Secure Hash-based Search Protocols for RFID Systems

He Jialiang[1] and Xu Zhiqiang[2]

*[*1]College of Information and Communication Engineering, Dalian Nationalities University, China*
[2]Department of digital media technology, Sichuan College of Media and Communications, China
urchin2012@sina.com and starsep928@yahoo.com.cn

Abstract

When RFID systems become pervasive in our life, tag search becomes crucial. However, the problem of RFID search has not been widely addressed in the literature. RFID search protocol which is used to find specific tags has many applications such as inventory management, supply chain management. In this paper, we propose a set of secure and private Hash-based RFID search protocols that can meet all known major attacks in RFID systems, and especially it can protect the privacy of mobile reader users.

Keywords: *RFID; Search Protocol; Security*

1. Introduction

Radio Frequency Identification (RFID) is a wireless technology which is used to automatic identify remote objects embedded with RFID tags [1]. RFID technology has been used in various application fields such as supply chain management, transportation, livestock management, e-payment system, e-passport system, patient medical care. A typical RFID system is composed of a backend server, readers and tags.

Key feature of RFID systems is a lack of physical contact between readers and tags, based on wireless communication; signal broadcasting, the existing RFID systems are vulnerable to many security attacks and privacy disclosure threats. Due to strictly limited calculation resources, small storage capacity and faint power supply of low-cost tags, it is difficult to apply an ordinary and complicated but safe cryptographic algorithm to a RFID system and these factors are hindering the rapid spread of this technology [2]. So designing an efficient and low-cost security scheme for RFID systems becomes an important research object.

Hence, a mobile reader has been developed in recent years to combine mobile technology with traditional RFID systems, through the integration of reading chips, PDA, and mobile devices, hence mobile RFID [3-6], it brings higher design requirements for RFID systems.

Recently, many RFID security protocols have been proposed. Usually, beyond RFID authentication protocols, the requirements for RFID systems from various application scenarios need use RFID search protocol. RFID search protocol which is used to find specific tags has many applications such as inventory management, supply chain management.

Security requirements for RFID search protocols based on static ID scheme include: meeting tag untraceability, meeting tag information protection, meeting privacy of search result, resist Denial of Service (DoS) attack and resist spoofing attack; security requirements for RFID search protocols based on dynamic ID scheme additionally include: meeting reader untraceability [9]. Presently, for the reason of convenient using and cost, lightweight methods like Hash, PRNG and CRC are used wildly in design of RFID security protocols. Especially, hash-based protocols have been researched actively.

The main contribution of this paper is to propose three hash-based RFID search protocols. The rest of this paper is organized as follows. In the second section, we propose a RFID search protocol based on static ID scheme. In the third section, we propose a RFID search protocol based on dynamic ID scheme for fixed RFID readers. In the forth section, we propose a RFID search protocol based on dynamic ID scheme for mobile RFID readers. Finally, the conclusion of this paper is provided in the fifth section.

2. A RFID search protocol based on static ID scheme

In [7], an efficient lightweight RFID mutual authentication protocol based on static ID scheme is proposed, this protocol only requires O(1) work to identify and authenticate a tag in the backend server and is particularly suitable for the low-cost RFID systems. This protocol is simply shown as follows:

2.1. Notation

Table 1. The Notations Used

Symbol	Meaning
H()	An one-way hash function, H: $\{0,1\}^{l*} \rightarrow \{0,1\}^{l}$ (The length of output is l)
PRNG()	The pseudo random number generator (The length of output is l_R, usually $l_R < l$)
$\oplus$	XOR operator
$\|\|$	Concatenation operator
M_L	The left part of the message M
M_R	The right part of the message M
R	The random number generated by the reader (The length is l_R)
ID	The unique index code of a tag (The length is l)
Info	Information of the corresponding tag
T	Temporary value (The length is l)
A→B:M	A sends message M to B

2.2. Assumptions

(1) The channel between the backend server and a reader is assumed secure. On the other hand, the channel between a reader and a tag is assumed insecure.

(2) The resources of each passive tag are constrained. In this protocol, each tag only needs to have a one-way hash function H( ), XOR operation capability and concatenation operation capability.

(3) A tag is not vulnerable to compromised with an adversary, that is to say, the adversary cannot acquire the inner information of the tag.

(4) The one-way hash function H( ) is secure enough against brute exhaustive search from an adversary.

