Applied Mathematical Sciences, Vol. 8, 2014, no. 125, 6245 - 6255
HIKARI Ltd, www.m-hikari.com
http://dx.doi.org/10.12988/ams.2014.48664

An Ultra-lightweight RFID Seeking Protocol for Low-cost Tags

Il-Soo Jeon

School of Electronic Engineering, Kumoh National Institute of Technology,
77 Sanho-Ro, Yangho-Dong, Gumi, Kyungsangpuk-Do 730-701, Korea

Eun-Jun Yoon*

Department of Cyber Security, Kyungil University,
33 Buho-Ri, Hayang-Ub, Kyungsan-Si, Kyungsangpuk-Do 712-701, Korea

Abstract

RFID systems are widely used in various applications, and attaching RFID tags to objects are increasing. Recently, Xie et al. defined RFID seeking concept which is finding a lost tag in a blind spot or a specified tag among lots of similar ones and proposed a lightweight RFID seeking protocol. Their protocol provides security and privacy against most of common malicious attacks. However, since the protocol uses one-way hash functions to meet the requirement of the security and privacy problems, it is hard to be implemented in the low-cost passive RFID tags which have very constrained resources. Also, the protocol is vulnerable to the reader compromise attacks. Therefore, we propose an Ultra-lightweight RFID seeking protocol that can resolve the flaws of Xie et al.'s protocol. The proposed protocol uses Pseudo Random Number Generator (PRNG) and XOR operations in the tags. Since EPC C1G2 standard supports PRNG, the proposed protocol can be easily implemented in the low-cost passive tags compliant with the standard.

Keywords: RFID Seeking, Ultra-lightweight Seeking Protocol, Low-cost passive RFID Tags

* Corresponding author

1 Introduction

Radio Frequency Identification (RFID) enables objects to be identified automatically by using radio signals. The applications of RFID technology are increasing day by day such as inventory control, supply chain management, access control, smart labels, natural habitat monitoring, etc. RFID systems are usually consisted of three components: tags, readers, and a backend server. Identifying objects using RFID system is that tags having their unique IDs are attached to objects, and readers read the tag ID and identify it by using the stored information in the backend server. It is assumed that the communications between the reader and the backend server are secure. However, since the communications between the reader and each tag performed through wireless channel, they are vulnerable to the various security attacks and privacy invasions. Therefore, we have to cope with the security and privacy problems when developing applications of RFID system.

RFID tags are generally divided into three types: active tags, passive tags, and semi-active tags [1,2]. Active tags have their own battery, but passive tags have no battery in them and can get the power from the radio signal by the reader. The characteristics of passive tags are to have very limited hardware resources, cheap price, and to be applied to various applications. Semi-active tags have their own battery, but the battery is only used to operate their internal circuits not to communicate.

Recently, Xie et al. defined RFID seeking concept which is finding a lost tag in a blind spot or a specified tag among lots of similar ones and proposed a seeking protocol [3]. They showed that their protocol is safe from the common security attacks. The protocol also supports server-less and privacy-friendly to both the reader and the tags. There are researches that are similar to the RFID seeking problem such as RFID searching problem [4-10] and RFID monitoring problem [11-14]. RFID searching is to find a particular tag among a group of tags, and RFID Monitoring is to detect the missing of tagged items [3].

Xie et al. insists that their protocol is lightweight. However, since hash functions are used in their protocol, it is difficult to be implemented for the low-cost passive tags which have extremely constrained resources. Therefore, in this paper, we propose an ultra-lightweight RFID seeking protocol that does not use hash functions. The proposed protocol uses Pseudo Random Number Generator (PRNG) and XOR operations in the tags. Since EPC C1G2 standard includes PRNG, the proposed protocol can be easily implemented in the low-cost passive tags compliant with the standard.

The rest of this paper is organized as follows. In the following section, we introduce related work and preliminaries. In section 3, we describe the presented RFID seeking protocol, then the security and performance analysis of the proposed protocol is discussed in section 4. Finally, the conclusion is given in section 5.

