Another Improvement of RAPP: An Ultra-lightweight Authentication Protocol for RFID

Xinying Zheng[1], Chien-Ming Chen[1,2], Tsu-Yang Wu[1,2], Eric Ke Wang[1,2],
and Tsui-Ping Chung[3]

[1] School of Computer Science and Technology, Harbin Institute of Technology
Shenzhen Graduate School, Shenzhen, China
xinying_15@163.com
[2] Shenzhen Key Laboratory of Internet Information Collaboration, Shenzhen, China
dr.chien-ming.chen@ieee.org, wutsuyang@gmail.com, wk_hit@hitsz.edu.cn
[3] Department of Industrial Engineering, Jilin University, Nanling Campus,
Changchun, China
tpchung@jlu.edu.cn

Abstract. RFID technology has received increasing attention; however, most of the RFID products lack security due to the hardware limitation of the low-cost RFID tags. Recently, an ultra-lightweight authentication protocol named RAPP has been proposed. Unfortunately, RAPP is insecure against several attacks. In this paper, we propose an improvement of RAPP. Security analysis demonstrated that our protocol can resist several kinds of attacks.

Keywords: RFID, mutual authentication, security protocol.

1 Introduction

RFID (Radio Frequency IDentification) is a technique for identifying objects via radio frequency. It has received increasing attention in many applications such as supply chain management systems, transportation, access control systems, ticketing systems and animal identification, etc.

An RFID system is composed of three components: a set of tags, RFID readers and one or more backend servers. A backend server stores the related information of tags, calculates the computational processes when authenticates a tag. An RFID reader (called as reader in this paper) accesses a backend server via secure network channel, and then acquires the information related to the tags. RFID tags are small electronic devices which composed of antennas, microprocessors and memory storages. A tag communicates with a reader by using radio frequency signals transmitting from the reader.

Security and privacy issues are concerned mostly in RFID applications. As a result, researchers have proposed many RFID authentication protocols. The RFID authentication protocol can be categorized into 4 classes. The first class

J.-S. Pan et al. (eds.), *Intelligent Data Analysis and Its Applications, Volume 1*,
Advances in Intelligent Systems and Computing 297,
DOI: 10.1007/978-3-319-07776-5_16, © Springer International Publishing Switzerland 2014

refers to protocols which apply conventional cryptographic functions. The second class refers to protocols that apply random number generator and one-way hash function. The third class refers to protocols that apply random number generator and Cyclic Redundancy Code checksum. The last one refers to those protocols that apply simple bitwise operations (such as XOR, AND, OR, etc.). Generally, the fourth class is treated as ultra-lightweight level.

Several ultra-lightweight authentication protocols for RFID have been proposed. However, most of these protocols are insecure. In this paper, we improved a well-known protocol named RAPP[1]. We also provide a detailed security analysis of the proposed protocol.

2 Related Work

With the rapidly growth of network technology, security issues have been concerned in various network environments [2–10]. In the RFID environment, security issues also receive increasing attention recently. In this paper, we put emphasis on RFID authentication protocol, especially focus on ultra-lightweight authentication protocols.

An ultra-lightweight authentication protocol means that it utilizes only simple bitwise operations on the tags. Several ultra-lightweight protocols have been proposed. Peris-Lopez et al. proposed a family of ultra-lightweight protocols [11–13] in 2006. Later, these protocols are demonstrated to be vulnerable to de-synchronization attacks and full-disclosure attacks [14, 15]. In 2007, Chien proposed another protocol named SASI [16]. However, SASI is vulnerable to de-synchronization attack [17–19], traceability attack [20] and full-disclosure attack [19, 21]. Although Pedro Peris-Lopez et al. [22] attempted to improve SASI, this work [22] is insecure against de-synchronization attack [23–25]. In 2009, Mathieu David et al. [26] introduced another protocol. Unfortunately, this work suffered from a new full-disclosure attack and a traceability attack [27]. In 2011, Aras Eghdamian etal. [28] proposed another ultra-lightweight protocol. However, [29] pointed out this protocol is vulnerable to full-disclosure attacks.