2.3. The (i +1)th Authentication Access

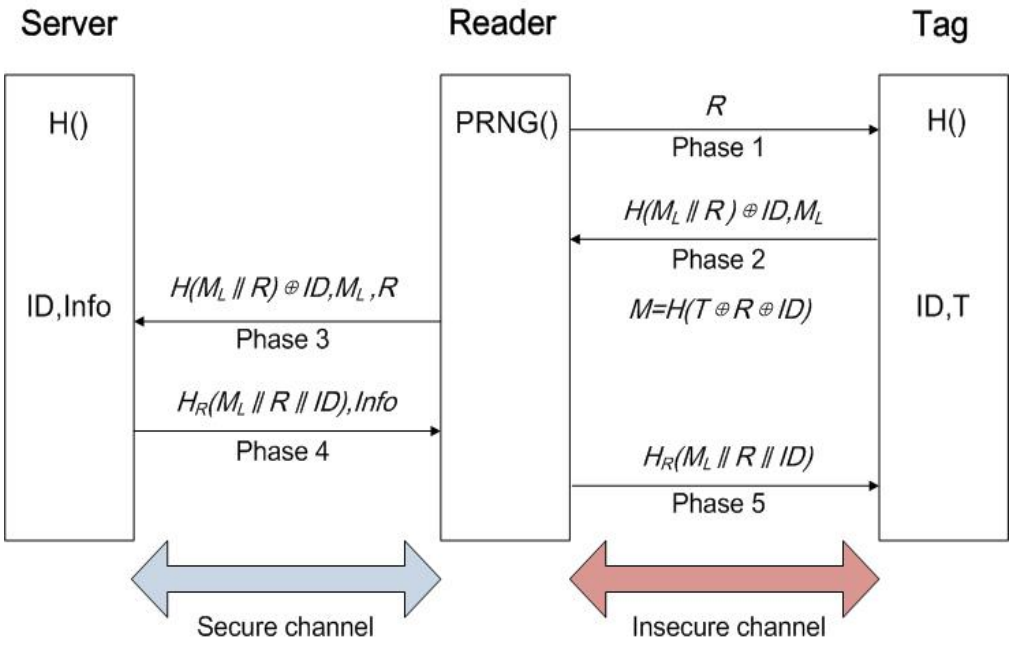

Figure 1. The Proposed Authentication Protocol

The detailed authentication access of this protocol refers to [7].

2.4. The Corresponding Search Protocol of this Authentication Protocol

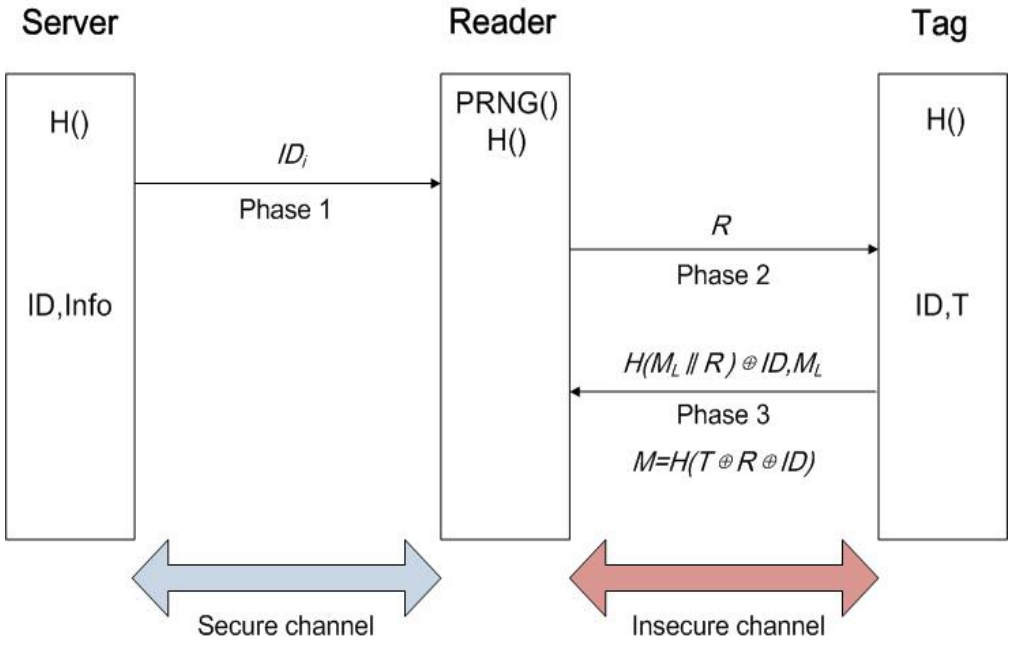

Figure 2. The Search Protocol

The execution access of the search protocol:

Step1: Server→Reader: ID_i
The Server chooses the ID of a specific tag (ID_i) and sends ID_i to the fixed reader.

