Advanced Science and Technology Letters
Vol.50 (CST 2014), pp.55-61
http://dx.doi.org/10.14257/astl.2014.50.09

A Novel RFID Authentication Protocol for Multiple Readers and Tag Groups

Jian Shen*[1,2,3], Haowen Tan[1,3], Yang Wang[1,3], Sai Ji[1,3], Jin Wang[1,3]

[1]Jiangsu Engineering Center of Network Monitoring, Nanjing University of Information Science &Technology, Nanjing, 210044, China
[2] Jiangsu Technology & Engineering Center of Meteorological Sensor Network, Nanjing University of Information Science & Technology, Nanjing, 210044, China
[3]School of Computer & Software, Nanjing University of Information Science &Technology, Nanjing , 210044, China

Abstract. Due to demands of RFID application in supply chain, various authentication protocols are proposed in the purpose of solving existing problems of grouping tags identification. However, it is proved that verifiers in these protocols are not aware of abnormal relating devices instantly, which may cause both security and technical risks and lie heavy upon identification of the problematic tags and readers. In this paper, we propose a lightweight RFID authentication protocol for multiple RFID readers and tag groups, according to which the verifier is able to cope with multiple readers and tag groups simultaneously and know the detailed status of the problematic tags.

Keywords: RFID authentication; multiple readers; tag groups.

1 Introduction

Radio Frequency Identification (RFID), confirmed to have great potential in many applications, is basically composed of the backend processing system (BPS), readers and tags. Through radio communication, the whole RFID system is capable of identifying large amounts of goods with tags attached on them [1, 2]. Under normal circumstances, communication between the verifier and readers is set to be completely secure in many RFID authentication protocols. As a matter of fact, portable readers can be produced in very small size, which communicate with the verifier in wireless way. As a result, it is necessary for the verifier to check out the validity of readers in case of forgery attack, which is taken into consideration in the proposed protocol [3]. In this paper, we propose a novel RFID authentication protocol for multiple readers and tag groups, where the verifier is able to cope with multiple readers and tag groups.

This paper is arranged as followed: in the following section, some related works about RFID authentication protocols are introduced. Our proposed protocol is

* The corresponding author

ISSN: 2287-1233 ASTL

described in detail in section 3. Security analysis of the protocol is shown in section 4. Performance analysis of the protocol is shown in section 5. Finally, the conclusion of this paper is covered in section 6.

2 Related Work

2.1 Grouping Proofs for Two Tags

In 2004, A. Juels proposed yoking proof to solve the simultaneously scanning problem of two tags [4]. The key idea of yoking proof is to link the two tags together to generate a proof with the help of random number generator in order to keep freshness of data in each session. After that, J. Saito and K. Sakurai [5] pointed out that the original yoking proof is vulnerable to replay attack and gave out "yoking proof using timestamp" to prevent the reuse of previous messages. In 2006, S. Piramuthu claimed that J. Satio and K. Sakurai's proof still showed no resistance against replay attack and presented a novel proof to withstand the replay attack [6]. In 2008, Lien et al. proposed "reading order independent yoking proof" where the verifier does not need to predefine the reading order of tags before verification [7].

2.2 Grouping Proofs for Multiple Tags

As extensions of two tags proofs, grouping proofs aim to generate a proof of multiple tags simultaneously. In 2006, L. Bolotnyy and G. Robins extended A. Juels's work and proposed generalized yoking proof in [8]. However, identities of individual tags in [8] are not hidden. After that, anonymous yoking proof is introduced in order to preserve the privacy of tags [9]. Considering of threat of certain reading order of the tags, reading order independent grouping proof is proposed by Y. Lien et al in [7]. In 2009, select-response grouping proof is designed by the method of letting the verifier be involved in the authentication instead of letting the verifier wait for the proof generated by the reader passively [10].

We classified all the grouping proofs mentioned above into two families from the way the reader communicates with tags: the serial family and the parallel family. In the serial family, the reader exchanges information with each tag one by one and links them like a chain, which guarantees the integrity of the message. In the parallel family, the entire RFID system broadcasts messages to every tag at the same time. The proofs in the parallel family are more efficient than that in the serial family but may cause communication block.

3 The Proposed Protocol

3.1 Detailed Design of the Protocol

We propose a novel RFID authentication protocol for multiple RFID readers and tag groups in this paper. In our design, the incorrect message will be abandon so as to reduce the communication and computational cost of the entire RFID system as well as protect privacy and security. The notations used in the proposed protocol are shown in Table 1.

It is assumed that the entire RFID system has large amounts of readers and tag groups. The verifier knows the secret of all the tags groups and readers. The proposed grouping protocol is shown in Fig. 1.

The process of the protocol is described in detail as follows:

1) The verifier *V* sends the query to all the readers.

2) The reader R_i generates a random number r_{R_i} on receiving the query. R_i computes $P_{R_i} = MAC_{S_{g_i}}(r_{R_i}, ID_{R_i})$ and broadcasts $(GID_i, ID_{R_i}, r_{R_i}, P_{R_i})$ to all the tag groups.