In 2012, Tian et al. [1] proposed a new ultra-lightweight RFID protocol named RAPP. The authors claimed that RAPP can withstand various attacks and provide strong data confidentiality and integrity. Unfortunately, several research have demonstrate that [29–32] is vulnerable various kinds of attacks. Fig. 1 shows the relation of the above protocols.

3 Security Requirement for RFID Authentication Protocol

3.1 Security Requirements

To defend against the common seen threats, the design of RFID systems should satisfy the following security requirements.

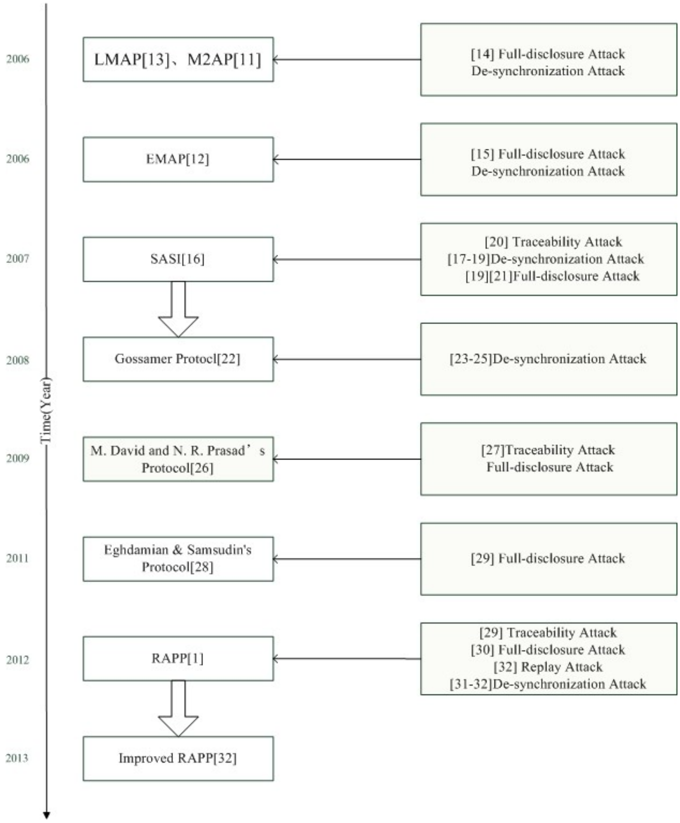
2006
LMAP[13]、M2AP[11]
[14] Full-disclosure Attack
De-synchronization Attack
2006
EMAP[12]
[15] Full-disclosure Attack
De-synchronization Attack
2007
SASI[16]
[20] Traceability Attack
[17-19]De-synchronization Attack
[19][21]Full-disclosure Attack
2008
Gossamer Protocl[22]
[23-25]De-synchronization Attack
Time(Year)
2009
M. David and N. R. Prasad' s
Protocol[26]
[27]Traceability Attack
Full-disclosure Attack
2011
Eghdamian & Samsudin's
Protocol[28]
[29] Full-disclosure Attack
2012
RAPP[1]
[29] Traceability Attack
[30] Full-disclosure Attack
[32] Replay Attack
[31-32]De-synchronization Attack
2013
Improved RAPP[32]

Fig. 1. Related Work of Ultra-Lightweight Authentication Protocol

- Uniqueness: Every tag in an RFID system should be unique, which means an RFID reader should be able to distinguish any RFID tag from the others. This requirement can be satisfied by assigning an unique identifier to each tag, and then the tag responds its identifier to the reader's queries.
- Reader-to-tag authentication: The reader should be able to confirm the identity information that an tag claimed is true. In most of the RFID application, the tag is used to uniquely identify an object or a person. If the reader-to-tag authentication cannot be fulfilled, anyone can forge an RFID tag with another tag's identity information, and then disguise itself as the genuine one.
- Tag-to-reader authentication: Since the adversary may use other invalid readers to query and collect data from the tags without arising carrier's attention. Thus, before transmitting any sensitive data, the tag should verify the reader's identity and authenticate the claimed identity is valid or not.

