BULGARIAN ACADEMY OF SCIENCES

CYBERNETICS AND INFORMATION TECHNOLOGIES • Volume **14**, No 4

Sofia • 2014

Print ISSN: 1311-9702; Online ISSN: 1314-4081
DOI: 10.1515/cait-2014-0010

RFID Tag Ownership Transfer Protocol with Retrospective Ability

Yong Gan, Lei He, Yi-feng Yin

School of Computer and Communication Engineering, Zhengzhou University of Light Industry, Zhengzhou, 450002, China
Emails: yongg@zzuli.edu.cn heleiresearch@126.com yinyifeng@yeah.net

Abstract: *Tag ownership transfer is an important process for RFID system. Besides the user needs to obtain the information concerning the quality of products in some scenarios, which are attached by tags. In this paper, we proposed an ownership transfer protocol with retrospective ability and analyzed its security level by using GNY logic. The results indicate that the ownership transfer protocol provides high-quality security to RFID systems. It provides an authentication between the tag and owners and location privacy of the tag. The protocol enables to resist a replay attack, man-in-the-middle attack and desynchronization attack. It also protects forward security and backward security. Moreover, it provides the information concerning the quality of the product attached by tags. We analyzed the performance of the protocol and implemented it. 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.*

Keywords: *RFID, ownership transfer, protocol, retrospective ability, GNY logic.*

1. Introduction

RFID is an automatic identification technology, which requires no physical contact. It is considered as the next generation object identification technology. Compared with the bar code, RFID provides services with faster recognition speed, higher identification rate and wider communication range. It is often applied in supply

chain management, healthcare, animal monitoring, etc. Generally, RFID system is composed of three components, namely a tag, a reader and a backend database. The tag is attached to an object and stores the related information about the object. RFID system can automatically identify and track that the tag has attached to object. The reader communicates with the tag and the backend database. It usually forwards the received messages to the tag or the backend database without modification. The backend database stores information about the tags and provides some services, such as query, authentication, authorization, etc.

RFID tag is divided into two categories, a passive tag and an active tag. An active tag provides power by a battery, while a passive tag mainly depends on the electromagnetic induction to generate power. The passive tag has been widespread because it is cheap and easy to use. However, a low-cost passive tag has limited computational capability and memory. In contrast, the active tag has sufficient computational resources.

One of the main issues of RFID technology is how to provide secure communication between the tag and the reader or a backend database. It is necessary to implement the cryptography algorithms to protect the communication. An assumption of the work is that the reader and the backend database have sufficient computational resources. That is, they can implement all kinds of algorithms to provide the security performance. Nevertheless, the low-cost tag cannot implement some complicated cryptography algorithms. It can only implement several lightweight operations, such as hash function, XOR, etc. Hence, it is difficult to ensure the security of the communication with the reader or the backend database for the low-cost tag.

An object which is attached by a tag usually belongs to the owner. The owner not only owns the object, but also shares confidential information with the tag and has the ability to access it. The object and the tag may correspond to multiple owners during the logistics process. The previous owner is the old owner, while the next owner is a new owner. It is necessary to securely transfer ownership among different owners.

In some scenarios, the quality of the object attached by the tag is vital, such as the applications in the fields of food, drug, electronic equipment, etc. Therefore, the tag needs to store quality information about the manufacturer, the producing area, the date of manufacturing, etc. It is important to obtain the information in order to guarantee the products quality for the owner.

We propose a RFID tag ownership transfer protocol with Retrospective Ability (RA). To provide retrospective ability, an encrypted lightweight certificate is added to the protocol. We analyze its security by using GNY logic and compare with other protocols. The result shows that the proposed protocol provides good secure properties. Compared with other protocols, our protocol has less computational time cost by the tag.

This paper is organized as follows. We describe the requirements of ownership transfer protocol in Section 2. Section 3 provides a brief overview of the related work. Section 4 proposes a tag ownership transfer protocol with retrospective ability. Section 5 presents brief security analysis of our protocol by using GNY

logic. In Section 6 we analyze the performance of the protocols. Moreover, we implement and simulate these protocols and carry out an empricial study. The last section concludes the paper.

