An Efficient Mutual Authentication protocol on RFID Tags

Hui-Feng Huang

Department of Information Management
National Taichung Institute of Technology, Taichung 404, Taiwan, R.O.C.
phoenix@ntit.edu.tw

Abstract. Recently, as low-cost radio frequency identification (RFID) becomes more pervasive in our daily lives, RFID systems may create new threats to security and privacy of individuals and organizations. It must have secure mutual authentication mechanisms to protect privacy information. However, the previous works on designing security protocols for RFID either do not conform to the EPCglobal Class 1 Generation 2 (GEN-2) standards or suffer from security flaws. In 2007, Chien and Chen proposed a mutual authentication protocol for RFID systems to improve the previous schemes. However, their scheme cannot efficiently retrieve the information of tags from its database for the authentication. To guarantee the quality of the growing popular communication services, it is urgent to construct efficient authentication for both parties of the tag and the back-end server such that the reader can quickly obtain the information of tag from its database. For light-weight calculation power of a tag and protecting the privacy of user (or product), this article proposes the RFID mutual authentication scheme based on GEN-2 standards. The proposed scheme can efficiently retrieve the information of tags from the database in the authentication process. Moreover, the proposed scheme can improve the previous schemes and provide anonymous property and forward secrecy.

Keywords: RFID system, security, authentication

1. Introduction

Owing to low cost and conveniences in identifying an object without physical contact, radio frequency identification (RFID) systems will replace the optical barcode on objects with consumer identification, the radio frequency identification RFID systems can be used in lots of applications such as supply chain management, parking garage management, and inventory controls and so on [1]. Radio frequency identification (RFID) is an automatic identification system that can remotely store and retrieve data about objects by using small devices called RFID tags. RFID systems consist of radio frequency (RF) tags and RF readers. Tag readers can question tags about their contents by broadcasting an RF signal, without physical contact. RFID devices can be broadly classified in two categories: those with a power supply that actively transmit to a reader are known as “active tags” and un-powered tags that are triggered by a

reader are called “passive tags”. EPCglobal and ISO are two important organizations standardizing and promoting technology. Especially, EPCglobal has great potential to influence the standard for RFID technology at the global scale [1]. One of the most important standards proposed by EPCglobal is EPCglobal Class 1 Generation 2 RFID specification (which is called GEN-2 RFID for short in this paper) that defines the functionality and operation of a RFID tag.

The current RFID system allows any reader to access any tag. The exposed private information stored in the tag could be jeopardized. Then, the widespread deployment of RFID systems into consumer products identification may expose potential security threats and risks either to corporations or individuals. For example, a dishonest company may try to collect information of competing company about physical distribution. By utilizing responses from a tag, an adversary may try to get knowledge of products which an individual user carries or trace a user. Therefore, the security of the RFID is becoming more and more important. It must have mutual authentication mechanisms to identify the legal tag and legal tag reader. Some RFID implementation would expose tags identifications when readers inquire them. In addition, the most important security requirement for user privacy is untraceability [2,11]. With an untraceability property, an attacker cannot track tags by suing interactions with tags. That is the values emitted by a tag must not be discriminated from the other tags. With anonymity, tags will not expose their identifications to eavesdroppers without authentications. It can protect the tag from tracing over wide areas.

To cope with the security threats, there are several protocols had been proposed to enhance the security of RFID systems [2-10]. However, most of previous protocols required the support of either hash function or encryption function on the tag. These protocols for RFID do not conform to the EPCglobal Class 1 Generation 2 (GEN-2) standards. Because the adopted hash functions cannot be supported on the current resource limited GEN-2 RFID specifications. Only few proposed schemes can be implemented on GEN-2 RFID tags [2,5]. Unfortunately, these schemes still suffer from security weaknesses, and they cannot provide anonymity property or forward secrecy. In 2007, Chien and Chen [11] proposed a mutual authentication protocol for RFID systems to improve the above mentioned schemes [2-10]. Their scheme is not only providing anonymity property and forward secrecy but also conforming to the GEN-2 standards. However, in Chien and Chen’s protocol [11], when the server receives the authentication request from the reader, it must iteratively pick up an entry information from its database to find a match tag. If it can find a match, then the authentication of the tag succeeds; otherwise it cannot pass the authentication. Their authentication process is repeated for each entry until it finds a match. It is not efficient for the reader to obtain the information of tags. To guarantee the quality of the growing popular communication services, it is urgent to construct efficient authentication for both parties of the tag and the back-end server such that the reader can quickly retrieve the information of tag from the back-end database.

For light-weight calculation power and protecting the privacy of a user (or product), this paper proposes the RFID mutual authentication scheme based on GEN-2 standards. The proposed method can immediately pick up an entry from its database for the authentication between the tag and the back-end server. It need not iteratively repeated for each entry until it finds a match. Therefore, the proposed protocol is

more efficient than Chien and Chen's scheme for the authentication. Moreover, the proposed scheme could protect a user (product) from tracing and provide the forward secrecy.