- Mutual authentication: An RFID system fulfills the property of mutual authentication if it satisfies both reader-to-tag authentication and tag-to-reader authentication.
- Integrity: The message receiver should be able to verify that the received messages has not been modified during transmission. That is, the attacker should not be able to forge a message to substitute the original one.
- Forward secrecy: The session key which derived from a secret key that used in one session will not compromise if the secret key is compromised in the future.
- Anonymity: The information emitted from a tag cannot be link to a product, a person or even the tag itself.
- Resistance to compromising attacks: It is difficult to prevent an adversary from stealing valid tags or readers and then physically compromising them. What we concerned is the impact to the entire system when the adversary acquires the stored data in these compromised devices. With the secrets stored inside the tag, the adversary may figure out a way to forge another valid tag without compromising it. In order to resist to such situation, the secrets should be independent among the tags.
- Resistance to denial-of-service attack: In RFID authentication protocol, the asynchronous data between the reader and the tag will result in authentication failure. And the tag can no longer be scanned by the readers, thus, its service is unavailable. As the result, the protocol should handle these data carefully, and maintain data recovery scheme.

4 The Proposed Protocol

In this section, we describe our protocol which is modified from RAPP [1]. Notations used in this paper are shown in Table 1.

Table 1. Notations

Notation	Description
$\oplus$	Bitwise XOR operation
$wt(x)$	Hamming weight of the binary string x
$f(x,y)$	A secure lightweight pseudo random function (PRF) which takes two inputs x, y and outputs a pseudo random value where $f(x,y) \neq f(y,x)$.
$Rot(x,y)$	Circular left rotation binary string x by $wt(y)$ bit(s)
$Per(x,y)$	The permutation operation of x according to y
r^i	A random number used for ith authentication
K_1^i, K_2^i	Two keys used for ith authentication
L	The bit length of one pseudonym or one key

Fig. 2 illustrates our design. Each tags has its static identification (ID), and pre-shares a pseudonym (IDS) and two keys with the reader. In our protocol, a reader and a tag authenticate to each other. After that, both reader and tag update the pseudonym and related keys individually. As shown in Fig. 2, reader not only stores new pseudonym IDS^{new} and key K_1^{new}, K_2^{new}, but also keeps old pseudonym IDS^{old} and key K_1^{old}, K_2^{old}. This is because we try to resist replay attacks and de-synchronization attacks.

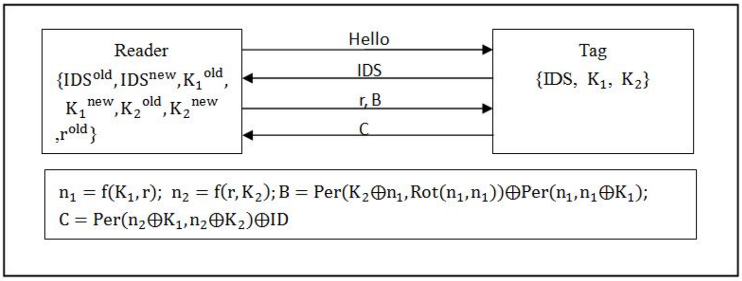
Reader
{IDS^old, IDS^new, K1^old, K1^new, K2^old, K2^new, r^old}
Hello
IDS
r, B
C
Tag
{IDS, K1, K2}
n1 = f(K1, r); n2 = f(r, K2); B = Per(K2⊕n1, Rot(n1, n1))⊕Per(n1, n1⊕K1);
C = Per(n2⊕K1, n2⊕K2)⊕ID

Fig. 2. The Proposed Protocol

As described above, after ith authentication round, the reader keeps IDS^i, IDS^{i-1}, K_1^i, K_2^i, K_1^{i-1},K_2^{i-1}, r^i. The detailed procedures of the $i+1$th authentication are listed as follows.

Step 1 A reader sends "Hello" message to a tag to initiate new protocol.

Step 2 This tag responds to the reader with its IDS^i.