2 Related Work and Preliminaries

In this section, we introduce Xie et al.'s seeking protocol [3] as a related research. They presented two application examples of RFID seeking scenario. One application scenario is to find a lost item in a blind spot like a secluded corner. Suppose a lady lost an expensive necklace in her way home. The necklace had been tagged with a tag-controlled indicator, which would generate sound/light alarms once the tag was activated. The lady had a PDA embedded with an RFID reader. She walked back along her track, holding the PDA to seek the necklace. When she was near the necklace, the tag was activated by the reader. And then, the tag-controlled indicator started an alarm via buzzing/flashing, guided the lady to find the lost necklace in bushes. The other application scenario is to find a specific tagged item among a mass of similar ones. Imagine that a postman was delivering lots of postal packages within a city. For each receiver, the postman needed to pick a specified package among similar others. If all packages had been tagged with tag-controlled indicators, the postman was able to seek a specific package by using his PDA embedded with an RFID reader i.e. after inputting a receiver's ID, the corresponding tag is activated, and the tag-controlled indicator starts buzzing/flashing, leading the postman to find the right package quickly [3].

Table 1. Notations used in Xie et al.'s protocol

Notation	Description
R_i, R'	Identifiers of readers
T_j, T_s, T'	Identifiers of tags
N_R, n_1, n_1', n_3	Random number generated by a reader
N_T, n_2, n_2'	Random number generated by a tag
$Rand_L$	Random number with bit length L
K_j	Secret of the tag T_j
S_j	Controlling state of T_j
L_i	Access list downloaded by the reader R_i from a certificate agency
Ctr_j	Counter of T_j
$H()$	Hash function
$PRNG()$	Pseudo Random Number Generator
$\oplus$	XOR operator
$\|$	String concatenation operator
$\rightarrow$	Message transmission

Assume an RFID system that consist of a set of readers $R = \{R_1, R_2, \dots, R_m\}$ and a set of tags $T = \{T_1, T_2, \dots, T_n\}$. Each tag has a binary state value *S* which controls a corresponding attached indicator. If the value of *S* is changed from 0 to 1, the indicator will be activated to generate sound/light alarm via buzzing/flashing. Each tag will also have its ID, a secret key. To describe protocol easily in this paper, some notations are used and summarized in Table 1.

Xie et al.'s protocol is composed of two phases: initialization phase and seeking phase. Each phase is briefly described below and illustrated in Fig. 1.

2.1 Initialization Phase

An RFID reader R_i downloads an Access List (AL) from a certificate authority (CA). The mobile reader is a portable device such as a PDA or a smart phone, rather than a well-protected backend server. Therefore, if the reader is stolen, then all tag's secrets in it would be revealed. To prevent from the problem, the secret key of each tag is not stored directly, but stored as a transformed key. The secret key K_j of the tag T_j in the reader R_i is stored as $H(R_i \| K_j)$ in the AL. Therefore, the AL of the reader R_i is $L_i = \{(T_1, H(R_1 \| K_1)), (T_2, H(R_2 \| K_2)), \ldots, (T_n, H(R_n \| K_n))\}$. Each tag T_j has a controlling binary state value S_j initialized to be passive, i.e. $S_j = 0$.

2.2 Seeking Phase

1. The reader R_i broadcasts α, β, N_R to seek a specified tag T_s, where $\alpha = H(T_s \| N_R) \oplus R_i$ and $\beta = H(R_i \| N_R) \oplus T_s$.
2. Each tag T_j computes $R' = H(T_j \| N_R) \oplus \alpha$ and $T' = H(R' \| N_R) \oplus \beta$. If $T' = T_j$, it means $T_j = T_s$, i.e. T_j is the tag sought by the reader, then T_j computes $\varepsilon = H(H(R' \| K_j) \| N_R \| N_T)$. Otherwise, it means $T_j \neq T_s$, i.e. T_j is not the tag sought by the reader, then T_j computes $\varepsilon = Rand_L$ where $Rand_L$ is random number with L bits. Each tag received the broadcasting message from the reader will generate ε, N_T that are different from each other. All the tags in the group respond to the reader with their own ε, N_T.
3. The reader R_i computes $\varepsilon' = H(H(R_i \| K_s) \| N_R \| N_T)$ using the values ε, N_T received from each tag. If $\varepsilon' = \varepsilon$, it means the seeking tag is found, then the reader computes $\theta = H(N_R \| N_T \| H(R_i \| K_s))$. Otherwise, the response is not from the seeking tag, then the reader computes $\theta = Rand_L$. Then, the reader responds to each tag with a corresponding θ.
4. Each tag computes $\theta' = H(N_R \| N_T \| H(R' \| K_j))$, which is compared with the received value θ. If $\theta' = \theta$, it means that T_j is the seeking tag by the reader, then T_j sets $S_j = 1$. Then, the tag-controlled indicator starts an alarm via buzzing/flashing. Therefore, the person holding the reader will find the lost item or the specified item.

