International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:3, No:11, 2009

Security Analysis on Anonymous Mutual Authentication Protocol for RFID Tag without Back-End Database and its Improvement

Songyi Kim, Kwangwoo Lee, Seungjoo Kim, Dongho Won

***Abstract*—**RFID (Radio Frequency IDentification) system has been widely used in our life, such as transport systems, passports, automotive, animal tracking, human implants, library, and so on. However, the RFID authentication protocols between RF (Radio Frequency) tags and the RF readers have been bring about various privacy problems that anonymity of the tags, tracking, eavesdropping, and so on. Many researchers have proposed the solution of the problems. However, they still have the problem, such as location privacy, mutual authentication. In this paper, we show the problems of the previous protocols, and then we propose a more secure and efficient RFID authentication protocol.

***Keywords*—** RFID, mutual authentication, serverless, anonymity.

I. Introduction

RFID system that is an automatic identification technology using radio frequency is a system to read and write the data of the entity [6]. RFID systems have been used in transport systems, passports, automotive, animal tracking, human implants, library, and so on. RFID systems consist of RF tags, or transponders, and RF readers or transceivers. The Fig. 1 shows the process of the general RFID system.

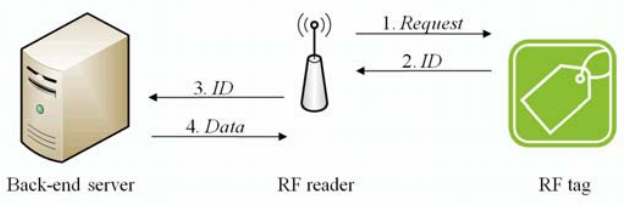

Fig. 1 general RFID system

The previous researchers in RFID authentication protocol attempt to solve the RFID security and privacy problem by utilizing the back-end server. In back-end server based RFID systems, the reader has to communicate with the back-end server to obtain the data from a tag. Therefore, back-end server based RFID systems are dependent on a reliable connection between a reader and the back-end server. However, the authentication protocol should be provided, even if the connection between the reader and the back-end server was not established. The several studies have recently been made on authentication protocol for RFID tag and reader without back-end server. The Fig. 2 shows the process of the authentication process without the back-end server.

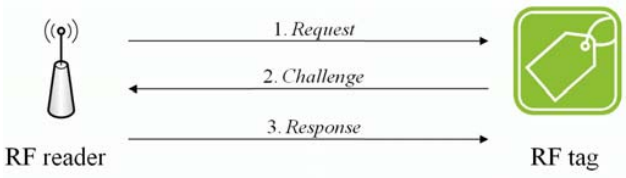

Fig. 2 serverless based RFID system

An authentication protocol for the tags and reader has the problems, such as the anonymity of the tags, the location privacy, and so on. In this paper, we propose a more secure and efficient authentication protocol that does not require the back-end server and provides the anonymity of the tags.

The rest of the paper is as follows. The next section reviews related work on requirements of the RFID system and existing proposed authentication protocols. In section 3, we propose a secure anonymous mutual authentication protocols for RFID tag without back-end server. This section is composed of four subsections: the first is organizations and notations; the second and third are the initial setup process of the reader and RFID tags; the forth propose a mutual authentication protocol without back-end server. In section 4, we analyze the security analysis and efficiency analysis with other protocols. Finally, we conclude our paper.

TABLE I
Requirements of the RFID authentication protocol

Requirements	Explanation
Confidentiality	The tag's private information must be kept secure to guarantee user privacy, and tag's information must be meaningless to any unauthorized users even though it can be easily obtained through eavesdropping by an attacker [8].
Anonymity	Although the tag's data are encrypted, the tag's unique identification information can be exposed since the encrypted data are constant. Therefore, it is important to make the information on the tag's anonymous [8].
Location privacy	The attackers know that when, form where and how much information is transmitted since the attackers can perform traffic analysis. The attackers can track the location of the tags [6].
Mutual authentication	Both parties authenticate themselves against each other [9].
Availability	In serverless system, the reader has to authenticate as well as provide security without server's intervention [10].