Step2: Reader→Tag: R
After receiving ID_i from the server, the reader would store ID_i in its memory and generate a random R, then send R to tags.

Step3: Tag→Reader: $H(M_L \| R) \oplus ID, M_L$
After receiving R, each tag near the reader would calculate $M = H(T \oplus R \oplus ID)$ and $\alpha = H(M_L \| R) \oplus ID$, then send α and M_L back to the reader. Subsequently the tag should calculate $T_{i+1} = M \oplus \alpha$ and save T_{i+1} in its memory. Especially, we use $H(T \oplus R \oplus ID)$ to substitute pseudo random number of the tag.
After receiving $H(M_L \| R) \oplus ID$ from each tag, the reader should calculate $ID' = H(M_L \| R) \oplus (H(M_L \| R) \oplus ID)$, If ID' equals to ID_i, the specific tag is found, or the tag is not the specific tag that the server would search.

2.5. Security Analysis of this Search Protocol

We would analyze this protocol to evaluate whether it meets the security requirements as follows:

(1) Tag untraceability
An adversary could eavesdrop the response message ($H(M_L \| R) \oplus ID, M_L$) from a tag, and analyze the information carefully and try to detect the user's location privacy by tracking the tag. Because the tag generates a new substituted random number $M = H(T \oplus R \oplus ID)$ during each authentication access, and updates $T_{i+1} = M \oplus (H(M_L \| R) \oplus ID)$ in the step2, so the adversary cannot differentiate which tag does the response from the message ($H(M_L \| R) \oplus ID, M_L$). So this protocol can meet tag untraceability.

(2) Tag information protection
Because the information of an ID (Info) stores in the backend server, an adversary cannot acquire the information of the ID. So this protocol can meet tag information protection.

(3) Spoofing attack
An adversary feigns a legitimate reader which sends a query with R to tags through the forward channel, and obtains the response of a tag ($H(M_L \| R) \oplus ID, M_L$). In the next search access, when a legitimate reader sends a query with R', the adversary feigns the tag and responds the legitimate reader with the obtained message ($H(M_L \| R) \oplus ID, M_L$) through the backward channel. However, the reader generates a new random number during each access, that is to say, $R \neq R'$, so the adversary cannot perform tag impersonation attack.

(4) Denial of Service (DoS) attack
As the ID of a tag is fixed, even if loss of message, power failure or loss of connection with the backend server happens during an authentication access, it would not affect the backend server, namely it would not lose the synchronization between the backend server and the tag, only resetting a new access is well, so this protocol can shield DoS attack well.

(5) Privacy of search result
This protocol can protect the search result of a reader. Because all tags nearby the reader respond to the request, an adversary cannot learn whether the reader found a specific tag or

not. Even if the specific tag itself cannot know whether the reader wants to find it or not, Since each tag would calculate $H(M_L \| R) \oplus ID$ of its own and send $H(M_L \| R) \oplus ID$ to the reader.

3. A RFID Search Protocol based on Dynamic ID Scheme for Fixed Reader

In [8], an efficient RFID mutual authentication protocol supporting tag ownership transfer is proposed, this protocol only requires O(1) work to identify and authenticate a tag in the backend server and is suitable for the low-cost RFID systems. The security and performance of the proposed protocol are analyzed as well. This protocol is simply shown as follows:

3.1. Notation

Table 2. The Notations Used

Symbol	Meaning
ID	The unique index code of a tag (The length is l)
IDS	The tags' unique index-pseudonym (The length is l)
Info	Information of the corresponding tag stored in the backend server
H()	An one-way hash function, H: $\{0,1\}^{l*} \rightarrow \{0,1\}^{l}$ (The length of output is l)
$E_k()$	Symmetry encryption function (The length of output is l)
PRNG()	The pseudo random number generator (The length of output is l_R, usually $l_R < l$)
$\oplus$	XOR operator
$\|$	Concatenation operator
M_L	The left part of the message M
M_R	The right part of the message M
R	The random number generated by the reader (The length is l_R)
T	Temporary value (The length is l)
Pre-x	The previous value of x
Cur-x	The current value of x
x_i	The x value in the (i)th session of this protocol
A→B:M	A sends message M to B

