International Journal of Networked and Distributed Computing, Vol. 3, No. 2 (April 2015), 128-136

Scenarios for An RFID Tag Ownership Transfer Protocol for A Closed Loop System

Gaith K.D. Al.
E-mail: g.aliyev76@gmail.com

Biplob Rakshit Ray
E-mail: brray@deakin.edu.au

Morshed Chowdhury
E-mail: muc@deakin.edu.au

School of Information Technology, Deakin University,Melbourne Burwood Campus, Australia

Abstract

In RFID system a tag is attached to an object which might own by a number of owners during its life time. This requires the RFID system to transfer ownership of the tag to its new owner. The ownership transfer has to protect privacy of current and new owner. Many ownership tag ownership transfer exists in the literature, however, most of them are impractical or insecure to implement on current passive RFID tags. We are proposing a timer based ownership transfer protocol for closed loop RFID systems. The proposal in this paper includes two implement scenario to cover diverse tags type. The protocol will ensure security and privacy of involved parties in the idle circumstances. Our comparison shows that the proposed protocol is more secure and practical than existing similar ones.

Keywords - Tag ownership transfer, RFID, Tag data confidentiality, transfer scenario

1. Introduction

Radio frequency Identification (RFID) is a data capturing technology which uses radio frequency (RF) to identify tags (also known as transponders). It is attached to an object such as products or animals and communicate wirelessly through reader (also known as scanners). The reader uses database server for further information about the object such as price, expiry date, etc.

The major achievement of RFID technology can be achieved by offering the ability and possibility for a large scale automated data collection wirelessly.

There are three types of tags: active, semi-active and passive. The active tag includes a power source. The semi-active has a battery to store energy but requires to power on by a reader. The reader generates a radio frequency (RF) transmission to power on the passive tags which has no power source of its own. The tags transmission range and bandwidth will depend on many factors such as the type of the tag, tag manufacture and design, etc.

The passive tags are usually low-cost tags, used widely for low value products of our everyday life which requires moderate security. To make the passive tag more economic, it is very important to be able to use the tag more than once which require changing its ownership from one owner to another. The tag ownership transfer is one of the key requirements for global implementation of networked RFID systems.

However many security and privacy threats might occur during the tag ownership transfer such as relay attacks, replay attacks, cloning, spoofing, Denial of Service (DoS), etc. These are serious concern for secure tag ownership transfer. In the recent years many security ownership transfer protocols attempt to deal with these threats which are discussed in details in section II. Hereby we are presenting a multi scenarios ownership transfer protocol based on a timer function in a closed loop system which is practical and secure.

2. Related Work

Many researchers worked on mutual authentication between tags and readers [3] [4]. However, the secure tag ownership transfer concept is newer and received less attention until recently when Osaka et al. [6] proposed a secure ownership protocol based on hash functions. Osaka was followed by other researchers who tried to propose improved version of [6] such as Wang et al.[7] and Jappinen [8]. However, [6, 7, 8] have de-synchronization problem [10].

Also Song et al. [9] have proposed an ownership protocol which is based on tag identifiers using hash chains but it was proven weak against eavesdrop attack made by the previous owner during the transfer.

Chen et al. [11] proposed a three phase's one to one tag ownership transfer but the mutual authentication was proven weak against replay attack. Lin et al [12] also proposed a one to one ownership protocol which is weak at DoS and de-synchronization attacks. Kapoor et al. [10] proposed a multi-tag and multi-owner RFID ownership transfer protocol which uses a TTP (trusted third party) as a middleware this was protocol found to be suffering from DoS attack and de-synchronization attack. An attacker can change the random number in acknowledgement transmission from tag to TTP which will be discarded by TTP as it has incorrect value. This situation can potentially be used to generate a de-synchronization attack for a specific period of time which will lead to DoS attack. Doss, R et al. [4] proposed a secure tag ownership transfer protocol for closed loop system based on The Quadratic Residue property. It is also insecure against impersonation attack and DoS attack [3].

Finally Ray et al. [3] proposed a secure mobile RFID ownership transfer protocol to cover all scenarios based on Diffie-Hellman secret Key exchange, although the protocol solved the windowing problem, however the Diffie- Hellman key exchange protocol itself was subject to weaknesses as suggested by Tang [5]. The Diffie- Hellman key exchange is vulnerable to Man-in-the-middle attack [6] that Ray et al. protocol suggests it would prevent.

