Cryptanalysis of Li-Wang Authentication Protocol for Secure and Efficient in RFID Communication

Chia-Hui Wei[1,2], Cheng-Ying Yang[3], Min-Shiang Hwang[4,*], Augustin Yeh-hao Chin[2]

[1]National Central Library, Taiwan
[2]Department of Computer Science, National Tsing Hua University, Taiwan
[3]Department of Computer Science, University of Taipei, Taiwan
[4]Department of Computer Science and Information Engineering, Asia University, Taiwan
500, Lioufeng Rd., Wufeng, Taichung 41354, Taiwan
[4]Department of Medical Research, China Medical University Hospital, China Medical University

[*]E-mail: mshwang@asia.edu.tw

Abstract. Recently, Li, Wang, *et al.* proposed a secure and efficient authentication protocol which enhances scalability function by using simple index. This study further demonstrates that their scheme could not resist denial of service attack.

Keywords: RFID, Privacy, Security, Scalability

1 Introduction

RFIDs are widely applied in various environments, i.e., internet of things (IOT) [1-4], near-field communication (NFC) [4-7], and vehicular ad hoc networks (VANET) [8-11]. In general, there are three parts in RFID systems: Tags, readers, and a database server [12]. The tags contain a limited processing unit and memory [13-15]. The main issues in RFID are the privacy and security [16]. The following five criteria for evaluation security are requirement for RFID communications: Tag information privacy disclosure, location privacy, replayed attack, denial of service, and forward security [17-19].

Many schemes had been proposed to improve the security for RFID systems [20-27]. Some schemes emphasize light weight and low cost RFID Protocols [20-23]. Some schemes are used in mobile agent device [24,25].

Recently, Li, Wang, *et al.* proposed an authentication protocol for secure and efficient RFID communication [26]. Their scheme is designed to solve the scalability problem which the reader is required to identify multiple tags simultaneously. In Li *et al.*'s protocol, the server only computes three times hash function in authentication processes. However, Li *et al.*'s protocol is vulnerable to denial of service (DoS) attack. In this article, we will point out the weakness of their protocol.

The rest of this article is organized as follows: we will review Li *et al.*'s authentication protocol in Section 2. Next, we will show the weakness of Li *et al.*'s authentication protocol in Section 3. Concluding remarks are finally made in Section 4.

2 Review of Li *et al.*'s Authentication Protocol

This protocol is based on hash function, and the following notations used throughout the paper are presented in Table 1. The protocol assumed that the connection between the servers as one entity and shares a secure channel, and the connection between the tag and the reader share an insecure channel, therefore an attacker could easily eavesdrop the transferred information.

Table 1 Notations are used in the protocol

$\oplus$	An exclusive-or operator
$\|\|$	A concatenation operation
h(),G()	A one-way hash function
K	A secret value shared by the database server and the tag
ID	A unique identifier of tag
M	The times which the tag had not updated ID and K
ID_{old}	A previous unique identifier of the tag
ID_{new}	A new unique identifier of the tag
K_{old}	A previous secret value
K_{new}	A new secret value
N_T	A random number generated by tag
N_R	A random number generated by reader

The reader has a pseudo-random number generator while the tag can generate random numbers and compute hash function. The authentication process is divided in five steps shown in Figure 1.

1) The reader sends a random number N_R and Query to the tag.
2) The reader generates N_T and computes $M_1 = h(K||N_R)$ and $M_2 = h(ID)$, and then sends M_1, M_2, and N_T to the reader.
3) After the reader received M_1, M_2, and N_T from the tag, the reader forwards M_1, M_2, N_T, and N_R to the server.
4) The server checks whether h(ID) is matched with $h(ID_{old})$ or $h(ID_{new})$. The server resets M = 0, computes $h(K_{new}||N_T)$, and updates database records $h(ID_{old}) = h(ID_{new})$, ID = G(ID), $h(ID_{new}) = h(ID)$, $K_{old} = K_{new}$, and $K_{new} = ID \oplus N_T \oplus N_R$ if $h(ID_{new})$ equal h(ID). Then, the server computes M = M+1, $h(K_{old} || N_T)$, and still uses the ID_{old} since the server does not update database records if $h(ID_{old})$ equal h(ID) and M < *UpperLimit*. Here, *UpperLimit* denotes a security level which is set by system administrator. When *UpperLimit* is a small value the system has high level security, and *UpperLimit* is a high value the system has low level security. Next, the server sends $h(K_{old} || N_T)$ or $h(K_{new} || N_T)$ to the reader.