3) The tag group g_i wakes up. Note that group g_i is assumed to have *k* tags from T_1 to T_k. These *k* tags begin to compute $P_{R_i}' = MAC_{S_{g_i}}(r_{R_i}, ID_{R_i})$ and compare with the received P_{R_i} to ensure the validity of R_i. After the authentication, each tag T_i generates a random number r_i using r_{R_i} as a seed and computes $Q_i = MAC_{S_{g_i}}(r_i, ID_{R_i}, ID_i)$. Then the tag T_i sends $(ID_{R_i}, r_i, GID_i, ID_i, Q_i)$ to R_i.

Table 1. Notations used in the proposed protocol

Symbol	Description
V	Verifier[1]
R_i	Reader *i*
T_i	Tag *i*
g_i	Tag group *i*
GID_i	Identifier of tag group *i*
ID_i	Identifier of tag *i*
r_i, r_{R_i}, r_{R_i}'	Random numbers
S_{g_i}	Secret of tag group *i*
MAC	Message Authentication Code
ID_{R_i}	Identifier of reader *i*

[1] In general, the backend processing system (BPS) and the verifier are considered as one entity.

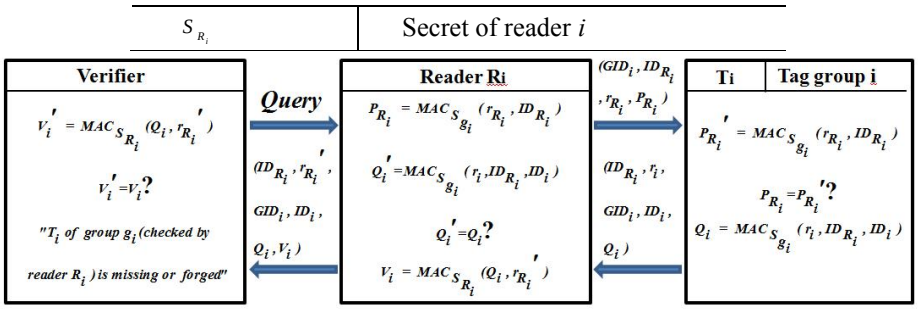

Fig. 1. A RFID authentication protocol for multiple RFID readers and tag groups.

4) The reader R_i computes $Q_i' = MAC_{S_{g_i}}(r_i, ID_{R_i}, ID_i)$ and checks it with Q_i to guarantee identities of tags. Then R_i identifies and abandons incorrect message and collects all the remaining tags into groups by its GID_i. R_i generates a random number r_{R_i}' and computes $V_i = MAC_{S_{R_i}}(Q_i, r_{R_i}')$ for each tag. At last, R_i adds V_i to the message received from T_i and relays $(ID_{R_i}, r_{R_i}', GID_i, ID_i, Q_i, V_i)$ to the verifier *V*.

5) The verifier computes $V_i' = MAC_{S_{R_i}}(Q_i, r_{R_i}')$ and compares it with V_i. If $V_i' = V_i$, authentication completes. If not, the verifier *V* terminates the protocol and shows "Tag T_i of group g_i (checked by reader R_i) is missing or forged".

3.2 Key Properties of the Protocol

The Mutual authentication: Mutual authentication is an important factor in grouping protocol verification. Due to the vulnerability of radio communication, it is significant for the verifier to check the validity of the readers. In our proposed protocol, the readers and tags authenticate with each other in the first time to guarantee the communicating entities are valid.

Reading order independence: Some grouping protocols arrange certain order for the tags to be checked. In this circumstance, the adversary may know the reading order of the tags and damage the RFID system. Hence, it is important to have the protocols independent on reading order. In the proposed protocol, it is not necessary for the tags to reply to the reader in a predefined reading order as our protocol belongs to the parallel family [7, 12].

4 Security Analysis

4.1 Resistance to Replay Attack

Mutual authentication is provided between the readers and tags, which strengthens the verification. Note that random numbers are used in every step of the protocol to prevent replay attack, which keeps the message fresh. In addition, the protocol encrypts the message with *MAC* computation and secret keys so as to defend against replay attack [7, 13].

4.2 Maintenance of Abnormal Tag Feedback

Our protocol can identify the abnormal tag and provide security protection. In our protocol, the verifier is able to acquire the detailed records of adversary's forgery attacks and finds out which tag is missing instantly [10], which is very important in practical situation. In other word, abnormal tag feedback improves the maintenance of tag groups, where the RFID system can check or replace the suspicious tags in time to preserve its integrity [14].

4.3 Ensuring of Reading Order Independent

The proposed protocol is independent of the reading sequence of RFID tags. In our scheme, the readers send information to all the tag groups at the same time and are capable of obtaining message from the specific tag groups whose GID_i are in accordance with the received group identifiers. Moreover, identities of the tags are involved in the verification so that the corresponding readers are able to identify the tags in any order. Without requiring a predefined sequence of tags, the entire RFID system in our protocol is efficient.