3. Our Proposed Protocol Details:

In this section, we detail the proposed protocol. We first detail initial setup which is followed by illustration and discussion of proposed protocol scenarios. For this discussion, we will use symbols detailed in Table 1.

3.1 Our proposed protocol setup (for all scenarios) :

- All tags, readers will have Timing Synchronization Function (TYF) [13] called timer which uses reader ID (RID) as seed. This timer is unique to a specific reader and always synchronized between reader ID and tag. The timer will be a secret changeable value in all transmissions. The change will depend on the owner request and protocol's requirement.
- The scheme will use a keyed hash function$H()$. The tag ID (TID) will be stored as $H_{tr}(TID)$ in tag where 'tr' is the timer. The TID is known to the database server and it will storetr, and $H_{tr}(TID)$for every tag.

Table 1: Symbols and their descriptions

Symbol	Explanations
tr,tr1	The Timer
TR_1,TR_2	Randomized timer
K	Random number
H()	Keyed Hash function
$DB1$	Current owner's database server
$DB2$	New owners' database server
$R1$	Current owner's reader
$R2$	New owner's reader
RID	Reader's ID
TID	Tad ID or serial of the tag
UK	Unknown tag

- There will be a verifier reader which verifies the activities of readers in its list at each end to ensure that unexpected transmission can be identified earlier and to prevent relay attack as well.
- The tag will have two modes, the R (read) mode which is used for reading the tags details and the RW mode (read and write) which is used for ownership transfer. Initially, all tags will be in the R mode. Figure 1 shows a tag with full setup.
- The tr will be checked and synchronized from time to time in tags by current owner's reader.

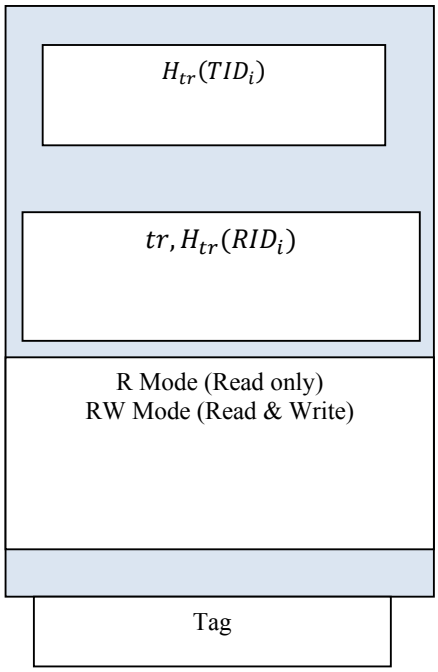

Figure 1: Tags setup and modes

3.2 Our Proposed Scenario 1

This scenario has higher computational cost on tag compare to scenario 2. It requires less backward connection.

I. Mutual Authentication stage:

This stage will start when the tags (which are subject to the ownership transfer) will receive a request to set them up to the RW mode from the current owner reader ($R1$). The $R1$ will send A from equation (1) to the tag. The A is calculated from equation (1) where hashed RID_i is concatenated with TR_1.TR_1 is calculated from equation (2) where tr value is XORed with random number K.

$$A = H_{tr}(RID_i) \parallel TR_1 \quad (1)$$

$$TR_1 = tr \oplus K \quad (2)$$

$$B = H_{tr}(TID_i) \oplus K \quad (3)$$

Once the tag receive the hashed RID_i as well asTR_1, it verifies current reader's ID using its pre-store value. If the verification returns true then the tags will change its mode from R to RW mode.

$$K = TR_1 \oplus tr \quad (4)$$

The tag then retrieves K from equation (4) and reply to current owner reader by sending$B$. The B is calculated in equation (3) where hashed tag ID is XORed with K.

The current owner reader verifies received $H_{tr}(TID_i)$ and K using database server's information. The tag can only reply with correct$K$, if it has synchronized and correcttr. In case of transmission delay or incorrect$K$, the reader discards all transmission. If the reader was unable to verify transmission from tag for second time it will mark the tag UK(unknown tag).