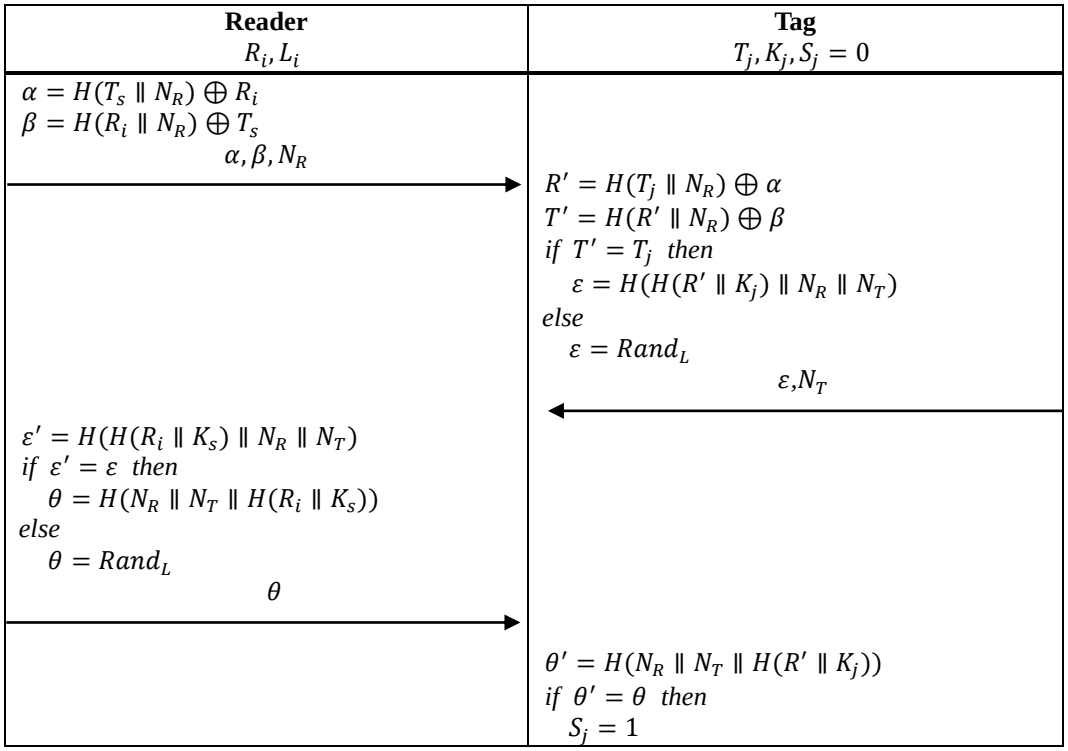

Fig. 1 Seeking Protocol of Xie et al.

3 The proposed protocol

In this section, we point out the flaws of Xie et al.'s protocol and propose an ultra-lightweight and more secure RFID seeking protocol. Xie et al.'s seeking protocol is serverless, privacy-friendly to both RFID readers and tags, and is secure against common attacks such as manipulating, replaying, tracing, Denial of Service (DoS), etc. However, since their protocol uses hash functions, it is difficult to be implemented in a low-cost passive tag which has very limited resources, and their protocol is not secure from the compromise attack of a reader. Since the protocol is based on serverless and the mobile readers, a user possessing the mobile reader can be stolen or lose it. If an attacker has the mobile reader, he/she can impersonate as a legal user. Therefore, we propose a more secure and lightweight RFID seeking protocol than Xie et el.'s protocol. The proposed protocol has a login process to enhance security and uses PRNG and XOR operations instead of hash functions in the tags to be an ultra-lightweight protocol for the low-cost passive tags.