Step 3 The reader checks the freshness of this received IDS. If the reader receives IDS^i, it generates a random value r^{i+1} and calculates n_1 and n_2 with K_1^i, K_2^i and r^{i+1}. It then calculates B and transmits B and r^{i+1} to the tag.

After transmitting B and r^{i+1}, the reader updates IDS^{i+1},K_1^{i+1} and K_2^{i+1} where $IDS^{i+1} = Per(IDS^i, n_1 \oplus n_2) \oplus K_1^i \oplus K_2^i$, $K_1^{i+1} = Per(K_1^i, n_1) \oplus K_2^i$ and $K_2^{i+1} = Per(K_2^i, n_2) \oplus K_1^i$. The reader also keeps IDS^i, K_1^i, K_2^i and r^{i+1} to prevent replay attacks and de-synchronization attacks.

Step 4 Upon receiving the messages, the tag calculates n_1 and B' with r^{i+1}, K_1^i, K_2^i. If B' equals B, the tag calculates C and sends it to reader.

After sending C to the reader, the tag also calculates IDS^{i+1},K_1^{i+1} and K_2^{i+1} similar to the equations in Step 3.

Step 5 The reader checks the received C with its secrets.

On the other hand, the reader may receive IDS^{i-1} in step 2. This is because the tag did not update its keys and IDS in the last authentication round for some reasons. As a result, it calculates B with K_1^{i-1},K_2^{i-1}, r^i and transmits B, r^i to the tag.

5 Security Aanlysis

In this section, we show that our design is secure against the following attacks.

Replay attack. The replay of tags message will not do harm to our protocol, since the reader stores the random numbers r of the last authentication round. If a reader receives an old IDS, indicating that the tag did not get messages r and B in the last round and update its secrets. In this case, the reader uses the old r to continue the protocol.

De-synchronization attack. If an adversary attempts to de-synchronize the shared values between tags and readers in our protocol, he can intercept the message B or message C, or let the reader and the tag use different n_1 and n_2 to update their data. Actually, intercepting C is useless because both the reader and tag have updated their data before C is sent. Besides, intercepting B will cause the reader update its IDS and keys, but the tag does not. Once the reader receives the old IDS, it will use the old r to continue the protocol. Moreover, letting the reader and the tag use different n_1 and n_2 to update their data is impossible because n_1 and n_2 are calculated using a pseudo random function. That is, an adversary cannot find the direct relationship between r and B or C.

Full-disclosure attack. The main idea behind this attack on RAPP is that the attacker can modify the message A and B to deduce the relationship of adjoining bit of n_1. However, In this protocol, an adversary cannot obtain K_1; thus, n_1 cannot be disclosed.

Traceability attack. An adversary cannot find the Hamming weight of n_1, n_2 or any other useful values, since all the values will be updated after each protocol round.

6 Comparison

In this section, we compare the performance of our protocol with RAPP in terms of computation operation, the storage requirement and the communication cost. As shown in Table 2, our scheme has a better performance. Note that L means the bit length of one pseudonym or one key.

Table 2. Notations

	RAPP	Our Protocol
Computation	17 $\oplus$, 11 permutations, 2 rotations	11 $\oplus$, 6 permutations, 1 rotations
Storage requirement	5L	4L
Communication	7L	5L

7 Conclusion

In this paper, we propose an improvement of RAPP. Security analysis demonstrated that our protocol can resist several kinds of attacks. We also show that our protocol has better performance than RAPP.

Acknowledgement. The work of Chien-Ming Chen was supported in part by the Project HIT.NSRIF. 2014098 Supported by Natural Scientific Research Innovation Foundation in Harbin Institute of Technology, in part by Shenzhen Peacock Project, China, under Contract KQC201109020055A, and in part by Shenzhen Strategic Emerging Industries Program under Grant ZDSY201206131 25016389. the work of Eric Ke Wang was supported in part by National Natural Science Foundation of China (No.61100192), and Shenzhen Strategic Emerging Industries Program under Grants No. JCYJ20120613151032592.