2. Ownership transfer protocol security requirements

Typically, an ownership transfer protocol contains the following three steps at least.

1) An old owner and a tag update of the secrets shared by them.

2) The old owner or the tag sends the updated secrets to a new owner in a secure way.

3) The new owner and the tag update the secrets.

An ownership transfer protocol must provide conventional secure properties, such as authentication, resistance to a replay attack and a man-in-the-middle attack, etc. More important, it has some distinctive secure properties, which include location privacy, resistance to a desynchronization attack, forward security and backward security.

- AUthentication (AU)

Authentication is an important and essential security requirement for RFID protocol. It can be divided into two categories, one-way authentication and two-way authentication. In the RFID system, the tag and the backend database usually implement two-way authentication. The tag verifies the backend database and vice versa. In some scenarios they implement one-way authentication. That is, the backend database confirms the tag identification.

- Location Privacy (LP)

Location privacy is a critical secure property for RFID systems. A tag is usually attached to the object. An adversary can interrogate the tag and track it by analyzing the messages sent by the tag. Further, the adversary can track the object by tracking the attached tag.

- Resistance to a Replay Attack (RRA)

The replay attack is a common attack method. It is connected with the fact that an adversary reuses the eavesdropped messages in order to be authenticated and obtain authorization. It can be resisted by adding freshness.

- Resistance to a Man-In-The-Middle Attack (RMITMA)

The man-in-the-middle attack is also a common attack method. It refers to the fact that an adversary in the middle of a tag and a backend database impersonates the backend database or the tag to participate in the protocol.

- Resistance to a Desynchronization Attack (RDA)

The desynchronization attack is a special attack method for the protocol of a RFID system. In some protocols the tag and the backend database need to update the shared secrets. However, it is difficult for them to update the secrets simultaneously. An adversary can interference with the communication between the tag and the backend database, which causes desynchronization of the secrets, respectively stored in the tag and the backend database. Afterwards, the tag and the

backend database use different secrets to implement the authentication. It causes authentication failing. The desynchronization attack can be seen as a kind of deny of a service attack.

- Forward Security (FS) and Backward Security (BS)

In a tag ownership transfer protocol, the new owner does not know the secrets shared by the tag and the old owner, while the old owner also does not know the secrets shared by the tag and the new owner. The former is forward security, and the latter is backward security. The new owner and the old owner need to update the secrets shared with the tag in order to provide forward security and backward security.

3. Related works

Much research has been done to protect the security of RFID systems. Tag ownership transfer has received attention in recent years. The researchers have proposed some protocols. The protocols proposed by S a i t o et al. [1] are earlier ownership transfer protocols. They have proposed two ownership transfer protocols. One needs a TTP (Trusted Third Party), the other one does not. The former cannot resist a desynchronization attack, while the latter is vulnerable to be intercepted, which will cause leak of the secrets shared by the owners and a tag.

O s a k a et al. [2] have proposed an efficient ownership transfer protocol. The old owner updates the key shared with the tag. Afterwards, it sends the updated key to a new owner to protect the forward security. The new owner also updates the key to provide backward security. This protocol is vulnerable to tracking an attack and a desynchronization attack. Y o o n and Y o o [3] have proposed an improved protocol. However, this protocol does not resist a tracking attack.

S o n g [4] has proposed a tag ownership transfer scheme. It mainly contains an ownership transfer protocol, a secret update protocol and an authorization recovery protocol. S h a o h u i [5] has analyzed the scheme and considered that it does not provide forward security. The new owner can deduce the secret shared by the tag and the old owner.

K u l s e n g et al. [6] have proposed two ownership transfer protocols. One involves TTP, the other does not involve TTP. In the protocol with TTP, both the TTP and the tag simultaneously update confidential information, namely, PIN. However, it does not describe how to guarantee the synchronization of the update procedure. Hence, it is vulnerable to a desynchronization attack. The protocol without TTP is vulnerable to a tracking attack.