3.2 The (i +1)th authentication access

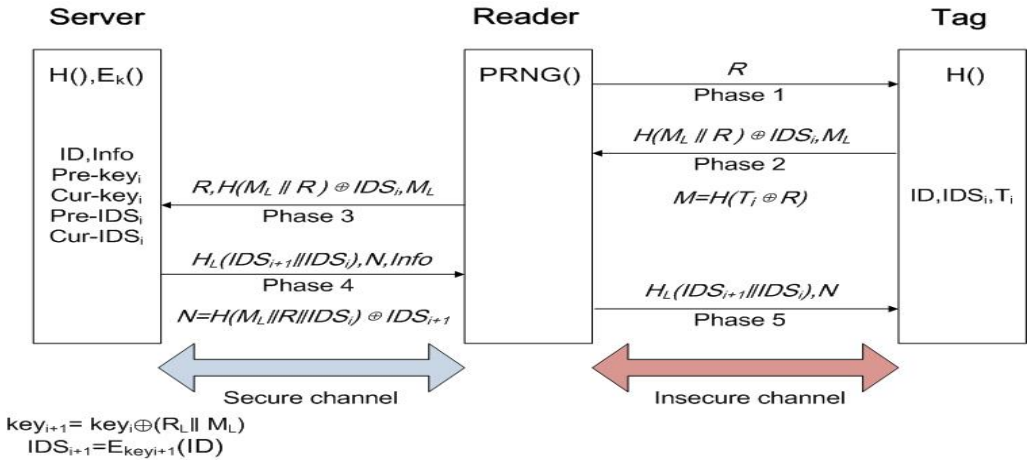

Figure 3. The Proposed Authentication Protocol

The assumptions of this protocol refer to Section 2.2. The detailed authentication access of this protocol refers to [8].

3.3. The Corresponding Search Protocol of this Authentication Protocol

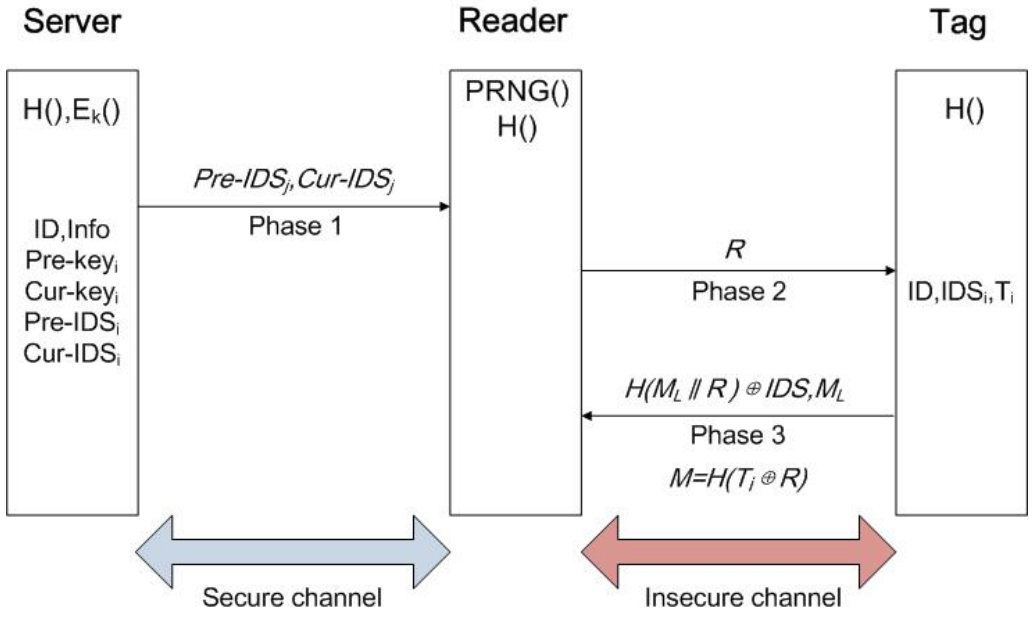

Figure 4. The Search Protocol

The execution access of the search protocol:

Step1: Server→Reader: Pre-IDS_j, Cur-IDS_j

The Server chooses the ID of a specific tag (ID_i) and sends Pre-IDS_j, Cur-IDS_j to the fixed reader.

Step2: Reader→Tag: R

After receiving Pre-IDS_j, Cur-IDS_j from the server, the reader would store Pre-IDS_j, Cur-IDS_j in its memory and generate a random R, then send R to tags.

Step3: Tag→Reader: $H(M_L \| R) \oplus IDS$, M_L

After receiving R, each tag near the reader should calculate $M = H(T \oplus R)$ and $\alpha = H(M_L \| R) \oplus ID$, then send α and M_L back to the reader. Subsequently the tag should calculate $T_{i+1} = M \oplus \alpha$ and save T_{i+1} in its memory. Especially, we use $H(T \oplus R)$ to substitute pseudo random number of the tag.