References

1. Tian, Y., Chen, G., Li, J.: A new ultralightweight rfid authentication protocol with permutation. IEEE Communications Letters 16(5), 702–705 (2012)
2. Chen, C.M., Lin, Y.H., Chen, Y.H., Sun, H.M.: Sashimi: secure aggregation via successively hierarchical inspecting of message integrity on wsn. Journal of Information Hiding and Multimedia Signal Processing 4(1), 57–72 (2013)
3. Wei-Chi, K., Chien-Ming, C., Hui-Lung, L.: Cryptanalysis of a variant of peyravian-zunic's password authentication scheme. IEICE Transactions on Communications 86(5), 1682–1684 (2003)
4. Wu, T.Y., Tseng, Y.M.: Further analysis of pairing-based traitor tracing schemes for broadcast encryption. Security and Communication Networks 6(1), 28–32 (2013)
5. Chen, C.M., Wang, K.H., Wu, T.Y., Pan, J.S., Sun, H.M.: A scalable transitive human-verifiable authentication protocol for mobile devices. IEEE Transactions on Information Forensics and Security 8(8), 1318–1330 (2013)
6. Hong, T.P., Lin, C.W., Yang, K.T., Wang, S.L.: Using tf-idf to hide sensitive itemsets. Applied Intelligence, 1–9 (2013)
7. Chien-Ming, C., Wei-Chi, K.: Stolen-verifier attack on two new strong-password authentication protocols. IEICE Transactions on Communications 85(11), 2519–2521 (2002)
8. Wu, T.Y., Tseng, Y.M.: Publicly verifiable multi-secret sharing scheme from bilinear pairings. IET Information Security 7(3), 239–246 (2013)
9. Chen, C.M., Chen, Y.H., Lin, Y.H., Sun, H.M.: Eliminating rouge femtocells based on distance bounding protocol and geographic information. Expert Systems with Applications 41(2), 426–433 (2014)
10. Sun, H.M., Wang, H., Wang, K.H., Chen, C.M.: A native apis protection mechanism in the kernel mode against malicious code. IEEE Transactions on Computers 60(6), 813–823 (2011)
11. Peris-Lopez, P., Hernandez-Castro, J.C., Estevez-Tapiador, J.M., Ribagorda, A.: M^2AP: A Minimalist Mutual-Authentication Protocol for Low-cost RFID Tags. In: Ma, J., Jin, H., Yang, L.T., Tsai, J.J.-P. (eds.) UIC 2006. LNCS, vol. 4159, pp. 912–923. Springer, Heidelberg (2006)
12. Peris-Lopez, P., Hernandez-Castro, J.C., Estevez-Tapiador, J.M., Ribagorda, A.: EMAP: An efficient mutual-authentication protocol for low-cost RFID tags. In: Meersman, R., Tari, Z., Herrero, P. (eds.) OTM 2006 Workshops. LNCS, vol. 4277, pp. 352–361. Springer, Heidelberg (2006)