K a r d a s et al. [7] have proposed an efficient authentication protocol supporting the ownership transfer for RFID systems. It contains a registration phase and an authentication phase. Once the tag ownership is required to transfer to the new owner, the tag synchronizes its state with the old owner. It runs at least two successful authentication protocols. Afterwards, the old owner sends the information concerning the tag to the new owner. The new owner obtains the ownership by updating the confidential information.

Z h o w et al. [8] have proposed an ownership transfer protocol in supply chains. There are five entities in the protocol, namely, an old owner, a new owner, a tag, a TTP and a third party logistics. This protocol is vulnerable to a desynchronization attack.

K a p o o r and P i r a m u t h u [9] have proposed two protocols. These two protocols implement symmetric key cryptography to encrypt the confidential information. The new owner obtains the ownership by a negotiating key with tag.

C h e n and C h i e n [10] have proposed an ownership transfer scheme. It contains six parties, a server, a cash register, a mobile reader, a tag, a user and an authorized agent. The scheme is divided into five phases, a registration phase, query and authentication phase, purchase phase, product authentication phase and ownership transfer phase. It does not explain in detail how the tag resists to a desynchronization attack.

4. Protocol description

In some scenarios, the owner needs to retrospect the information ensuring that the product guarantees its quality. Our protocol provides authentication, ownership transfer and product retrospective ability. The old owner authenticates the tag and determines the identification of the tag. Afterwards, it transfers the tag ownership to a new owner and provides the quality information of the tag to the new owner. The notations in Table 1 are used throughout the paper. The protocol is illustrated in Fig. 1.

Table 1. Notations

Notation	Meaning
k	The current key shared by the owner and the tag
k_{new}	The new key shared by the new owner and the tag
k_{OT}	The Ownership Transfer key shared by the owner and the tag
k_{cert}	The key shared by the owner and the tag which is used to encrypt or decrypt product information
ID_{OO}	Old Owner IDentification
ID_{NO}	New Owner IDentification
r_i	i-th random number
a, b	Concatenation of messages a and b
H(a)	One way Hash function of message a
“x”	String “x”
$\oplus$	XOR operation

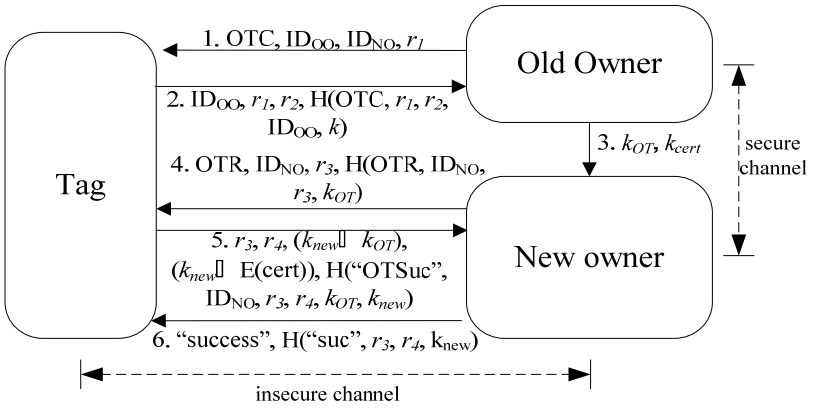

Fig. 1. Ownership transfer protocol

1) The old owner generates a random number r_1 and an ownership transfer command (OTC). It sends {OTC, ID$_{OO}$, ID$_{NO}$, r_1} to the tag.

2) The tag checks the received ID$_{OO}$. If it is not correct, the tag generates a random message and sends it to the old owner. Otherwise, the tag generates a random number r_2 and computes H (OTC, r_1, r_2, ID$_{OO}$, k). It sends {ID$_{OO}$, r_1, r_2, H(OTC, r_1, r_2, ID$_{OO}$, k)} to the old owner. In addition, it computes H ("OT", r_1, r_2, ID$_{OO}$, k) and sets it as k_{OT}.

3) The old owner checks whether the received message is correct through its database. If it is not correct, the protocol is terminated. Otherwise, it authenticates the tag and computes k_{OT} in the same way. The old owner sends k_{OT} and k_{cert} to the new owner in a secure channel. The former is used to transfer the tag ownership from the old owner to the new owner. The latter is used to decrypt the quality information of a product.