5) The reader forwards $h(K_{old} \| N_T)$ or $h(K_{new} \| N_T)$ to the tag that is decided by $h(ID_{old}) = h(ID)$ or $h(ID_{new}) = h(ID)$. The tag computes $h(K \| N_T)$ and compares it with the received value from the reader. Next, the tag updates $ID = G(ID)$, $K = ID \oplus NT \oplus NR$ if $h(K \| N_T)$ is equal with the received value.

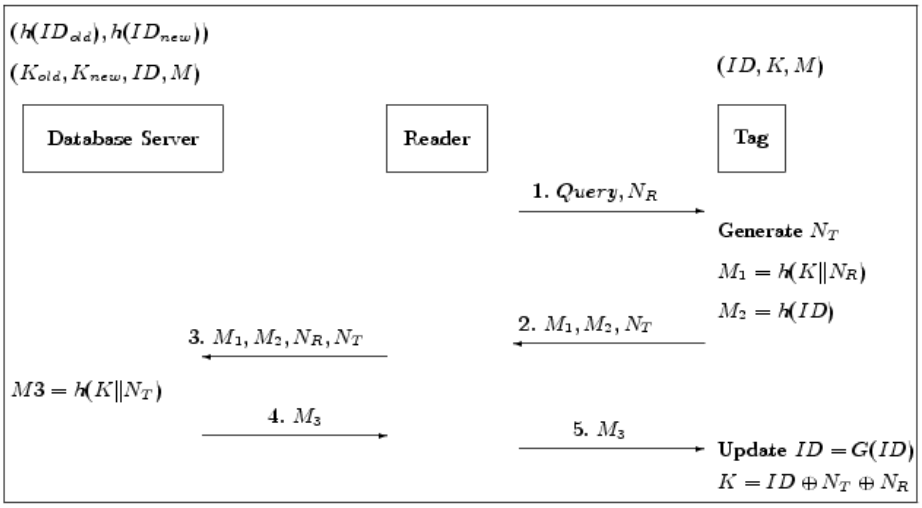

Fig.1 Li-Wang authentication protocol

3 Weakness of Li *et al.*'s Authentication Protocol

In [26], the security analysis indicates that the Li *et al.*'s authentication protocol is secure against denial of service (DoS) under certain conditions. For the DoS attack, Li *et al.*'s authentication protocol claims that their protocol can regain synchronization after losing it. More precisely, an attacker can counterfeit M_3 thus the M_3 of tag is updated while the M_3 of server is not, thus resulting in the de-synchronization between the database server and the tag. The prerequisites are given that an attacker must be able to eavesdrop and intercept message on the communication between the tag and the reader. The two rounds of attack steps are shown in Figure 2.

1) In the first round, the reader and the tag are communicating normally while the attacker intercepts the message that is explained in the following. The reader generates a random number N_R and then sends Query and N_R to the tag.
2) After receiving the message, the tag generates a random number N_T and computes $M_1 = h(S \oplus N_R \oplus N_T)$ and then sends it to the reader. The attacker eavesdrops and records the message N_T while interrupting the message when the tag attempts to send the message (M_1, M_2, N_T) to the reader.
3) In the second round, an attacker obtains the message and then forges a reader to send the message to the tag to update secret value of tag but not the database server. The attacker sends message to the tag Query, N'_T, which is obtained from the first round. After the tag received the messages, the tag computes $M'_1 = h(K \| N'_T)$ and $M_2 = h(ID)$ and then sends it to the reader.

4) After the attacker intercepted the message M'_T, the attacker interrupts the message, and the message M'_1, M_2 are not sent to the database server. The attacker submits the obtained message M'_1 to the tag, and then the tag computes $h(K||N'_T)$ and check whether it is equal with the received M'_1 or not. The tag updates ID and K if the M'_1 is correct. The attacker repeats the first and the second round again, which would result in the de-synchronization of the values ID and K of database server and the tag.