13. Peris-Lopez, P., Hernandez-Castro, J., Estevez-Tapiador, J., Ribagorda, A.: LMAP: A Real Lightweight Mutual Authentication Protocol for Low-Cost RFID tags. In: Proc. of the 2nd Workshop on RFID Security (2006)
14. Li, T., Wang, G.: Security Analysis of Two Ultra-Lightweight RFID Authentication Protocols. In: Venter, H., Eloff, M., Labuschagne, L., Eloff, J., von Solms, R. (eds.) New Approaches for Security, Privacy and Trust in Complex Environments. IFIP, vol. 232, pp. 109–120. Springer, Boston (2007)
15. Li, T., Deng, R.: Vulnerability Analysis of EMAP-an Efficient RFID Mutual Authentication Protocol. In: Proc. of the 2nd Inter. Conf. on Availability, Reliability and Security, pp. 238–245 (2007)
16. Chien, H.Y.: SASI: A New Ultralightweight RFID Authentication Protocol Providing Strong Authentication and Strong Integrity. IEEE Trans. on Dependable and Secure Computing 4(4), 337–340 (2007)
17. Cao, T., Bertino, E., Lei, H.: Security analysis of the sasi protocol. IEEE Transactions on Dependable and Secure Computing 6(1), 73–77 (2009)
18. Sun, H.M., Ting, W.C., Wang, K.H.: On the Security of Chien's Ultralightweight RFID Authentication Protocol. IEEE Trans. on Dependable and Secure Computing 8(2), 315–317 (2009)
19. D'Arco, P., De Santis, A.: On ultralightweight rfid authentication protocols. IEEE Transactions on Dependable and Secure Computing 8(4), 548–563 (2011)
20. Phan, R.W.: Cryptanalysis of a New Ultralightweight RFID Authentication Protocol – SASI. IEEE Trans. on Dependable and Secure Computing 6(4), 316–320 (2009)
21. Hernandez-Castro, J.C., Tapiador, J.M., Peris-Lopez, P., Quisquater, J.J.: Cryptanalysis of the sasi ultralightweight rfid authentication protocol with modular rotations. arXiv preprint arXiv:0811.4257 (2008)
22. Peris-Lopez, P., Hernandez-Castro, J.C., Tapiador, J.M.E., Ribagorda, A.: Advances in ultralightweight cryptography for low-cost RFID tags: Gossamer protocol. In: Chung, K.-I., Sohn, K., Yung, M. (eds.) WISA 2008. LNCS, vol. 5379, pp. 56–68. Springer, Heidelberg (2009)
23. Bilal, Z., Masood, A., Kausar, F.: Security analysis of ultra-lightweight cryptographic protocol for low-cost rfid tags: Gossamer protocol. In: International Conference on Network-Based Information Systems, NBIS 2009, pp. 260–267. IEEE (2009)
24. Yeh, K.H., Lo, N.: Improvement of two lightweight rfid authentication protocols. Information Assurance and Security Letters 1, 6–11 (2010)
25. Tagra, D., Rahman, M., Sampalli, S.: Technique for preventing dos attacks on rfid systems. In: 2010 International Conference on Software, Telecommunications and Computer Networks (SoftCOM), pp. 6–10. IEEE (2010)
26. David, M., Prasad, N.R.: Providing strong security and high privacy in low-cost rfid networks. In: Schmidt, A.U., Lian, S. (eds.) MobiSec 2009. LNICST, vol. 17, pp. 172–179. Springer, Heidelberg (2009)
27. Hernandez-Castro, J.C., Peris-Lopez, P., Phan, R.C.W., Tapiador, J.M.: Cryptanalysis of the david-prasad rfid ultralightweight authentication protocol. In: Radio Frequency Identification: Security and Privacy Issues. Springer (2010) 22–34
28. Eghdamian, A., Samsudin, A.: A secure protocol for ultralightweight radio frequency identification (rfid) tags. In: Abd Manaf, A., Zeki, A., Zamani, M., Chuprat, S., El-Qawasmeh, E. (eds.) ICIEIS 2011, Part I. CCIS, vol. 251, pp. 200–213. Springer, Heidelberg (2011)

29. Avoine, G., Carpent, X.: Yet another ultralightweight authentication protocol that is broken. In: Hoepman, J.-H., Verbauwhede, I. (eds.) RFIDSec 2012. LNCS, vol. 7739, pp. 20–30. Springer, Heidelberg (2013)
30. Shao-hui, W., Zhijie, H., Sujuan, L., Dan-wei, C.: Security analysis of rapp an rfid authentication protocol based on permutation. Technical report, Cryptology ePrint Archive, Report 2012/327 (2012)
31. Ahmadian, Z., Salmasizadeh, M., Aref, M.R.: Desynchronization attack on rapp ultralightweight authentication protocol. Information Processing Letters 113(7), 205–209 (2013)
32. Zhuang, X., Wang, Z.H., Chang, C.C., Zhu, Y.: Security analysis of a new ultralightweight rfid protocol and its improvement. Journal of Information Hiding and Multimedia Signal Processing 4(3) (2013)