The remainder of this paper is organized as follows. In the next section, we will propose the mutual authentication protocol based on the RFID system. The security analysis of the proposed scheme is presented in Sections 3. And some conclusions will be made in the last section.

2. The Proposed Scheme

This section will propose a new efficient mutual authentication protocol for RFID systems. The assumption, initial setup, and authentication process are described as follows:

2.2 Assumption and Initial Setup

The proposed scheme is based on the EPCglobal Class 1 Generation 2 standards (GEN-2), where PRNG (Pseudo Random Number Generator) and Cyclic Redundancy code (CRC) operator are supported on passive tags [1]. The reader R connects with a legal back-end sever that has database D. We assume an attacker (or illegal reader) can monitor and modify the communications between the reader and the tags, but the communication between the reader and the back-end server (database) is secure. Here, the function $h(\ )$ means the Pseudo Random Number Generator.

In the initial stage, tag t_i and the back-end sever share the identifier ID_i, a secret key k_i, n_i, and a function $h(\ )$. The number n_i is randomly selected by the back-end server for a tag t_i. The back-end database contains fields *ID*, *N*, *K*, K_{last}, and N_{last} which save the identity of tag t_i; the current number of tag t_i, the current secret key k_i of tag t_i, the preceding secret key k_i^{last}, and the preceding number n_i^{last}, respectively. Here, the preceding k_i^{last} and n_i^{last} are the previous information which are replaced by the current values k_i and n_i, respectively. Based on GEN-2 standards, the tag and the reader *R* has the PRNG (Pseudo Random Number Generator $h(\ )$) to generate a random number for the authentication process.

Initially, the fields *ID*, *N*, and *K* are set up with the ID_i, the current number n_i, and the initial secret key k_i of each tag t_i, respectively; and all values of the field K_{last} and N_{last} are null in the back-end database. The roles of K_{last} and N_{last} are to prevent desynchronization.

Authentication Process

We depict the process of authentication between tag t_i and the back-end server as follows:

Step 1. Reader R generates and saves a new pseudorandom number s by utilizing PRNG, and sends s to tag t_i.

Step 2. Tag t_i also generates a new pseudorandom number r_1 and computes $r_2 = h(r_1 \| k_i \| s) \oplus ID_i$. Then, tag t_i sends r_1, r_2, and its current random number n_i to the reader R, where $\|$ is the concatenation of operations.

Step 3. After receiving r_1 and r_2, reader R delivers r_1, r_2, n_i, and s to the back-end server.

Step 4. When the back-end server receives the authentication request from the reader R, according to the current number n_i from one of fields N and N_{last}, it picks up an entry information (ID_i, k_i, k_i^{last}) of tag t_i from its database. It then computes and checks whether any of the following two equations hold.

$$r_2 = h(r_1 \| k_i \| s) \oplus ID_i \text{ or } r_2 = h(r_1 \| k_i^{last} \| s) \oplus ID_i . \quad (1)$$

In equation (1), it is depending on which value of fields N and N_{last} matches the current number n_i. If field N matches n_i, it checks whether equation $r_2 = h(r_1 \| k_i \| s) \oplus ID_i$ hold. Similarly, when the field N_{last} matches n_i, it checks whether equation $r_2 = h(r_1 \| k_i^{last} \| s) \oplus ID_i$ hold. If equation $r_2 = h(r_1 \| k_i \| s) \oplus ID_i$ or $r_2 = h(r_1 \| k_i^{last} \| s) \oplus ID_i$ holds, then authentication of the tag t_i succeeds, and the server performs the next step; otherwise, it sends a "failure" message to the reader R to stop the process.

Step 5. If the back-end server successfully authenticates tag t_i in step 4, it computes $r_3 = h(r_2 \| k_i \| s) \oplus ID_i$ or $r_3 = h(r_2 \| k_i^{last} \| s) \oplus ID_i$ depending on which value k_i or k_i^{last} satisfies in the verification equation (1) in step 4. It also updates the value of field N into $h(n_i \oplus k_i)$ and the value of field N_{last} into n_i; and updates the value of field K into $h(k_i)$ and the value of field K_{last} into k_i if $r_2 = h(r_1 \| k_i \| s) \oplus ID_i$ in equation (1); otherwise, it does not update the information of fields N, N_{last}, K, and K_{last}. Then, the server sends r_3 and the information of tag t_i to reader R.