4.4 Against Clandestine Scan

In the proposed protocol, it is difficult for the adversary to obtain privacy information of the tags through clandestine scan. The tags will check GID_i and group secret before responding anything to ensure the validity of the readers [10]. As a result, malicious readers are refused to continue the communications since they are unknown of the GID_i and corresponding secret keys.

5 Performance Analysis

In our protocol, the verification process is simple. Note that only MAC functions are included in the computational operations, which is appropriate for low-price tags. In addition, the reader can identify the message intended to be sent to the verifier, which is applicable in practical situation and reduces computation cost of the verifier. Moreover, it needs to be stressed that most of the previous proposed grouping protocols are only good for single-reader occasion and do not take multiple-readers into consideration [5, 6, 7, 9, 10], while our protocol is capable of dealing with large amounts of tag groups and readers at the same time. The fact that massive tag groups and readers are under verification process simultaneously improves the speed of the whole system so the protocol is more efficient than aforementioned protocols.

6 Conclusions

In this paper we propose a RFID authentication protocol for multiple RFID readers and tag groups to verify groups of tags, where the verifier is able to know the detailed status of ineffective tags. The protocol is reading order independent and more efficient and secure than previous protocols. Furthermore, the entire RFID system is available to scan several readers and tag groups, which is very useful in RFID applications.

Acknowledgements. This work is supported by the National Science Foundation of China under Grant No.61300237, the research fund from Jiangsu Technology & Engineering Center of Meteorological Sensor Network in NUIST under Grant No.KDXG1301, the research fund from Jiangsu Engineering Center of Network Monitoring in NUIST under Grant No. KJR1302, the Natural Science Foundation of Jiangsu Province under Grant No.BK2012461, the 2013 Nanjing Project of Science and Technology Activities for Returning from Overseas, and the PAPD fund.

References

1. Chien, H. Y. and Liu, S. B.: Tree-Based RFID Yoking Proof. International Conference on Networks Security. Proc. of Wireless Communications and Trusted Computing (NSWCTC'09), vol. 1, pp. 550-553, Apr. 2009.
2. Sun, D. Z. and Zhong, J. D.: A Hash-Based RFID Security Protocol for Strong Privacy Protection. Proc. of IEEE Transactions on Consumer Electronics, vol. 58, pp. 1246-1252, Nov. 2012.
3. Jules, A.: RFID Security and Privacy: A Research Survey. IEEE Journal on Selected Areas in Communications, vol. 24, no.2, pp. 381-394, Feb. 2006.
4. Juels, A.: Yoking-proofs for RFID tags. Proc. of the Second IEEE Annual Conference on Pervasive Computing and Communications Workshops, pp. 138-143, Mar. 2004.

5. Satio, J. and Sakurai, K.: Grouping proof for RFID tags. Proc. of the 19th International Conference on Advanced Information Networking and Applications, vol. 2, pp. 621-624, Mar. 2005.
6. Piramuthu, S.: On Existence for Multiple RFID Tags. Proc. of IEEE International Conference on Pervasive Services(ICPS'06), pp. 317-320, Jun. 2006.
7. Lien, Y., Leng, X., Mayes, K. and Chiu, J. H.: Reading Order Independent Grouping Proof for RFID Tags. Proc. of IEEE International Conference on Intelligence and Security Informatics (ISI'2008), pp. 128-136, Jun. 2008.
8. Bolotnyy, L. and Robins, G.: Generalized "Yoking-proofs" for a Group of RFID Tags," Proc. of International Conference on Mobile and Ubiquitous Systems, pp. 1-4, Jul. 2006.
9. Lin, C. C., Lai, Y. C., Tygar, J. D., Yang, C. K. and Chiang, C. L.: Coexistence Proof Using Chain of Timestamps for Multiple RFID Tags. Proc. of Advances in Web and Network Technologies, and Information Management, pp. 634-643, 2007.
10. Leng, X., Lien, Y., Mayes, K., and Chiu, J. H.: Select-Response Grouping Proof for RFID Tags. Proc. of First Asian Conference on Intelligent Information and Database Systems (ACIIDS 2009), pp.73-77, Apr. 2009.
11. Burmester, M., Medeiros, B. D., and Motta, R.: Provably Secure Grouping-Proofs for RFID Tags. Proc. of International Federation for Information Processing, pp. 176-190, 2008.
12. Sun, H., Ting, W., and Chang, S.: Offlined simultaneous grouping proof for RFID tags. Proc. of the 2nd International Conference on Computer Science and its Applications, pp. 1-6, 2009.
13. Liu, H., Ning, H., Zhang, Y., He, D., Xiong, Q. and Yang, L. T.: Grouping-Proofs-Based Authentication Protocol for Distributed RFID Systems. Proc. of IEEE Transactions on Parallel and Distributed Systems, vol. 24, pp. 1321-1330, Jul. 2013.
14. Costa, F., Genovesi, S., Monorchio, A. and Manara, G.: Perfect metamaterial absorbers in the ultra-high frequency range. Proc. Int. Symp. Electromagn. Theory, pp. 701 -703, 2013.