The proposed protocol is composed of three phases: registration phase, initialization phase, and login and seeking phase. We describe the detail procedure of each phase below and illustrate briefly in Fig. 2.

3.1 Registration Phase

A user holding a mobile reader submits a user ID (UID), a mobile ID (R), and a password (Pwd) to a certificate authority (CA) via secure channel. Then, CA stores the user's information in the database. The password is stored as a hashed value, i.e. $H(Pwd)$ instead of *PWD*.

3.2 Initialization Phase

The initialization phase of the proposed protocol is similar to that of Xie et al.'s protocol. A user holding a RFID reader R_i downloads an Access List (AL) from the CA. The AL of the reader R_i is $L_i = \{(UID, H(Pwd)), (T_1, PRNG(R_i \oplus K_1)), (T_2, PRNG(R_i \oplus K_2)), \dots, (T_n, PRNG(R_i \oplus K_n))\}$. In the AL, the user's password, Pwd is stored as the form of $H(Pwd)$, and the secret key K_j of the tag T_j is stored as $H(R_i \oplus K_j)$. The tag T_j has a controlling binary state value S_j initialized to be passive, i.e. $S_j = 0$. The tag T_j has a counter Ctr_j whose initial value is set to 0. The counter is used as a component of PRNG seed to generate a pseudo random number in the tag.

3.3 Login and Seeking Phase

1. A user requests a login to the reader R_i and inputs the user ID, *UID* and the password, *PWD*, then R_i computes $H(Pwd)$. If *UID* and $H(Pwd)$ are equal to those of L_i, then proceeds next step. Otherwise, R_i terminates the session.
2. The reader R_i computes $A = PRNG(T_j) \oplus R_i$, $B = PRNG(R_i \oplus K_j) \oplus n_1$, and $C = PRNG(n_1 \oplus R_i)$ where n_1 is a random number generated by the reader. Then, the reader broadcast A, B, C to seek a specified tag T_j.
3. Each tag T_j computes $R_i' = A \oplus PRNG(T_j)$, $n_1' = B \oplus PRNG(R_i' \oplus K_j)$, and $C' = PRNG(R_i' \oplus n1')$. Then the tag compares the computed C' with the received C. If $C = C'$, it means T_j is the tag sought by the reader, T_j increment the counter Ctr_j and computes $n_2 = PRNG(Ctr_j \oplus K_j)$, $D = n_1' \oplus n_2$, and $E = PRNG(n_2 \oplus T_j)$ where n_2 is a pseudo random number generated by the tag. Otherwise, it means T_j is not the tag sought by the reader, then T_j computes $D = n_1' \oplus C'$ and $E = PRNG(n_1' \oplus T_j)$. Each tag that received the broadcasting message from the reader will generate D, E that are different from each other. All the tags within the reading range of the reader respond to the reader with their own D, E.
4. The reader R_i computes $n_2' = D \oplus n_1$ and $E' = PRNG(n_2' \oplus T_j)$ using the values D, E received from each tag. If $E' = E$, it means the seeking tag is found, then the reader computes $F = PRNG(n_1 \oplus n_2' \oplus R_i \oplus T_j)$. Otherwise, the response is not from the seeking tag, and the reader com-

putes $F = n_3$ where n_3 is a random number generated by the reader. Then, the reader R_i responds to each tag with a corresponding F.

5. Each tag computes $F' = PRNG(n_1' \oplus n_2 \oplus R_i' \oplus T_j)$, and F' is compared with the received value F. If $F' = F$, it means that the tag T_j is the seeking tag by the reader, then the tag T_j sets $S_j = 1$. Then, the tag-controlled indicator starts an alarm via buzzing/flashing. Therefore, the person holding the reader will find the lost item or the specified item easily.

In the proposed protocol, we used a counter Ctr_j in the tag T_j, which was not in Xie et al.'s protocol. To generate a pseudo random number of the tag T_j in the proposed protocol, the counter Ctr_j contributed as a part of the seed of PRNG.