4) The new owner generates an ownership transfer request (OTR) and a random number r_3. It sends {OTR, ID$_{NO}$, r_3, H(OTR, ID$_{NO}$, r_3, k_{OT})} to the tag.

5) The tag checks the received ID$_{NO}$ and H (OTR, ID$_{NO}$, r_3, k_{OT}). If one of them is not correct, the tag generates a random message and sends it to the new owner. Otherwise, it generates a random number r_4 and a new key k_{new}. It computes ($k_{new}\oplus k_{OT}$), $k_{new}\oplus$E(cert) and H ("OTSuc", ID$_{NO}$, r_3, r_4, k_{OT}, k_{new}). E (cert) is the encrypted digital certificate information of the product, which is stored in the tag and written by the manufacturer. It can be verified by the new owner through a Public Key Infrastructure (PKI) after being decrypted. It is possible to use a lightweight certificate considering the limited computational resource. The tag sends {r_3, r_4, ($k_{new}\oplus k_{OT}$), ($k_{new}\oplus$E(cert)), H("OTSuc", ID$_{NO}$, r_3, r_4, k_{OT}, k_{new})} to the new owner.

6) The new owner obtains k_{new} and verifies whether the received H ("OTSuc", ID$_{NO}$, r_3, r_4, k_{OT}, k_{new}) is correct. If it is not correct, the protocol is terminated. Otherwise, the tag ownership has been transferred to the new owner. The new owner stores k_{new} and E (cert). It decrypts E (cert) by using k_{cert} and verifies the

certificate to obtain the quality information, such as the manufacturer of the product. The new owner sends {"success", H ("suc", r_3, r_4, k_{new})} to the tag.

7) The tag checks whether the received message is correct. If it is not correct, the protocol is terminated. Otherwise, the procedure of the ownership transfer is completed and $k = k_{new}$ is set.

5. Protocol analysis

GNY logic is a logic method to analyze the security of a protocol, which was proposed by G o n g L i et al. [11]. In this paper, we use GNY logic to briefly analyze our protocol. It contains three phases, a formal description, initial assumptions and a reasoning process. In order to facilitate the analysis, it is assumed that the channels between the tag and the owners are not secure, while the other channel is secure. The expressions and inference rules we used comply with the paper proposed by G o n g et al. [11].

5.1. Formal description of the protocol messages

PM1: $T \lhd * OTC, *ID_{OO}, *ID_{NO}, * r_1$
PM2: $OO \lhd ID_{OO}, r_1, * r_2, H(OTC, r_1, r_2, ID_{OO}, k)$
PM3: $T \lhd *OTR, *ID_{NO}, * r_3, *H(OTR, ID_{NO}, r_3, k_{OT})$
PM4: $NO \lhd r_3, * r_4, *\{k_{new}\}_{k_{OT}}, *\{E(cert)\}_{k_{new}}, *H(\text{"OTSuc"}, ID_{NO}, r_3, r_4, k_{OT}, k_{new})$
PM5: $T \lhd$ "success", $H(\text{"suc"}, r_3, r_4, k_{new})$

5.2. Initial assumptions

A1: $T|\equiv \# r_2$
A2: $T \ni k$
A3: $OO \ni k$
A4: $OO|\equiv \# r_1$
A5: $OO|\equiv OO \overset{k}{\longleftrightarrow} T$
A6: $T \ni k_{OT}$
A7: $T|\equiv NO \overset{k_{OT}}{\longleftrightarrow} T$
A8: $NO \ni k_{OT}$
A9: $NO|\equiv \# r_3$
A10: $NO|\equiv NO \overset{k_{OT}}{\longleftrightarrow} T$
A11: $NO|\equiv NO \overset{k_{new}}{\longleftrightarrow} T$
A12: $T|\equiv \# r_4$

5.3. Security objectives and inference process

PG1: $T|\equiv \# k_{OT}$(PM1, A1, A2, F10)
PG2: $OO|\equiv T \ni k$(PM2, A3, A4, A5, I3, I6)
PG3: $T|\equiv NO \ni k_{OT}$(PM3, A6, PG1, A7, I3, I6)
PG4: $NO \ni k_{new}$(PM4, A8, P6)