If TID_i and K is valid then current owner's database server ($DB1$) sends B and K to new owner's database server ($DB2$) and request for RID_{i+1}. The $R1$ then writes RID_{i+1} to tag and ends its transmission. The $DB2$ will generate TR_2 in equation (5) where random number$K$ is XORed with new owner's timertr_1.

$$TR_2 = tr_1 \oplus K \quad (5)$$

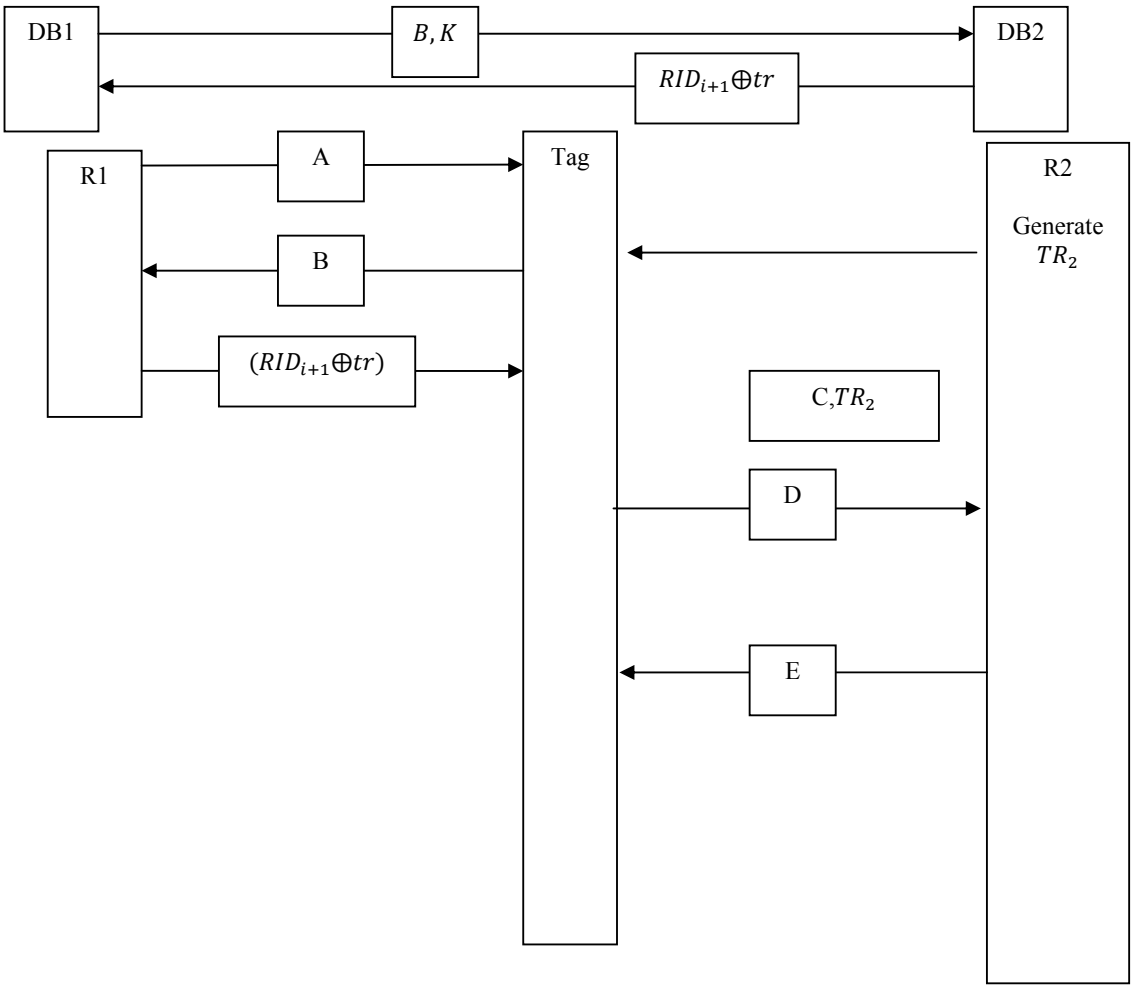

Figure 2: Details of the protocol scenario 1(2 stages).