Reader R_i, L_i	**Tag** $T_j, K_j, S_j = 0, Ctr_j = 0$
R_i receives user ID, *UID* and password, *Pwd* R_i computes $H(Pwd)$ *If UID and* $H(Pwd) \neq$ *those of* L_i *then Exit* *else* $A = PRNG(T_j) \oplus R_i$ $B = PRNG(R_i \oplus K_j) \oplus n_1$ *//*n_1*: Nonce* $C = PRNG(n_1 \oplus R_i)$ A, B, C →	

	$R_i' = A \oplus PRNG(T_j)$
	$n_1' = B \oplus PRNG(R_i' \oplus K_j)$
	$C' = PRNG(R_i' \oplus n1')$
	if $C = C'$ *then*
	$Ctr_j = Ctr_j + 1$
	$n_2 = PRNG(Ctr_j \oplus K_j)$
	$D = n_1' \oplus n_2$
	$E = PRNG(n_2 \oplus T_j)$
	else
	$D = n_1' \oplus C'$
	$E = PRNG(n_1' \oplus T_j)$
	D, E ←

$n_2' = D \oplus n_1$
$E' = PRNG(n_2' \oplus T_j)$
if $E = E'$ *then*
$F = PRNG(n_1 \oplus n_2' \oplus R_i \oplus T_j)$
else
$F = n_3$ *//*n_3*: Random No.*
F →	

	$F' = PRNG(n_1' \oplus n_2 \oplus R_i' \oplus T_j)$ *if* $F = F'$ *then* $S_j = 1$

Fig. 2 Proposed Seeking Protocol

4 Security Analysis and Performance Evaluation

In this section, we analyze the security and privacy of the proposed protocol and evaluate its performance

4.1 Security Analysis

- **Resistance to replay attack**

The reader and the tag can generate random (or pseudo random) numbers and use them in their communication messages. Since the random numbers are changed each session, communication messages can keep freshness. Therefore, the replay messages cannot be authenticated by either the reader or the tag. Thus, the proposed protocol can resist the replay attacks.

- **Resistance to DoS attack**

The proposed protocol does not need synchronization between the reader and the tag. Even though an attacker does de-synchronization attacks by blocking some communication messages in a session, there is no problem to be authenticated in another session between the reader and the tag. Therefore, the proposed protocol is safe from the DoS attacks.

- **Resistance to message modification**

Most of the communication messages were created by PRNG. If an attacker make modified messages that can pass the mutual authentication, he/she has to know the seed value of PRNG such as tag's secret key, tag's ID, reader's ID, and/or the counter value. However, since the attacker cannot extract the information from the communication messages, the proposed protocol has resistance to the message modification.

- **Resistance to tracking**

In the propose protocol, an attacker is unable to extract the ID of a reader or the ID of a tag by eavesdropping the reader's broadcasting messages or the response messages of the tags, because those IDs are not exposed directly but fused in the messages by PRNG and XOR operations. In addition, since the reader and the tags use random (or pseudo random) number for the message freshness, the messages generated by the same tag are different from each other in every session. Therefore, the proposed protocol provides anonymity and resistance to tracking for both the reader and the tags.

- **Resistance to impersonation attack**

Assume a reader was lost or stolen, and an attacker has the reader. Since the attacker does not know the password, he/she cannot success a login. Therefore, the attacker cannot impersonate as a legal user of the reader. Even though the attacker knows the contents of the AL in the reader, he/she cannot acquire any

secret keys of the tags. Therefore, the attacker cannot impersonate as a legal tag. Thus, proposed protocol is safe from the impersonation attacks for both the reader and the tags.

4.2 Performance Evaluation

The performance of the proposed protocol is compared to the Xie et al.'s protocol in Table 2. The target of performance evaluation is only the performance of tag side, because we can assume that the reader has powerful hardware and software to run the protocols. The comparison factors are composed of security, operation types, and communication costs in tag side. In Table 2, L denotes the length of each item in the communication messages.

As we can see in Table 2, the proposed protocol is more secure than Xie et al.'s protocol. The length of the communication messages is shorter than Xie et al.'s protocol. In our protocol, the computation costs and implementation space will be reduced considerably by using PRNG operations instead of hash functions. Therefore, we can say that our protocol will be a good option for various applications of RFID systems which use the low-cost passive tags.