S. Kim, K. Lee, S. Kim and D. Won are with Information Security Group, Sungkyunkwan University, 300 Cheoncheon-dong, Jangan-gu, Suwon-si, Gyeonggi-do, 440-746, Korea ({s2kim, kwlee, skim, dhwon}@security.re.kr)
Corresponding author: Dongho Won.

II. Related Works

The requirements of the RFID authentication protocol for the RF tags and the reader is as following TABLE I.

RFID tags have recently been used in various applications. Therefore, many researches have been conducted on authentication protocol for RF tags and the reader without back-end server. In this paper, we review the Tan et al [1], [2] and Han et al [3], and then we propose the our protocol that satisfies the requirements of the RFID authentication protocol and a more secure and efficient protocol.

TABLE II shows the notations used in the previous protocols.

TABLE II
Notations for Tan et el. and Han et el.

Notation	Representation
CA	Off-line registration authority
id_i	Unique identifier of authorized reader
id_j	Unique identity of authorized tag
r_i	Random number generated by id_i
r_j	Random number generated by id_j
s_j	Secret for RFID tag id_j
$h(\bullet)$	One-way hash function
$\|\|$	Concatenation of bit-strings
L	Authentication list of the reader
m	CA defined number of bits, $m < l$
l	Number of bits of hash function $h(\bullet)$

In 2008, Tan et al. proposed a secure and serverless RFID authentication protocol. Their authentication list L is shown as following.

$$L \leftarrow h(id_i \| s_j) : id_j$$

The authentication protocol is shown in Fig. 3.

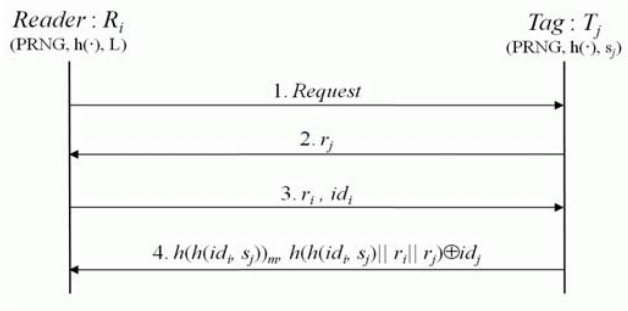

Fig. 3 Authentication protocol proposed by Tan et el.

1) RFID reader R_i sends an access request to RFID tag T_j.
2) T_j checks the request and generates a random number r_j, and then T_j sends to R_i.
3) R_i generates a r_i and sends r_i and its identifier id_i to T_j.
4) T_j sends its identity id_j as $h(h(id_i, s_j))_m, h(h(id_i, s_j) \| r_i \| r_j) \oplus id_j$.

Han et al. proposed an anonymous mutual authentication protocol, in 2007. The structure of authentication list is shown as following. 'k' means that the RFID in the k-th authentication process for the tag T_j.

$$L \leftarrow h(id_i \| s_j) : id_j : k$$

An authentication protocol proposed by Han et al. is described in Fig. 4.

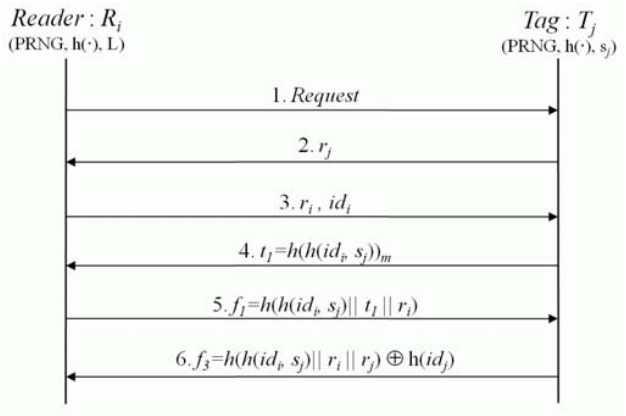

Fig. 4 Authentication protocol proposed by Han et el.