The new owner's reader $R2$ will send C and TR_2 to the tag. The C is calculated by XORing hashed new owner's RID ($H_{tr}(RID_{i+1})$) and tr_1 in equation (6). The tag will verify correctness of RID_{i+1} using its stored values. If RID_{i+1} send from R2 is valid then the tag sends D to the R2 where D is calculated by XORing hashed TID_i and K as shown in equation (7).

$$C=H_{tr_1}(RID_{i+1}) \oplus tr_1 \quad (6)$$

$$D = H_{tr}(TID_i) \oplus K \quad (7)$$

Here the new owner's reader will compare the correctness of the transmission from the tag by verifying equality of$D == B$. If $B == D$ then the mutual authentication stage will be successfully completed. Otherwise $DB2$ will mark the tag as $UK$and send D back to $DB1$ for further investigation.

II. Ownership transfer stage:

After completing the mutual authentication stage, the new owner will generate new tag ID TID_{i+1}.Then it sends E to the tag and request to execute write operation to change the TID. The E is calculated from equation (8) where hashed TID_{i+1} is XORed with tr_1.

The tag retrieves $H_{tr_1}(TID_{i+1})$ as it knows tr_1 using K value on TR_2.

$$E = H_{tr_1}(TID_{i+1}) \oplus tr_1 \quad (8)$$

It then replaces its old $H_{tr}(TID_i)$ with new $H_{tr_1}(TID_{i+1})$ which ends the ownership transfer. At this point forward only new owner can read the tag usingTID_{i+1}.

3.3 Our Proposed Scenario 2

In this scenario the new owner DB2 starts the ownership transfer protocol when it sends its hashed reader ID (RID_{i+1}) to DB1 through the backend channel.

Once the current owner receives(RID_{i+1}) , the tags (which are subject to the ownership transfer) will receive a request to set them up to the RW mode from the current owner reader $(R1)$. The $R1$ will send A Xored with (RID_{i+1}) to the tag. A is calculated from equation (9) where hashed RID_i is concatenated with TR_1.TR_1 is calculated from equation (10) where tr value is XORed with random number K. (See figure no. 3).

$$A = H_{tr}(RID_i) \parallel TR_1 \quad (9)$$

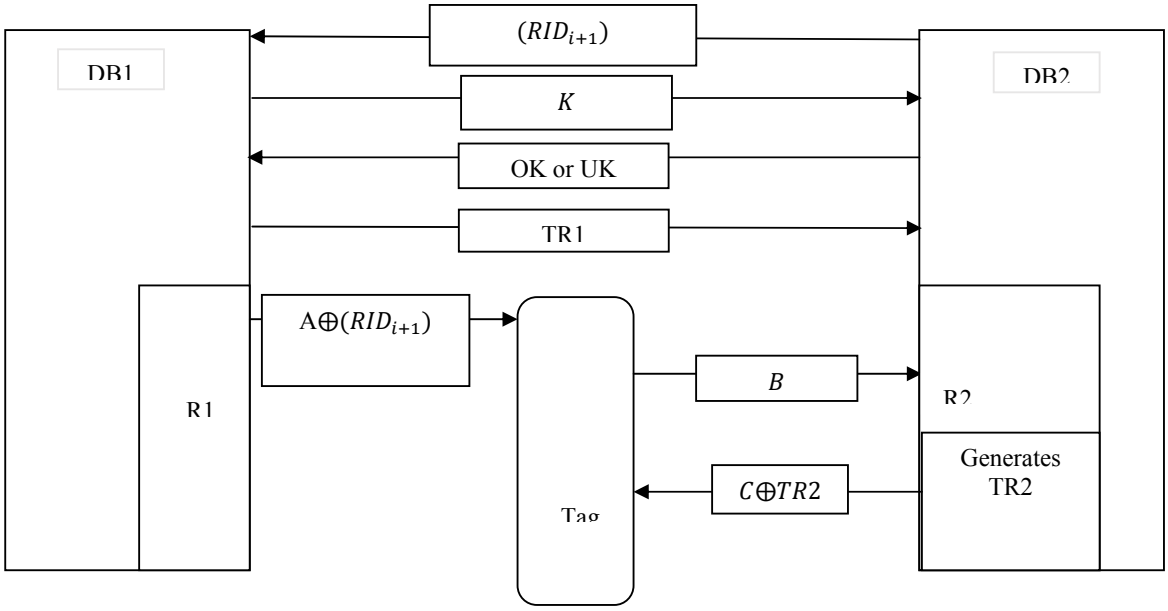

Figure 3: Details of the proposed protocol Scenario 2.

$$TR_1 = tr \oplus K \quad (10)$$

$$B = H_{tr}(TID_i) \oplus K \quad (11)$$

Once the tag receive the hashed RID_i as well as TR_1, it verifies current reader's ID using its pre-store value. If the verification returns true then the tags will change its mode from R to RW mode.

$$K = TR_1 \oplus tr \quad (12)$$

The tag then retrieves K from equation (12), and forward to the new owner reader (RID_{i+1}) by sending B. B Is calculated in equation (11) where hashed tag ID is XORed with K.