Table 2. Comparisons of Performance

Protocol / Comparison factor	Xie et al.'s protocol [3]	Proposed protocol
Resistance to replay attack	Yes	Yes
Resistance to DoS attack	Yes	Yes
Resistance to message modification	Yes	Yes
Resistance to tracking	Yes	Yes
Resistance to impersonation attack	No	Yes
Communication message length	6L	5L
Operation types	$H()$,$\oplus$	$PRNG()$,$\oplus$

5 Conclusion

In this paper, we proposed a secure and ultra-lightweight RFID seeking protocol for the low-cost passive tags. The proposed protocol does not use hash functions but use PRNG and XOR operations in the tags. Those operations are good enough at the aspect of both computation costs and implementation space. Since the proposed protocol can meet the requirements of EPC C1G2 standard, it can be easily implemented in the low-cost passive tags compliant with the standard. Therefore, it will be a good solution for the RFID application systems using low-cost passive RFID tags.

Acknowledgements: Il-Soo Jeon was supported by Research Fund, Kumoh National Institute of Technology. Eun-Jun Yoon was supported by Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education, Science and Technology(No. 2010-0010106).

References

[1] M. Moessner and G. N. Khan, Secure authentication scheme for passive C1G2 RFID tags, *Computer Networks*, **56(1)** (2012), 273–286.

[2] C. Lee, S. Park, K. Lee, and D. Won, An attack on an RFID authentication protocol conforming to EPC class 1 generation 2 standard, *ICHIT*, (2011), 448–495.

[3] W. Xie, L. Xie, C. Zhang, Q. Wang, J. Xu, Q. Zhang, and C. Tang, RFID seeking: finding a lost tag rather than only detecting its missing, *Journal of Network and Computer applications*, **42** (2014), 135-142.

[4] C.C. Tan, B. Sheng, and Q. Li, Secure and serverless RFID authentication and search protocols, *IEEE Transactions on Wireless Communications*, **7(4)** (2008), 1400-1407.

[5] C.C. Tan, B. Sheng, and Q. Li, Serverless search and authentication protocols for RFID, *Proceedings of the 5th annual IEEE international conference on pervasive computing and communications*, (2007) WhitePlains, NY, United States, 3–12.

[6] T.Y. Won, J.Y. Chun, and D.H. Lee, Strong authentication protocol for secure RFID tag search without the help of central database, *IEEE/IFIP International Conference on Embedded and Ubiquitous Computing*, (2008), 153–158.

[7] Z. Kim, J. Kim, K. Kim, I. Choi, and T. Shon, Untraceable and serverless RFID authentication and search protocols, *2011 IEEE 9th International Symposium on Parallel and Distributed Processing with Applications Workshops*, (2011), 278–283.

[8] C.F Lee, H.Y Chien, and C.S Laih, Server-less RFID authentication and searching protocol with enhanced security, *International Journal of Communication Systems*, **25** (2012), 376-385.

[9] J.Y. Chun, J.Y. Hwang, and D.H. Lee, RFID tag search protocol preserving privacy of mobile reader holders, *IEICE Electron Express*, **8** (2011), 50–56.

[10] E.J. Yoon, Cryptanalysis of an RFID Tag Search Protocol Preserving Privacy of Mobile Reader, *International Federation for Information Processing*, (2012), 575–580.

[11] C.C. Tan, B. Sheng, and Q. Li, Efficient techniques for monitoring missing RFID tags, *IEEE Trans. On Wireless Communication*, **9** (2010), 1882–1889.

[12] C. Ma, J. Lin, and Y. Wang, Efficient missing tag detection in a large RFID system, *Proceedings of the 11th IEEE international conference on trust, security and privacy in computing and communications*, 2012, 185–192.
[13] T. Li, S. Chen, and Y. Ling, Identifying the missing tags in a large RFID system, *Proceedings of the 11th ACM international symposium on mobile ad hoc networking and computing*, 2010, 1–10.
[14] W. Luo, S. Chen, T. Li, and S. Chen, Efficient missing tag detection in RFID systems, *IEEE INFOCOM*, (2011), 356–360.

Received: August 30, 2014