After receiving $H(M_L \| R) \oplus ID$ from each tag, the reader should calculate $IDS' = H(M_L \| R) \oplus (H(M_L \| R) \oplus IDS)$. If IDS' equals to Cur-$IDS_j$, the specific tag is found; or IDS' equals to Pre-IDS_j, the specific tag is found also, but in the last authentication access, the tag has not updated key and IDS successfully for some reason.

3.4. Security Analysis of this Search Protocol

We would analyze this protocol to evaluate whether it meets the security requirements as follows:

(1) Tag untraceability

An adversary could eavesdrop the response message ($H(M_L \| R) \oplus IDS, M_L$) from a tag, and analyze the information carefully and try to detect the user's location privacy by tracking the tag. Because the tag generates a new substituted random number $M = H(T \oplus R)$ during each authentication access, and updates $T_{i+1} = M \oplus (H(M_L \| R) \oplus IDS)$ in the step2, so the adversary cannot differentiate which tag does the response from the message ($H(M_L \| R) \oplus IDS, M_L$). So this protocol can meet tag untraceability.

(2) Tag information protection

Because the information of an ID (Info) stores in the backend server, an adversary cannot acquire the information of the ID. So this protocol can meet tag information protection.

(3) Spoofing attack

An adversary feigns a legitimate reader which sends a query with R to tags through the forward channel, and obtains the response of a tag ($H(M_L \| R) \oplus IDS, M_L$). In the next search access, when a legitimate reader sends a query with R', the adversary feigns the tag and responds the legitimate reader with the obtained message ($H(M_L \| R) \oplus IDS, M_L$) through the backward channel. However, the reader generates a new random number during each access, that is to say, $R \neq R'$, so the adversary cannot perform tag impersonation attack.

(4) Denial of Service (DoS) attack

As pseudonym IDS of a tag is mutative, even if loss of message, power failure or loss of connection with the backend server happens during an authentication access, it will lead to dy-synchronization between the backend server and the tag, and this protocol can solve this problem in the next search access by transmitting pseudonym Pre-IDS and Cur-IDS. So this search protocol can shield DoS attack well.

(5) Privacy of search result

This protocol can protect the search result of a reader. Because all tags nearby the reader respond to the request, an adversary cannot learn whether the mobile reader found a specific tag or not. Even if the specific tag itself cannot know whether the reader wants to find it or not, Since each tag would calculate $H(M_L \| R) \oplus IDS$ of its own and send $H(M_L \| R) \oplus IDS$ to the reader.

4. A RFID Search Protocol based on Dynamic ID Scheme for Mobile Reader

To solve the security and privacy problem in RFID tag search systems, many search protocols were proposed recently [9-15], We would propose a RFID search protocol based on dynamic ID scheme for mobile reader as follows. The notation used in this protocol refers to Section 3.1.

4.1. Assumptions

(1) The channel between the server and a reader is assumed insecure for wireless connection, and the channel between a reader and a tag is assumed insecure either, we assume that an adversary could observe and manipulate communications between insecure channels.

(2) The resources of each passive tag are constrained. In this protocol, each tag only needs to have a one-way hash function H( ), XOR operation capability and concatenation operation capability.

(3) A tag is not vulnerable to compromised with an adversary, that is to say, the adversary cannot acquire the inner information of the tag.

(4) The one-way hash function H( ) is secure enough agaist brute exhaustive search from an adversary.