R1 will sends K to R2 via DB2 through the back end channel, here R2 will verify K received from both B and DB1 if they were Identical R2 will send Confirmation and request TR1 from DB1 In case of transmission delay or incorrect K, the reader discards all transmission. If the reader was unable to verify transmission from tag for second time it will mark the tag UK(unknown tag).

Once DB1 receives confirmation (OK) from R2 through DB2, DB1 will send TR1 to R2 through back end channel.

The $DB2$ will generate TR_2 in equation (13) where random number K is XORed with new owner's timer tr_1.

$$TR_2 = tr_1 \oplus K \quad (13)$$

The new owner's reader $R2$ will generate new tag ID TID_{i+1}.Then it sends C Xored with TR2 to the tag and request to execute write operation to change the TID. The C is calculated from equation (14). Where hashed TID_{i+1} is XORed with tr_1. The tag retrieves $H_{tr_1}(TID_{i+1})$ as it knows tr_1 using K value on TR_2.

$$C = H_{tr_1}(TID_{i+1}) \oplus tr_1 \quad (14)$$

It then replaces its old $H_{tr}(TID_i)$ with new $H_{tr_1}(TID_{i+1})$ which ends the ownership transfer. At this point forward only new owner can read the tag using TID_{i+1}.Then the tag will change its mode back to read only (R) after the last transmission.

4. Security Analysis

In both scenarios above we notice that the protocol is simple but effective at the same time, since the secret key Timer (tr) changes all the time it will be very hard to trace the TID by any malicious reader. The captured information by eavesdroppers will be useless also because of randomness and changing nature of tr. The protocol will provide the following security measures:

- ***Tag ID anonymity:*** The tag ID is hashed and encrypted with keyed hash $H_{tr}(TID_i)$, it won't be possible to detect or compromising the tag. Also the tag will not reveal transmitted data since the communication between the tag and readers will have random values as we can see in both scenarios of the protocol (see figure 2 and 3). In Table 2 we represent our proposed two protocol scenarios and their defense against the attacks shown compared to the other protocols.
- ***Forward security:*** For scenario 1 as shown above in equation (8) if the tag has been compromised and its current ID has been obtained this will not allow the attacker to trace any previous communication since the value E XORed the hashed $H_{tr_1}(TID_{i+1})$ with tr1 and stored this value in the tag. The same thing can be said for Scenario 2 , see formula (14).
- ***Forward Untractability:*** In both scenarios the old owner cannot compromise the new secret key or the new TR since the new owner will generate a new secret key TR2 by XORing the tr1 with the K as shown in equation (5) and equation (13) in scenario 1

and scenario 2 .So the old owner won't be able to retrieve $tr1$which will be the secret key for the tag.

- ***Relay, replay attacks, Man in the middle and eavesdropping attacks:*** In scenario 1 above, the attacker will be unable to impersonate a new owner by recording and replaying messages from previous rounds. Even if the attacker was recording and replaying messages from previous rounds, the attacker will be unable to establish a communication with the tag as the timer changes in every read which leads to change the value of A as shown in equation (1) and (2).The Same way we can prove that the values of A, B, C, D and E won't be as same for the second round.While in scenario 2 we can see that the Value of A also depends on the timer as shown in equations (9) and (10) while the other values are also changeable for the next round as they all depend on the timer function. So recording and replaying previous rounds won't be successful. This will leads us to the conclusion that our proposed protocol will reduce the eavesdropping attacks to the minimum. Also the reader ID's will always be hashed during transmission and concatenated with $TR1$ as shown in equation (1) and equation (9) or XORed with tr and $tr1$ as showen in equation (6) for the first scenario. which will prevent the MIMT (man-in-the-middle) attack from retrieving the reader ID's to talk to the tag.
- ***DoS attacks:*** For both scenarios the tags are in their R mode all the time which makes them ignores any attempt to write on them and will respond only to the transmission from the trusted readers (R1). So it won't be possible to overwhelm the tags with messages as they will ignore them all as long as they did not came from the trusted readers. Also blocking the messages won't affect the system as the trinstalled individually at every tag, reader and DB that makes them run independently and ignore any messages with incorrect value.

