	√	×	√	√	×
[5]	√	√	√	×	√	√	√	√

[6]	✓	✓	✓	✓	✓	✓	✓	✗
[7]	✓	✓	✓	○	✓	✓	✓	✗
[8] with TTP	✓	✓	✓	✓	✓	✓	✓	✓
[8] without TTP	✓	✓	✓	✓	✓	✓	✓	✗
Our protocol	✓	✓	✓	✓	✓	✓	✓	✓

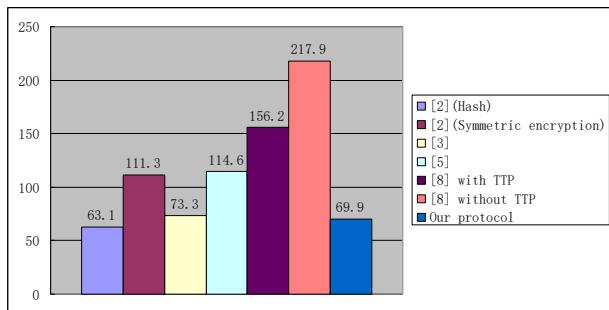


FIGURE 3 Computation time cost by tag(μs)

7 Conclusions

In the paper we propose a secure group ownership transfer protocol with independence of old owner. It can transfer the ownership of a group of tags simultaneously. Another important property of our protocol is the independence of

old owner. It is assumed that the new owner and tag are beyond the interrogation scope of old owner when they negotiate new key in other ownership transfer protocols, while our protocol does not need such assumption in contrast. We analyze the security of our protocol by using GNY logic. The result shows that our protocol has good security. It provides mutual authentication, the independence of old owner, forward security and backward security. It can resist replay attack, man-in-the-middle attack, de-synchronization attack and tracking attack. The result of implementing and simulation shows that our protocol is efficient and suitable for low-cost tag.

Acknowledgments

This paper is sponsored by National Natural Science Foundation of China No. 61340059, 61272038.

References

- [1] Saito J, Imamoto K, Sakurai K 2005 Reassignment scheme of an RFID tag's key for owner transfer *Embedded and Ubiquitous Computing-EUC 2005 Workshops* (Nagasaki, Japan, 6-9 December) Springer: Berlin 1303-12
- [2] Fouladgar S, Afifi H 2007 *Journal of Communications* 2(6) 6-13
- [3] Dimitriou T 2008 rfidDOT: RFID delegation and ownership transfer made simple *Proceedings of the 4th international conference on Security and privacy in communication networks(Istanbul, Turkey 22-25 September) ACM New York*
- [4] Kulseng L, Yu Z, Wei Y, Guan Y 2010 Lightweight mutual authentication and ownership transfer for RFID systems *INFOCOM (San Diego, Canada, 14-19 March) IEEE: Washington DC* 1-5
- [5] Zhou W, Yoon E J, Piramuthu S 2011 Varying levels of RFID tag ownership in supply chains *On the Move to Meaningful Internet Systems: OTM 2011 Workshops* (Crete, Greece 17-21 October) Springer: Berlin 228-35
- [6] Song B, Mitchell C J 2011 *Computer Communications* 34(4) 556-66
- [7] Fernandez-Mir A, Trujillo-Rasua R, Castella-Roca J, Domingo-Ferrer J 2012 *Lecture Notes in Computer Science* 7055 147-62
- [8] Kapoor G, Piramuthu S 2012 *IEEE Transactions on Systems, Man, and Cybernetics Part C Applications and Reviews* 42(2) 164-73
- [9] Gong L, Needham R, Yahalom R 1990 Reasoning about belief in cryptographic protocols *IEEE Computer Society Symposium on Research in Security and Privacy (Oakland, Canada 7-9 May) IEEE Washington DC* 234-48

Authors

	Lei He, China. Current position, grades: lecturer in School of Computer and Communication Engineering, Zhengzhou University of Light Industry, China. University studies: Master Degree in Cryptography from Southwest Jiaotong University in 2006. Scientific interest: Wireless network security and cryptography. Publications: 20 papers.
	Yong Gan, China. Current position, grades: professor in School of Computer and Communication Engineering, Zhengzhou University of Light Industry. University studies: PhD in Computer Science and Technology from Xi'an Jiaotong University. Scientific interest: computer network and its security. Publications: 30 papers.
	Yifeng Yin, China. Current position, grades: professor in School of Computer and Communication Engineering, Zhengzhou University of Light Industry. University studies: Ph.D. from Xidian University in 2009. Scientific interest: cryptography, information security.