1) RFID reader R_i sends an access request to RFID tag T_j.
2) T_j checks the request and generates a random number r_j, and then T_j sends to R_i.
3) R_i generates a r_i and sends r_i and its identifier id_i to T_j.
4) T_j computes $h(h(id_i, s_j))_m$ and choose the first m bits of it to get t_1, and then sends to R_i.
5) R_i searches his authentication list L using $h(h(id_i, s_j))_m$, and then computes f_1 and sends to T_j.
6) T_j sets $f_2 = h(h(id_i, s_j) \| t_1 \| r_i)$ and compares the received f_1. If they are equal, then T_j forwards its pseudo-identity $h(id_j)$ as f_3.

Tan et el. claimed that the protocol provides the mutual authentication. The reader confirms that the tag is authorized by CA. However, they did not provide the reader authentication to the tag. Therefore, Tan et al. did not provide mutual authentication between RF tags and the reader. Han et al. provide the mutual authentication using the comparison of f_1 and f_2, $f_5 = f_3 \oplus f_4$. The tag believes the reader is authorized to access to the tag through the f_1. The reader believes the tag is

authorized by CA. However, the rounds and the computational complexity have been increased. Moreover, it did not satisfy the location privacy because always the same responses of the same reader's request. If the RFID authentication protocol does not provide the location privacy, tracking attack is possible.

III. Proposed Authentication Protocol

In this section, we present the proposed authentication protocol that provides anonymous mutual authentication and the location privacy.

A. Composition of the RFID system and notations

We propose the authentication protocol that does not require the back-end server. Our proposed authentication protocol is composed of the RF tag, the reader, and CA.

1) CA: CA is a trusted party responsible for deploying all the RF tags and the authorizing any RFID reader.
2) RF reader: The reader can authenticate the RFID tags without back-end server. Thus, each reader has a unique identifier and an authentication list.
3) RFID tag: Each tag contains a unique identity and a unique secret. The secret is only known by the particular tag and the CA.

TABLE III describe the notations used in our protocol.

TABLE III
NOTATIONS FOR THE RPOPOSED PROTOCOL

Notation	Representation
id_i	Unique identifier of authorized reader (128bit)
id_j	Unique identity of authorized tag (128bit)
r_i	Random number generated by id_i (128bit)
r_j	Random number generated by id_j (128bit)
s_j	Secret for RFID tag id_j
m	CA defined number of bits, $m < l$
$h(\bullet)$	One-way hash function
$\|\|$	Concatenation of bit-strings
L	Authentication list of the reader
l	CA defined number of bits, $m < l$ Number of bits of hash function $h(\bullet)$
$Request$	Request message header (4bit)

B. Initial setup process (from CA to the reader)

We assume that CA cannot be compromised, and that all readers once authenticated by the trusted CA. The reader needs to register at the CA that assign a list of hash valuation of identities of RFID tags to the RFID reader. The authentication list L is shown as following.

$$L \leftarrow h(id_i \| s_j) : id_j$$

The reader only knows the outcome of the $h(id_i \| s_j)$. Consequently it does not know the secret of the tags s_j.

C. Initial setup process (from CA to the tag)

The tag should shares a secret s_j with CA, and then the tag can be authorized by the reader. The authorized tag contains a unique identity id_j and a unique secret s_j. The secret s_j is known only by the tag itself and CA.

D. Proposed protocol

After the initial setup, the proposed authentication protocol is described in Fig. 5.

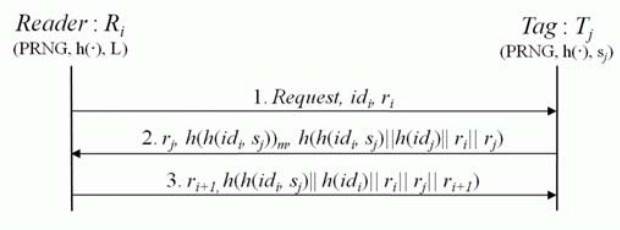

Fig. 5 The proposed protocol

1) The reader sends the request message to the tag. The message contains the identifier and the random number generates by itself.
2) The tag T_j checks the request and generates the random number r_j. T_j chooses the m bits of $h(h(id_i \| s_j)$ that get using the hash function $h(\bullet)$, its secret s_j, and the reader's id id_i. T_j computes its pseudo-identifier $h(id_j)$ and then sets $h(h(id_i \| s_j) \| h(id_j) \| r_i \| r_j)$. Finally, T_j sends to the reader R_i.
3) R_i compares $h(h(id_i \| s_j)_m$ with its list L. If they are equal, the reader believes that the tag is authorized by CA. The reader obtain $h(id_j)$ in its authentication list L. It generates the random number r_{i+1}, and then it computes $h(h(id_i \| s_j) \| h(id_j) \| r_i \| r_j \| r_{i+1})$. Finally, the reader forwards to the tag.