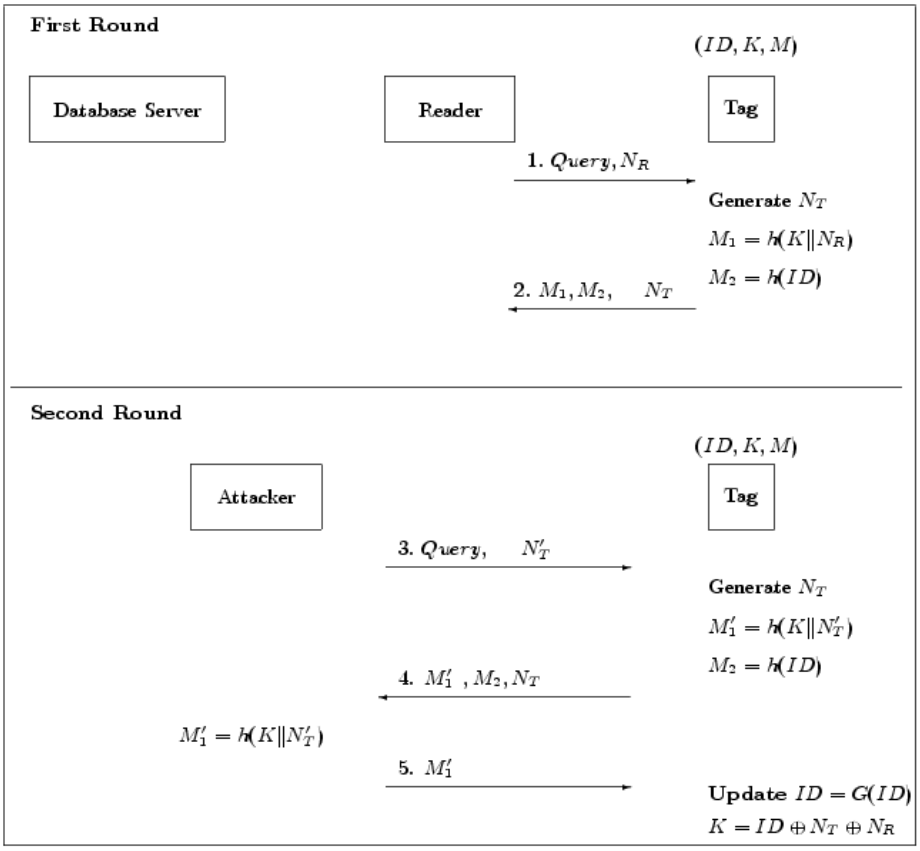

Fig.2 Weakness of Li *et al.*'s authentication protocol

In Li *et al.*'s authentication protocol, the critical point is at the final step $M_3 = h(K||N'_T)$ because the tag is updated with ID and K if M_3 is correct. However, M_3 uses K and N_T while N_T is public, thus N_T can be eavesdropped and resubmitted to the tag. The tag does not record the value is generated last time by N_T itself. Therefore, the tag computes the message $h(K||N_T)$ when an attacker sends the last value N_T, which is equal with final step M3, to the tag. Later, the attacker could successfully send counterfeit message $h(K||N_T)$ to the tag. Therefore, the secure value K and ID of tag are updated, but the database server does not. This attack needs to be executed twice, so

the database has no matching keys to complete the mutual authentication in next session that incurs DoS attacks.

4 Conclusions

In this paper, we reviewed Li *et al.*'s authentication protocol. Next, we showed the vulnerability of Li *et al.*'s authentication in DoS attack. In summary, the attackers typically focus on determining a tag's secret, or replaying message observed from previous communications between the tag and the reader.

5 Acknowledgments

This research was partially supported by the Ministry of Science and Technology, Taiwan, R.O.C., under contract no.: MOST 106-2221-E-468-002, MOST 106-3114-E-005-001, and MOST 106-2221-E-845-001.