Table 2: Comparison between proposed and a number of existing protocols

Security concerns and threats compared to the protocols	Tag ID anonymity	Forward security	Forward untractability	Relay & replay attacks	Dos attack	Imprisonment attack
Our proposed protocol Scenario 1	Yes	Yes	Yes	Yes	Yes	Yes
Our proposed protocol Scenario 2	Yes	Yes	Yes	Yes	Yes	Yes
Osaka et al.[6]	Yes	No	Yes	Yes	No	Yes
Dimitriou	Yes	Yes	No	Yes	No	No
Song and Mitchell[9]	Yes	Yes	No	Yes	No	Partially secure
Kapoor and	Yes	No	No	Yes	No	Yes

Piramuthu(with TTP)[10]						
Kapoor andPiramuthu (with TTP)[10]	Yes	No	No	Yes	Yes	Yes
Dos and Wanlei[4]	Yes	Yes	Yes	Yes	No	No
Ray et al.[3]	Yes	Yes	Yes	No	Yes	Yes

5. Conclusion

We have presented two new scenarios protocol with an independent changeable timer installed on all three components of the RFID system that works as a changeable secret key. The proposed protocol is immune against many major security threats and attacks as shown in the security analysis. These two new protocol scenarios used for tag ownership transfer in a closed loop system might light the way for further studies and development.

References:

[1] Pateriya& Sharma, (2011), "the Evolution of RFID Security and Privacy: A Research Survey", International Conference on Communication and Network Technologies.

[2] Syamsuddin, Han and Dillon,(2012), "A Survey on Low- cost RFID Authentication Protocols", ICACSIS.

[3] Ray, BR, Chowdhury, M & Abawajy, J 2012, 'Secure mobile RFID ownership transfer protocol to cover all transfer scenarios', in Computing and Convergence Technology (ICCCT), 2012 7th International Conference on, pp. 1185-92.

[4] Doss,R&Wanlei, Z (2012),"A secure tag ownership transfer scheme in a closed loop RFID system", in Wireless Communications and Networking Conference Workshops (WCNCW), IEEE.

[5] Qiang Tang & Chen, (2005), "Weaknesses in two groupsDiffie-Hellman Key exchange protocols".

[6] K.Osaka, T. Takagi, K. Yamazaki, and O.Takahashi, "An Efficient and secure RFID Security Method with Ownership Transfer", in 2006 International Conference on Computational Intelligence and Security. Ieee, Nov.2006, pp. 1090-1095.

[7] C.-H. Wang and S. Chin, "A new RFID authentication protocol with ownership transfer in an insecure communication environment", in proc. Of 9th International Conference on Hybrid Intelligent Systems, 2009.

[8] P.Japinnen and H. Hamalainen, "Enhanced RFID security method with ownership transfer", in proc. Of International Conference on computational Intelligence and Security, 2008.

[9] B.Song and C.J. Mitchell, "Scalable RFID security protocols supporting tag ownership transfer", Computer Communications, vol.34,no.4, pp.556-566, Apr.2011.

[10] G.Kapoor and S.Piramuthu, "Vulnerabilities in some recently proposed RFID ownership transfer protocols", IEEE Communications Letters, vol. 14, no.3, pp.260-262, Mar.2010.

[11] H.Chen, W.Lee, Y. Zhao, and Y.Chen, "Enhancement of the RFID Security Method with Ownership Transfer", in ICUIMC, 2009.

[12] I.C.Lin, C.W. Yang, S.-C. Tsaur(2010), Non-identifiable RFID Privacy protection with ownership transfer, International Journal of Innovative Computing, Information, and Control.

[13] D. Zhou and T.H. Lai, "A Compatible and Scalable Clock Synchronization Protocol in IEEE 802.11 ad Hoc Networks, "in the Proceedings of the 2005 International Conference on Parallel Processing.