4.2. The Execution Access of the Proposed Search Protocol

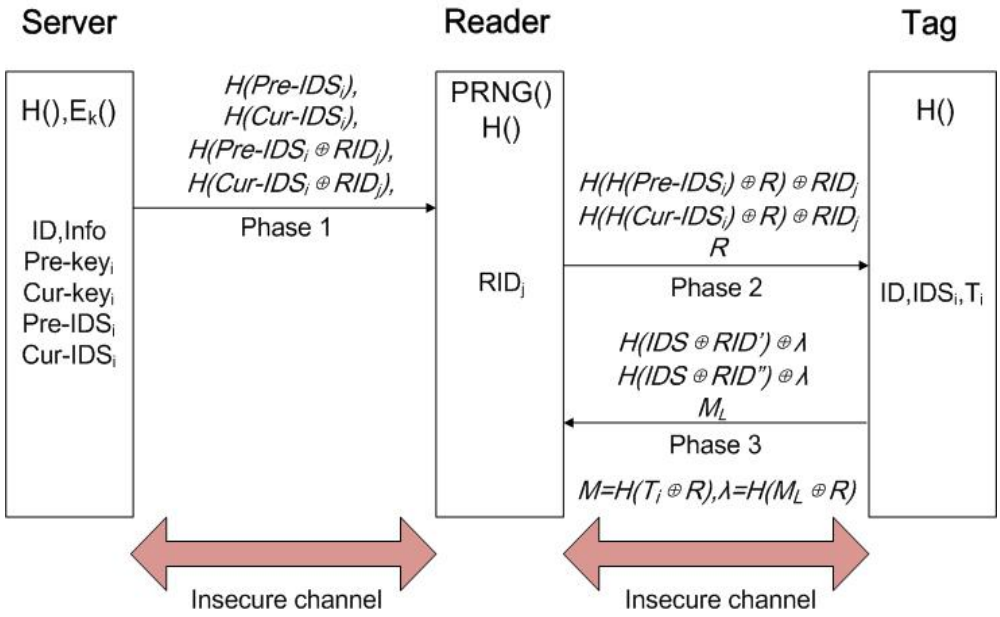

Figure 5. The Proposed Search Protocol

The execution access of the proposed search protocol:

Step1: Server→Reader: $H(Pre\text{-}IDS_i)$, $H(Cur\text{-}IDS_i)$, $H(Pre\text{-}IDS_i \oplus RID_j)$, $H(Cur\text{-}IDS_i \oplus RID_j)$

The Server chooses the ID of specific tag (ID_i) and calculates $H(Pre\text{-}IDS_i)$, $H(Cur\text{-}IDS_i)$, $H(Pre\text{-}IDS_i \oplus RID_j)$, $H(Cur\text{-}IDS_i \oplus RID_j)$, then sends $H(Pre\text{-}IDS_i)$, $H(Cur\text{-}IDS_i)$, $H(Pre\text{-}IDS_i \oplus RID_j)$, $H(Cur\text{-}IDS_i \oplus RID_j)$ to the reader (RID_j).

Step2: Reader→Tag: $H(H(Pre\text{-}IDS_i) \oplus R) \oplus RID_j$, $H(H(Cur\text{-}IDS_i) \oplus R) \oplus RID_j$, R

After receiving $H(Pre\text{-}IDS_i)$, $H(Cur\text{-}IDS_i)$, $H(Pre\text{-}IDS_i \oplus RID_j)$, $H(Cur\text{-}IDS_i \oplus RID_j)$ from the server, the reader would store $H(Pre\text{-}IDS_i \oplus RID_j)$, $H(Cur\text{-}IDS_i \oplus RID_j)$ in its memory and generate a random R, then calculate $H(H(Pre\text{-}IDS_i) \oplus R) \oplus RID_j$, $H(H(Cur\text{-}IDS_i) \oplus R) \oplus RID_j$ and send $H(H(Pre\text{-}IDS_i) \oplus R) \oplus RID_j$, $H(H(Cur\text{-}IDS_i) \oplus R) \oplus RID_j$, R to tags.

Step3: Tag→Reader: $H(IDS \oplus RID') \oplus \lambda$, $H(IDS \oplus RID'') \oplus \lambda$, M_L

After receiving $H(H(Pre\text{-}IDS_i) \oplus R) \oplus RID_j$, $H(H(Cur\text{-}IDS_i) \oplus R) \oplus RID_j$, R from the reader, each tag near the reader should calculate $M = H(T \oplus R)$ firstly, then calculate $RID' = H(H(IDS) \oplus R) \oplus (H(H(Cur\text{-}IDS_i) \oplus R) \oplus RID_j)$ and $RID'' = H(H(IDS) \oplus R) \oplus (H(H(Pre\text{-}IDS_i) \oplus R) \oplus RID_j)$, subsequenty calculate $\lambda = H(M_L \oplus R)$, $H(IDS \oplus RID') \oplus \lambda$, $H(IDS \oplus RID'') \oplus \lambda$, then send $H(IDS \oplus RID') \oplus \lambda$, $H(IDS \oplus RID'') \oplus \lambda$, M_L to the reader. Subsequently the tag should calculate $T_{i+1} = M \oplus \alpha$ and save T_{i+1} in its memory. Especially, we use $H(T \oplus R)$ to substitute pseudo random number of the tag.