PG5: NO ∋ E(cert) (PM4, PG4, P6)
PG6: NO| ≡ T~ k_{new}(PM4, A8, A9, A10, I3, I7)
PG7: NO| ≡ T ∋ (k_{OT}, k_{new})(PM4, A8, A9, A10, I3, I6)
PG8: T| ≡ NO ∋ k_{new}(PM5, A11, A12, I3, I6)

From the analysis procedure we find that the old owner authenticates the tag in our protocol. The old owner generates a new temporary key and sends it to the new owner, which protects the forward security. The new owner and the tag implement mutual authentication and key negotiation. The new key which is negotiated by the new owner and the tag, replaces the temporary key, which protects the backward security. Thus the new owner obtains the tag ownership. Moreover, the new owner obtains a certificate concerning the product stored in the tag to obtain the quality information.

We find that our protocol resists a replay attack and a man-in-the-middle attack from the reasoning procedure. An adversary cannot track the tag by analyzing the eavesdropped messages. The protocol resists a desynchronization attack because the last key is stored. The owner and the tag can use it to resynchronize their states.

We compare the security of our protocol with other protocols, as shown in Table 2. The symbol "√", means that the security requirement is met, while the symbol, "×", indicates that the security requirement is unsatisfied.

Table 2. Security comparison with other protocols

Protocol	AU	LP	RRA	RMITMA	RDA	FS	BS	RA
[1](with TTP)	√	√	√	√	×	√	√	×
[1](without TTP)	×	×	√	×	×	√	√	×
[2]	√	×	√	√	√	√	√	×
[3]	√	×	√	√	√	√	√	×
[4]	√	√	√	√	√	×	√	×
[6](with TTP)	√	√	√	√	×	√	√	×
[6](without TTP)	√	×	√	√	√	√	√	×
[7]	√	√	√	√	√	√	√	×
[8]	√	√	√	√	×	√	√	×
[9](with TTP)	√	√	√	√	√	√	√	×
[9](without TTP)	√	√	√	√	√	√	√	×
[10]	√	√	√	√	×	√	√	×
Our protocol	√	√	√	√	√	√	√	√

6. Performance analysis, implementation and simulation of the protocols

In the RFID system, we consider that the reader and the backend database have sufficient computation, while the low-cost tag has a limited computational resource. Hence, the performance of a tag is important for RFID systems. In this section we study some important performance indicators of the tag, for example, the memory cost, the computational amount and time of sending a message. The performance of our protocol is compared with protocols in [2, 3, 8 and 9] in Table 3. In the table the memory cost shows the memory which is used to store the secrets shared by the tag

and the owners. It is assumed that the length of a secret is *l* bits. The computational amount denotes the amount of computation which is implemented by a tag. HF is a hash function computation. PRF is a pseudo-random function computation. EF is an encryption function computation. The time of sending a message indicates the time of a tag sending a message to the owners.

Table 3. Performance comparison with other protocols

Indikator	[2]	[3]	[8]	[9](with TTP)	[9](without TTP)	our protocol
Memory cost	2	2l	5l	3l	2l	3l
Computational amount	2HF	6HF	1PRF+2EF	2EF+2PRF+2HF	4EF+1PRF+2HF	2PRF+5HF
Times of sending a message	2	1	1	1	2	2

We implement our protocol, as well as the protocols in [3, 8 and 9] to obtain experimental data. The computational time cost by a tag to perform the ownership transfer is an important performance indicator, because the tag has limited computational resource, while the owners have sufficient computational resource. The experimental data is shown in Fig. 2. From the result we find that the cost time of our protocol is shorter than in the others. It is 95.3% of the protocol proposed by Yoon and Yoo, which is the shortest among the other protocols.