6 References

1. Xu, D., Wu, Z., *et al.*: Internet of things: Hotspot-based discovery service architecture with security mechanism. International Journal of Network Security, 17(2), 208-216 (2015)
2. Liu, L., Cao, Z., Markowitch, O.: A note on design flaws in one aggregated-proof based hierarchical authentication scheme for the internet of things. International Journal of Electronics and Information Engineer, 5(2), 88-92 (2016)
3. Mayzaud, A., Badonnel, R., Chrisment, I.: A taxonomy of attacks in RPL-based internet of things. International Journal of Network Security, 18(3), 459-473 (2016)
4. Ling, J., Wang, Y., Chen, W.: An improved privacy protection security protocol based on NFC. International Journal of Network Security, 19(1), 39-46 (2017)
5. Feng, T.H., Hwang, M.S., Syu, L.W.: An authentication protocol for lightweight NFC mobile sensors payment. Informatica, 27(4), 723-732 (2016)
6. Ma, Y.: NFC communications-based mutual authentication scheme for the internet of things. International Journal of Network Security, 19(4), 631-638 (2017)
7. Chi, Y.L., Chen, C.H., Lin, I.C., Hwang, M.S.: The secure transaction protocol in NFC card emulation mode. International Journal of Network Security, 17(4), 431-438 (2015)
8. Zhao, H., Sun, D., Yue, H., *et al.*: Dynamic trust model for vehicular cyber-physical systems. International Journal of Network Security, 20(1), 157-167 (2018)
9. Wang, Y., Zhong, H., Xu, Y., Cui, J.: ECPB: Efficient conditional privacy-preserving authentication scheme supporting batch verification for VANETs. International Journal of Network Security, 18(2), 374-382 (2016)
10. Ibrahim, S., Hamdy, M., Shaaban, E.: Towards an optimum authentication service allocation and availability in VANETs. International Journal of Network Security, 19(6), 955-965 (2017)
11. Zeng, S., Huang, Y., Liu, X.: Privacy-preserving communication for VANETs with conditionally anonymous ring signature. International Journal of Network Security, 17(2), 135-141 (2015)

12. Chen, C.L., Lai, Y.L., Chen, C.C., *et al.*: RFID ownership transfer authorization systems conforming EPCglobal class-1 generation-2 standards. International Journal of Network Security, 13, 41-48 (2011)
13. Wei, C.H., Hwang, M.S., Chin, A.Y.H.: A secure privacy and authentication protocol for passive RFID tags. International Journal of Mobile Communications, 15(3), 266-277 (2017)
14. Khedr, W.: On the security of Moessner's and Khan's authentication scheme for passive EPCglobal C1G2 RFID tags. International Journal of Network Security, 16(5), 369-375 (2014)
15. Wei, C.H., Hwang, M.S., Chin, A.Y.H.: An authentication protocol for low-cost RFID tags. International Journal of Mobile Communications, 9(2), 208-223 (2011)
16. Zhang X., King, B.: Security requirements for RFID computing systems. International Journal of Network Security, 6, 214-226 (2008)
17. Wei, C.H., Hwang, M.S., Chin, A.Y.H.: A mutual authentication protocol for RFID. IEEE IT Professional, 13(2), 20-24 (2011)
18. Xie, R., Jian, B.Y., Liu, D.W.: An improved ownership transfer for RFID protocol. International Journal of Network Security, 20(1), 149-156 (2018)
19. Cao, T., Shen, P.: Cryptanalysis of two RFID authentication protocols. International Journal of Network Security, 9(1), 95-100 (2009)
20. Cui, P.Y.: An improved ownership transfer and mutual authentication for lightweight RFID protocols. International Journal of Network Security, 18(6), 1173-1179 (2016)
21. Naveed, M., Habib, W., Masud, U., *et al.*: Reliable and low cost RFID based authentication system for large scale deployment. International Journal of Network Security, 14(3), 173-179 (2012)
22. Qian, Q., Jia, Y.L., Zhang, R.: A lightweight RFID security protocol based on elliptic curve cryptography. International Journal of Network Security, 18(2), 354-361 (2016)
23. Chikouche, N., Cherif, F., Cayrel, P.L., Benmohammed, M.: Improved RFID authentication protocol based on randomized McEliece cryptosystem. International Journal of Network Security, 17(4), 413-422 (2015)
24. Wei, C.H., Hwang, M.S., Chin, A.Y.H.: Security analysis of an enhanced mobile agent device for RFID privacy protection. IETE Technical Review, 32(3), 183-187 (2015)
25. Wei, C.H., Hwang, M.S., Chin, A.Y.H.: An improved authentication protocol for mobile agent device in RFID. International Journal of Mobile Communications, 10(5), 508-520 (2012)
26. Li, J., Wang, Y., Jiao, B., Xu, Y.: An authentication protocol for secure and efficient RFID communication. In: International Conference on Logistics Systems and Intelligent Management, pp. 1648-1651 (2010)