After receiving $H(IDS \oplus RID') \oplus \lambda$, $H(IDS \oplus RID'') \oplus \lambda$, M_L from each tag, the reader should calculate $H(M_L \oplus R)$, then calculate $V_1 = H(M_L \oplus R) \oplus (H(IDS \oplus RID') \oplus \lambda)$ and $V_2 = H(M_L \oplus R) \oplus (H(IDS \oplus RID'') \oplus \lambda)$. If $V_1 = H(Cur\text{-}IDS_i \oplus RID_j)$, the specific tag is found; or the reader checks whether $V_2 = H(Pre\text{-}IDS_i \oplus RID_j)$ or not, if $V_2 = H(Pre\text{-}IDS_i \oplus RID_j)$, the specific tag is found, but in the previous authentication access, the tag has not updated IDS successfully for some reason. If $V_1 <> H(Cur\text{-}IDS_i \oplus RID_j)$ and $V_2 <> H(Pre\text{-}IDS_i \oplus RID_j)$, then the tag is not the specific tag that the server would search.

4.3. Security Analysis of this Search Protocol

We would analyze this protocol to evaluate whether it meets the security requirements as follows:

(1) Tag untraceability

An adversary could eavesdrop the response message ($H(IDS \oplus RID') \oplus \lambda$, $H(IDS \oplus RID'') \oplus \lambda$, M_L) from a tag, and analyze the information carefully and try to detect the user's location privacy by tracking the tag. Because the tag generates a new substitute random number M during each access, so the adversary cannot differentiate which tag does the response from the message ($H(IDS \oplus RID') \oplus \lambda$, $H(IDS \oplus RID'') \oplus \lambda$, M_L). So this protocol can meet tag untraceability.

(2) Reader untraceability

Each message from a mobile reader is changed in every session, since a mobile reader generates a fresh random R in each session and RID of the mobile reader is not transmitted in plaintext. So an adversary cannot trace the movements of a mobile reader holder.

(3) Tag information protection

Because the information of an ID (Info) stores in the backend server and is not transmitted through the channel from the backend server to the reader, an adversary cannot acquire the information of the ID. So this protocol can meet tag information protection.

(4) Replay attack

In each session, the mobile reader would generate a new random R and a tag would generate a new substitute random M, so replay attack can be prevented in this protocol due to the message transmitted for each access is different. Different value of $H(M_L \oplus R)$ is utilized in individual access and M_L plays a key role in providing different value of $H(M_L \oplus R)$ to conceal $H(IDS \oplus RID')$, $H(IDS \oplus RID'')$ of the tag. An adversary cannot acquire $H(\ )$ so as to calculate $H(M_L \oplus R)$, so it is impossible for the adversary to perform replay attack.

(5) Denial of Service (DoS) attack

This protocol is based on dynamic ID mechanism, for solving the problem of Denial of Service attack in an execution access of corresponding authentication protocol of this RFID system, the shared value Pre-IDS and Cur-IDS between the backend server and the tag should be considered, so $H(Pre\text{-}IDS_i)$, $H(Cur\text{-}IDS_i)$, $H(Pre\text{-}IDS_i \oplus RID_j)$, $H(Cur\text{-}IDS_i \oplus RID_j)$ have been calculated, $H(Pre\text{-}IDS_i \oplus RID_j)$, $H(Cur\text{-}IDS_i \oplus RID_j)$ are regarded as authentication secret. Even if the backend server and the tag have lost synchronization for some reason in previous authentication access, the tag can be found successfully.

(6) Privacy of search result

This protocol can protect the search result of a mobile reader. Because all tags nearby the mobile reader respond to the request, an adversary cannot learn whether the mobile reader

found a specific tag or not. Even if the specific tag itself cannot know whether the mobile reader wants to find it or not, Since T_i does not know the identifier RID_j of the reader, T_i cannot decide whether the RID' or RID" which is extracted from the received broadcasted message is correct or not.

5. Conclusion

Effective tag search is a necessary tool in many RFID applications with a large number of tagged items. In this paper, we first proposed a set of protocols for a RFID reader to search for a particular tag based on its identity, these protocols incorporate anti-asynchronization mechanisms. We analyzed their resistances of those protocols to common security and privacy attacks. We concluded that the proposed protocols are both secure and private. In addition, the system scalability issues are well solved in this paper, all these proposed protocols only require O(1) work to search and identify a tag in the reader and is suitable for the low-cost RFID systems.

Acknowledgements

This work was supported in part by Heilongjiang Province Science and Technology Research Grant of the Education Department No. 12533002.