Step 6. The reader retrieves the information of tag t_i and forwards r_3 to tag t_i. Upon receiving r_3, tag t_i computes $r_3' = h(r_2 \| k_i \| s) \oplus ID_i$ by using its secret key k_i, and then checks if $r_3' = r_3$. If it holds the current secret key k_i and random number n_i of tag t_i are replaced by $h(k_i)$ and $h(n_i \oplus k_i)$, respectively.

In the proposed scheme, it constructs a function chain of information as follows: The function chain starts from secret t, the second secret key x_2 is $h(t)$, and the other j-*th* element x_j is $h(x_{j-1})$ for each tag. Similarly, if a tag has the (j-1)-*th* random number y_{j-1} and (j-1)-*th* secret key x_{j-1}, then the j-*th* random number y_j is

$h(y_{j-1} \oplus x_{j-1})$ for the tag. For security, the random numbers s and r_1 should be used only one time in the protocol. The above processes are briefly illustrated in Figure 1.

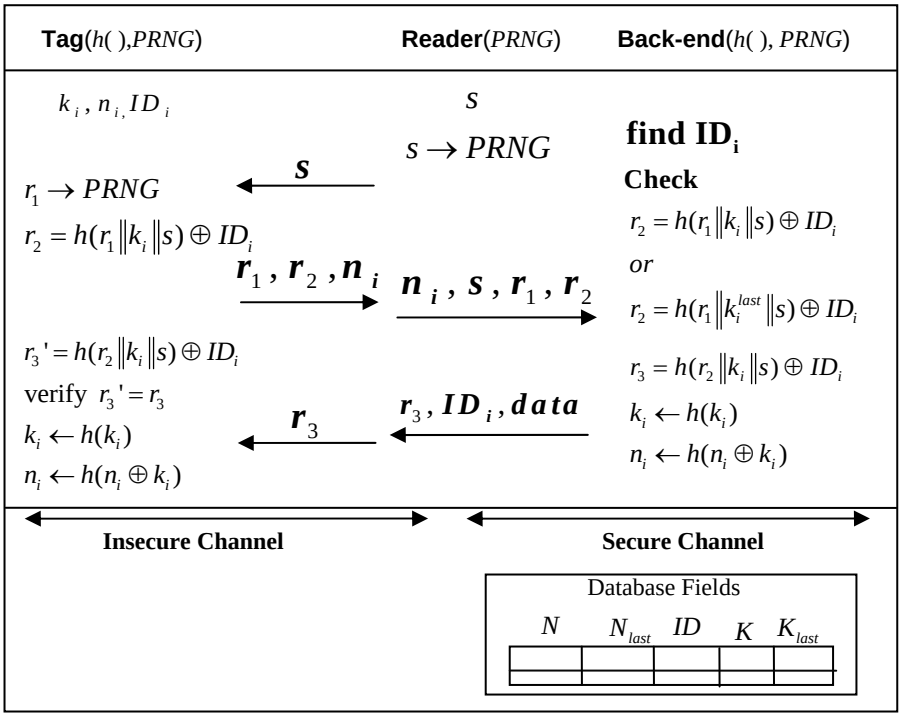

Fig. 1. The proposed Scheme

3. Security Analysis

In this section, we analyze the security of the proposed scheme. Due to the challenge of response technology and the freshness of random numbers s and r_1 per session, the proposed scheme achieves mutual authentication of the reader (sever) and the tag, and can resist the replay attack. In the proposed method, the design of simultaneously maintaining the old key (or old number) and the new key (or new number) for each tag in the back-end database can resist the Denial of Services attack (DOS). That is, the back-end database has been replaced by the current (or new) key with $h(k_i)$ and the current number $h(n_i \oplus k_i)$; however, when reader R sends the "r_3" command to tag t_i, it can suddenly be intercepted or modified by an attacker. Tag t_i will then hold the old key k_i and old number n_i. Thus, the shared information between the tag and the server (database) will be out of synchronization. In this situation, if the back-end

database only keeps the new information $h(k_i)$ and $h(n_i \oplus k_i)$ for each tag, then the tag and the reader can no longer authenticate each other. Then, the back-end database can deny the services for the tag. The DOS attack succeeds. Therefore, in our scheme, the back-end database simultaneously maintains old information and new information which can then resist the DOS attack.

On the other hand, only randomized data (s, r_1, r_2, r_3, n_i) are transmitted on the wireless channel between the reader R and tag t_i; and the information of tag t_i is only transmitted from the back-end sever to reader R through the secure channel. Therefore, the privacy and anonymity properties for tag t_i are ensured. With $r_2 = h(r_1 \| k_i \| s) \oplus ID_i$ and $r_3 = h(r_2 \| k_i \| s) \oplus ID_i$, an attacker can obtain $h(r_2 \| k_i \| s) \oplus h(r_1 \| k_i \| s)$ by computing $r_2 \oplus r_3$. However, it is not helpful for him to retrieve the secret key k_i of tag t_i.