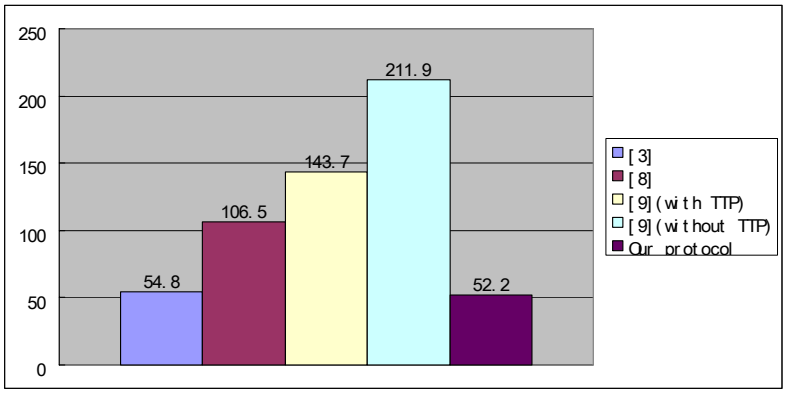

Fig. 2. Computational time cost by a tag (μs)

7. Conclusion

In this paper we propose a tag ownership transfer protocol with retrospective ability and analyze its security by using GNY logic. The result illustrates that the proposed protocol provides authentication between the owners and the tags. It ensures forward security, backward security and user's location privacy. It also resists a replay attack, a man-in-middle attack and a desynchronization attack. The protocol provides a certificate of the product attached by tags to guarantee the product's quality. In order to analyze its performance, empirical study is carried out. The results show that the performance of the protocol is better than the presented in [3, 8, 9]. In future we intend to investigate how to further reduce the computational effort of the tags.

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

References

1. Saito, J., K. Imamoto, K. Sakurai. Reassignment Scheme of An RFID Tag's Key for Owner Transfer. – In: Embedded and Ubiquitous Computing – EUC 2005 Workshops, Berlin, Springer, 2005, 1303-1312.
2. Osaka, K., T. Takagi, K. Yamazaki et al. An Efficient and Secure RFID Security Method with Ownership Transfer. – In: International Conference on Computational Intelligence and Security, IEEE, Washington, DC, 2006, 1090-1095.
3. Yoon, E.-J., K.-Y. Yoo. Two Security Problems of RFID Security Method with Ownership Transfer. – In: IFIP International Conference on Network and Parallel Computing, IEEE, Washington, DC, 2008, 68-73.
4. Song, B. RFID Tag Ownership Transfer. – In: Proceedings of Workshop on RFID Security, 2008.
   http://events.iaik.tugraz.at/RFIDSec08/Papers/Publication/15%20-%20Song%20-%20Owner ship%20Transfer%20-%20Paper.pdf
5. Shaohui, W. Analysis and Design of RFID Tag Ownership Transfer Protocol. – In: Proceedings of the 2011 International Conference on Informatics, Cybernetics, and Computer Engineering, Berlin, Springer, 2012, 229-236.
6. Kulseng, L., Z. Yu, Y. Wei, et al. Lightweight Mutual Authentication and Ownership Transfer for RFID Systems. – In: INFOCOM, 2010 Proceedings IEEE, IEEE, Washington, DC, 2010, 1-5.
7. Kardas, S., A. Arslan, S. Celik, et al. An Efficient and Private RFID Authentication Protocol Supporting Ownership Transfer, 2011.
   http://eprint.iacr.org/2011/667.pdf
8. Zhou, W., E. J. Yoon, S. Piramuthu. Varying Levels of RFID Tag Ownership in Supply Chains. – In: On the Move to Meaningful Internet Systems: OTM 2011 Workshops, Springer Berlin Heidelberg, Berlin, 2011, 228-235.
9. Kapoor, G., S. Piramuthu. Single RFID Tag Ownership Transfer Protocols. – IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews, Vol. **42**, 2012, No 2, 164-173.
10. Chen, C. L., C. F. Chien. An Ownership Transfer Scheme Using Mobile RFIDs. – Wireless Personal Communications, Vol. **68**, 2013, No 3, 1093-1119.
11. Gong, Li, R. Needham, R. Yahalom. Reasoning about Belief in Cryptographic Protocols. – In: 1990 IEEE Computer Society Symposium on Research in Security and Privacy, IEEE, Washington, DC, 1990, 234-248.