References

[1] L. Wang, X. Yi, C. Lv and Y. Guo, "Security Improvement in Authentication Protocol for Gen-2 Based RFID System", Journal of Convergence Information Technology, AICIT, vol.6, no.1, pp.157-169, **(2011)**.
[2] Ari Juels, "RFID security and privacy: a research survey", Journal of Selected Areas in Communications, Institute of Electrical and Electronics Engineers, vol. 24, no. 2, **(2006)**, pp. 381-394.
[3] M.-H. Yang, "Controlled Delegation Protocol in Wireless RFID Networks", Journal on Wireless Communications and Networking, Journal on Wireless Communications and Networking Press, **(2010)**, pp. 1-13.
[4] M. Son, Y. Lee and C. Pyo, "Design and Implementation of Mobile RFID Technology in the CDMA Networks", Proceedings of the 8th International Conference Advanced Communication Technology (ICACT '06), **(2006)**, pp. 1033-1036.
[5] N. Park, H. Kim, K. Chung and S. Sohn, "Design of an Extended Architecture for Secure Low-cost 900MHz UHF Mobile RFID Systems", Proceedings of the 10th IEEE International Symposium on Consumer Electronics (ISCE '06), **(2006)**, pp. 666-671.
[6] K. Penttila, N. Pere, M. Soini, L. Syd Anheimo and M. Kivikoski, "Use and Interface Definition of Mobile RFID Reader Integrated in a Smart Phone", Proceedings of the 9th International Symposium on Consumer Electronics (ISCE '05), **(2005)**, pp. 353-358.
[7] H. Jialiang, O. Dantong and Y. Yuxin, "An Efficient Lightweight RFID Authentication Protocol for Low-cost Tags", Advances in Information Sciences and Service Sciences, AICIT, vol. 3, no. 9, , pp. 331-338.
[8] H. Jialiang, O. Dantong and X. Youjun, "An Efficient RFID Authentication Protocol Supporting Tag Ownership Transfer", International Journal of Advancements in Computing Technology, AICIT, vol. 4, no. 4, **(2012)**, pp. 244-253.
[9] J. Young Chun, J. Yeon Hwang and D. Hoon Lee, "RFID tag search protocol preserving privacy of mobile reader holders", IEICE Electronics Express, Electronics Express, vol. 8, no. 2, **(2011)**, pp. 50-56.
[10] Y. Zuo, "Secure and private search protocols for RFID systems", Information Systems Frontiers, Springer, vol. 12, **(2010)**, pp. 507-519.
[11] M. E. Hoque, F. Rahman, S. I. Ahamed, J. H. Park, "Enhancing Privacy and Security of RFID System with Serverless Authentication and Search protocols in Pervasive Environments", Wireless Personal Communications, Wireless Personal Communications Press, vol. 55, no. 1, **(2009)**, pp. 65-79.
[12] C. Tan, B. Sheng and Q. Li, "Secure and Serverless RFID Authentication and Search Protocols", IEEE Transfer, Wireless Communication, vol. 7, no. 4, **(2008)**, pp. 1400-1407.
[13] S. I. Ahamed, F. Rahman, E. Hoque, F. Kawsar and T. Nakajima, "S3PR: Secure Serverless Search Protocols for RFID", Proceedings of the 2th International Conference on Infrormation Security and Assurance, **(2008)**, pp. 187-192.

[14] T. Y. Won, J. Y. Chun and D. H. Lee, "Strong Authentication Protocol for Secure RFID Tag Search Without Help of Central Database", Proceedings of 2008 IEEE/IFIP International Conference on Embedded and Ubiquitous Computing, vol. 2, **(2008)**, pp. 153-158.
[15] S. I. Ahamed, F. Rahman, E. Hoque, F. Kawsar and T. Nakajima, "Secure and Efficient Tag Searching in RFID Systems using Serverless Search Protocol", Security and Its Applications, Security and Its Applications Press, vol. 2, no. 4, **(2008)**, pp. 57-66.

Authors

He Jialiang borned in 1977, received the PhD degree in computer software and theory from Jilin University of China in 2012 and the Master degree in computer application from Jilin University of China in 2004. Now he is an associate professor at College of Information and Communication Engineering, Dalian Nationalities University, China. His papers have been published in some well-known international Journals and IEEE conferences. His main interests include Mobile Internet, Internet of Things, and Intelligent Business Information Processing.

Xu Zhiqiang borned in 1981, received the Bachelor degree in communication Engineering from Communication University of China in 2004 and the Master degree in Electronics and Communication Engineering from Communication University of China in 2012. At present, he is an assistant professor of Communication & Media Institute of Sichuan, China. He is experienced the fields of Mobile Internet, Internet of Things, Intelligent Information Processing, etc., he also is a candidate of MSc of Technopreneurship & Innovation Program in Nanyang Technological University in Singapore.