The messages in the protocol are only distinguished by the authorized tags and the reader because bit length is defined by the tags and the reader. The reader believes that the tag is authorized to CA using the message 2. The tag authenticates the reader using the message 3. Finally, the proposed protocol provides the mutual authentication.

IV. Security and Efficiency Analysis

In this section, we provide the security analysis and the comparison of the efficiency between the proposed protocol and the previous protocols.

A. Security analysis

We analyze how the proposed protocol satisfies the requirements described in TABLE I.

TABLE IV
COMPARISON OF THE REQUIREMENTS FOR THE RFID SYSTEM

Requirements	Tan et al.[2]	Han et al.[3]	Proposed protocol
Confidentiality	O	O	O
Anonymity	O	O	O
Location privacy	O	X	O
Mutual authentication	X	O	O
Availability	O	O	O

O : satisfied, X : not satisfied

1) Confidentiality: Every message in the authentication process is a secure against the unauthorized eavesdropper. It does not contain the usable information because it is a result of the hash function. Therefore, our proposed protocol satisfies the confidentiality.
2) Anonymity: In the authentication process, it should not revealed the any usable information about the tags. Our proposed protocol performed XOR operation with hashed tag's id. Thus, we satisfy the anonymity.
3) Location privacy: If the same reader requests to the same tags, the tag answers the same response. In that case, the tag will be able to track the movements or locations. We answer the different response, even if the same reader is querying the same tag. Therefore, we provide the location privacy.
4) Mutual authentication: We provide the tag-to-reader authentication using the message 2 and the reader-to-tag authentication using the message 3. Therefore, we provide the mutual authentication.
5) Availability: Whenever the authentication process should be able to authenticate. We can provide the authentication protocol for the RFID tags and the reader without back-end server. Therefore, we satisfy the availability.

We show the security against the available attacks in RFID system as following TABLE V.

TABLE V
SECURITY COMPARISON BETWEEN OUR PROPOSED PROTOCOL AND THE PREVIOUS SCHEMES

Attacks	Tan et al.[2]	Han et al.[3]	Proposed protocol
Eavesdropping	O	O	O
Replay attack	O	O	O
Cloning attack	O	O	O
Type attack	O	O	O
Tracking attack	O	X	O
Man-in-the-middle attack	O	O	O

O : secure, X : insecure

1) Eavesdropping: The adversary cannot get the any useful information through the eavesdropping. Therefore, our proposed protocol is a secure against eavesdropping.
2) Replay attack: The tag generates the different response in the every transaction using the random number. If the same reader request to the same tag, it cannot use the previous message. Thus, the replay attack is impossible.
3) Cloning attack: The attacker cannot predict the random number generated by the reader. Moreover, he does not know the tag's secret that shares with *CA*. Therefore, the adversary cannot make the fake tag.
4) Type attack: The type attack is possible when the challenge-message and the response-message is similar and equal the length. Therefore, our proposed protocol is a secure against the type attack.
5) Tracking attack: Han et al.'s protocol did not provide the location privacy. Therefore, the attacker will be able to track the movement of the tag. In our protocol, we generate the different message for each query. Thus, tracking attack is impossible.
6) Man-in-the-middle attack: Our proposed protocol is impossible to man-in-the-middle attack because the attacker does not know tag's secret. Therefore, he cannot generate the hash using the random number.

If the attacker obtains the authenticated reader, he cannot know the each tag's secret because they only have the hashed value. Therefore, the attacker cannot impersonate the other tags.

B. Efficiency analysis

The TABLE VI shows the efficiency of the proposed protocol comparing with the previous RFID authentication protocols.