In the proposed scheme, the current number n_i is replaced by $h(n_i \oplus k_i)$ after each successful authentication. That is, the number n_i is only used one time. Therefore, without knowing the current secret key k_i of tag t_i, even if an attacker can obtain the data (s, r_1, r_2, r_3, n_i) in this session, it is very hard for him to trace the same tag t_i for the next communication by means of n_i. Moreover, because the secure key k_i and current number n_i are updated after each successful authentication and the key and current number are generated by applying the Pseudo Random Number Generator $h(\ )$, the compromise of a tag would not lead to the tracing the previous communications for the same tag. It is very hard for an attacker to access the tags and trace the tags, hence forward secrecy is achieved. Therefore, the proposed scheme provides mutual authentication for a tag and the server in the RFID system and offers an anonymity property to protect tags from tracing. In summary, our scheme is not only resisting the replay attack and DOS attack but also providing forward secrecy, privacy property, and anonymity property.

With regard to the authentication process, in Chien and Chen's scheme [11], when the server receives the authentication request from the reader *R*, it iteratively picks up an entry information from its database to find a match tag. If it can find a match, then the authentication of the tag succeeds; otherwise it cannot pass the authentication. Their authentication process is repeated for each entry until it finds a match. It is not efficient for the authentication between the tag and the back-end server.

In the proposed scheme, the back-end database contains fields ID, N, K, K_{last}, and N_{last} which save the identity of tag t_i; the current number of tag t_i, the current secret key k_i of tag t_i, the preceding secret key k_i^{last}, and the preceding number n_i^{last}, respectively. Here, the preceding k_i^{last} and n_i^{last} are the previous information which are replaced by the current values k_i and n_i, respectively. When the back-end server receives the authentication request from the reader *R*, according to the transmission number n_i of tag, from one of fields N and N_{last}, it can quickly provide an entry

information (ID_i, k_i, k_i^{last}) of tag t_i from its database to achieve the authentication. It need not iteratively repeated for each entry until it finds a match. Therefore, the proposed protocol is more efficient than Chien and Chen's scheme [11] for the authentication.

4. Conclusions

For light-weight calculation power of a tag and protecting the privacy and confidential information of a user (product), we propose a new efficient RFID mutual authentication scheme based on GEN-2 standards. Through our authentication protocol, the reader can efficiently retrieve the information of tag from a database. Moreover, the proposed scheme provides forward secrecy and has the anonymity property that could protect a user (product) from tracing over wide areas. It is very convenient and efficient for many applications.

References

1. EPCglobal, http://www.EPCglobalinc.org/.
2. D. N. Duc, J. Park, H. Lee, and K. Kim, "Enhancing security of EPCglobal GEN-2 FRID tag against traceability and cloning," *The 2006 Symposium on Cryptography and Information Security*, 2006.
3. A. D. Henrici and P. Muller, "Hash-based enhancement of location privacy for radio-frequency identification devices using varying identifiers," *IEEE International Workshop on Pervasive Computing and Communication Security-PerSec*, pp.149-153, March 2004.
4. S. M. Lee, Y. J. Hwang, D. H. Lee, and J. I. Lim, "Efficient authentication for low-cost RFID systems," *International Conference on Computational Science and its Applications-ICCSA*, pp. 619-627, May 2005.
5. S. Karthikeyan and M. Nesterenko, "RFID security without extensive cryptography," *Proceedings of the 3rd ACM Workshop on Security of Ad Hoc and Sensor Networks*, pp. 63-67, 2005.
6. D. Molnar and D. Wagner, "Privacy and security in library RFID: issues, practices, and architectures," *ACM Conference on Computer and Communications Security-ACM CCS*, pp. 210-219, October 2004.
7. M. Ohkubo, K. Suzuki, and S. Kinoshita, "Cryptographic approach to privacy-friendly tags," *RFID Privacy Workshop*, November 2003.
8. S. A. Weis, S. E. Sarma, R. L. Rivest, and D. W. Engels, "Security and privacy aspects of low-cost radio frequency identification systems," *The Proceedings of the First Security in Pervasive Computing, LNCS*, vol. 2802, pp. 201-212, 2003.
9. K. Rhee, J. Kwak, S. Kim, and D. Won, "Challenge-response based RFID authentication protocol for distributed database environment," *International Conference on Security in Pervasive Computing-SPC 2005*, pp. 70-84, 2005.
10. Y. Yang, K. Ren, and K. Kim, "Security and privacy on authentication protocol for low-cost radio", *The 2005 Symposium on Cryptography and Information Security*, 2005.
11. H. Y. Chien and C. H. Chen, "Mutul Authentication Protocol for RFID Conforming to EPC Class 1 Generation 2 Standards," *Computer Standards and Interfaces*, pp. 254-259, vol. 29, 2007.