TABLE VI
EFFICIENCY COMPARISON BETWEEN OUR PROPOSED PROTOCOL AND THE PREVIOUS SCHEMES

		Tan et al.[2]	Han et al.[3]	Proposed protocol
Reader	H	1	2	2
	X	1	1	-
	R	1	1	1
Tag	H	3	4	4
	X	1	1	-
	R	1	1	1
Rounds		4	6	3

H : the number of hash operation, X : the number of XOR operation,
R : the number of random number generator

We compared between our proposed protocol and the previous proposed protocols of the authentication protocols for the RFID tags and the reader without back-end server. When the proposed protocol is compared with Han et al., it reduced the communication rounds and the computation. Moreover we solved the problem of the location privacy. Also, when our protocol is compared with Tan et al., the proposed protocol provides mutual authentication that both tag-to-reader and reader-to-tag authentication. Therefore, our proposed protocol is a more secure and efficient.

V. Conclusion

In this paper, we have been studied the previous RFID authentication protocols that does not require the back-end server. The previous protocols still have security problems, such as mutual authentication and location privacy. Therefore, we try to resolve it.

Our proposed protocol has reduced the computational complexity and communication rounds. Moreover, we solved the problem of the location privacy. Finally, we show that the proposed protocol is a more secure and efficient as compare our protocol with the previous protocols.

Acknowledgment

* This work was supported by Defense Acquisition Program Administration and Agency for Defense Development under the contract UD070054AD.
* This research was supported by the MKE(Ministry of Knowledge Economy), Korea, under the ITRC(Information Technology Research Center) support program supervised by the NIPA(National IT Industry Promotion Agency)" (NIPA-2009-(C1090-0902-0016)).

References

[1] C.C. Tan, B.Sheng, and Qun Li, "Serverless Search and Authentication Protocols for RFID", Pervasive Computing and Communications 2007(PerCom 2007), pp.3-12, August. 2007.
[2] C.C. Tan, B.Sheng, and Qun Li, "Secure and Serverless RFID Authentication and Search Protocols", IEEE Transactions on Wireless Communications, vol.7, no.4, pp.1400-1407, April. 2008.
[3] S. Han, T.S.Dillon, and E. Chang, "Anonymous Mutual Authentication Protocol for RFID Tag Without Back-End Database", Springer, Mobile Sensor Networks 2007(MSN 2007), Lecture Notes in Computer Science vol.4864, pp.623-632, November 2007.
[4] Dirk Henrici and Paul Muller, "Hash-based Enhancement of Location Privacy for Radio-Frequency Identification Devices using Varying Identifiers", Proceedings of Workshop on Pervasive Computing and Communications Security, pp.149-153, 2004.
[5] JangYoung Chung, YoungSik Hong, "RFID Authentication Protocol Verification in Serverless Environment", Korea information science society, vol.35, no.1-(A), pp.140-145, June 2008.
[6] Keunwoo Rhee, Jin Kwak, Seungjoo Kim, and Dongho Won, "Challenge-Response Based RFID Authentication Protocol for Distributed Database Environment", International Conference on Security in pervasive Computing (SPC), pp.70-84, 2008.
[7] Hye-Jin Kwon, Jae-Wook Lee, Dong-Ho Jeon, and Soon-Ja Kim, "Easy to Search for Tags on Database and Secure Mutual Authentication Protocol for RFID system", Korea institute of information security and cryptology, vol. 18, no.5, pp.125-134, 2008.
[8] Batbold Toiruul, KyungOh Lee, HyunJun Lee, YoungHan Lee, and Yoon Young Park, "Mutual-Authentication Mechanism for RFID Systems", Lecture Notes in Computer Science, vol.4325, pp.449-460, 2006.
[9] Manfred Aigner and Martin Feldhofer, "Secure Symmetric Authentication for RFID Tags", Telecommunication and Mobile Computing(TCMC), March 2005.
[10] Sheikh I. Ahamed, Farzana Rahman, Endadul Hoque, Fahim Kawsar, and Tatsuo Nakajima, "S3PR:Secure Serverless Search Protocols for RFID", Information Security and Assurance, pp.187-192, April 2008.