International Journal of Hybrid Information Technology
Vol.7, No.2 (2014), pp.139-150
http://dx.doi.org/10.14257/ijhit.2014.7.2.14

A Hash-based RFID Search Protocol for Mobile Reader

He Jialiang[1], Xu Youjun[2] and Xu Zhiqiang[3]

*[1]*College of Information and Communication Engineering, Dalian Nationalities University, China*
[2]*College of Computer Science and Information Technology, Daqing Normal University, China*
[3]*Department of digital media technology, Sichuan College of Media and Communications, China*

urchin2012@sina.com; xu_youjun@sohu.com; starsep928@yahoo.com.cn

Abstract

Mobile readers are used more and more remarkably, so a persistent connection between a backend server and mobile readers cannot be guaranteed, it brings higher security requirements for RFID systems. RFID search protocol which is used to find specific tags has many applications such as inventory management, supply chain management. In this paper, a hash-based RFID search protocol for mobile readers is proposed, it can meet all known major attacks in RFID systems, and it can protect the privacy of mobile reader holders especially.

Keywords*: RFID; Search Protocol; Mobile Reader*

1. Introduction

Radio Frequency Identification (RFID) is a technology which is used to automatically identify objects by wireless scanning without manual intervention; it has been used in various real-life application fields such as supply chain management, transportation, e-payment system, patient medical care. Comparing with traditional barcode technology, it has many advantages. A typical RFID system consists 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 [1]. So designing an efficient and low-cost security scheme for RFID systems becomes a challenging and important research object.

Recently, combining mobile technology with traditional RFID systems, through the integration of reading chips, PDA, and mobile devices, hence mobile RFID, such mobile readers are used more and more remarkably [2-5], so a persistent connection between a backend server and mobile readers cannot be guaranteed, it brings higher security requirements for RFID systems.

Many RFID security protocols have been proposed recently. Usually, beyond RFID authentication protocols, the requirements for RFID systems from various application fields call for more cryptographic protocols, for instance, RFID search protocol. RFID search

ISSN: 1738-9968 IJHIT

protocol which is used to find specific tags has many applications such as inventory management, supply chain management.

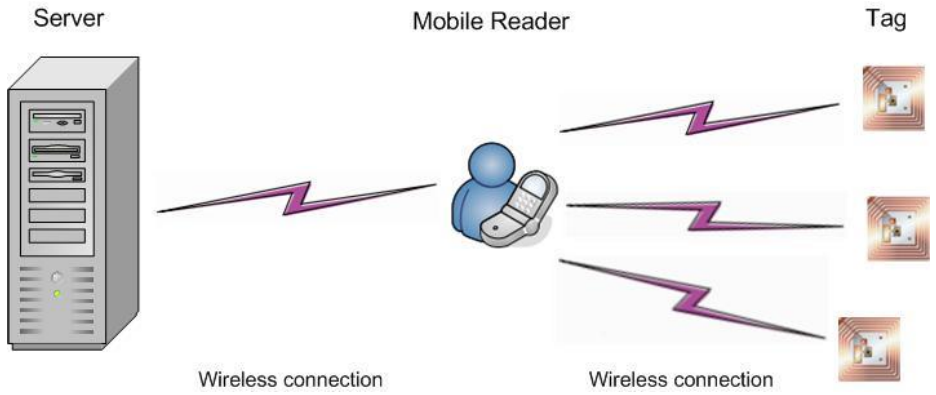

Figure 1. Wireless RFID environment [6]

The main contribution of this paper is to propose a hash-based RFID search protocol for mobile readers. The rest of this paper is organized as follows. In the second section, security requirements for RFID search protocols design are generalized. In the third section, the related research work is introduced. In the forth section, a new hash-based RFID search protocol is proposed. In the fifth section, security properties of the proposed protocol are analyzed. Finally, the conclusion of this paper is provided in the sixth section.

2. Security Requirements for RFID Search Protocols

Mobile RFID systems are confronted with more kinds of security threats than fixed RFID systems, for a search protocol of mobile RFID systems; it should meet security requirements as follows:

(1)Tag untraceability

If responding message from a tag always contains a changeless value, namely the response are linkable to each other or distinguishable from those of other tags, an adversary can recognize and locate the tag by intercepting and analyzing. That is to say, the location privacy of the user (human being, or animal, or article) that attached by the tag can be traced [7].

(2)Reader untraceability

The privacy of mobile holders should be considered. Since users commonly handle mobile readers while RFID-tagged objects are attached to goods or products in RFID tag search systems. Moreover, the signal strength of a reader is much stronger than that of a tag. So a message from a reader can be more easily eavesdropped than a message from a tag [8]. If querying message from a mobile reader always contains a changeless value, an adversary can recognize and locate the reader by intercepting and analyzing. That is to say, the location privacy of the holder that attached by the reader can be traced.

(3)Tag information protection

A tag is always attached to an article, or a human being, or an animal, so through all the execution access of a search protocol, an illegimate user should not acquire the legimate holder’s detailed information.

(4)Replay attack

Such an attack in which an adversary repeatedly launches a message that obtained by eavesdropping or intercepting from a regular communication between a reader and a tag during a normal search access.

(5)Denial of Service (DoS) attack

According to whether the backend server and a tag update the identifier or not in an entire authentication access, RFID authentication protocols are divided into dynamic ID mechanism and static ID mechanism. For the protocols based on dynamic ID mechanism, in a execution access of corresponding authentication protocol of this RFID system, if an adversary disturbs the communications between a reader and a tag by means of intercepting or blocking messages transmitted, the secret value that shared between the server and the tag cannot be updated successfully in this authentication access, it would cause losing synchronization between the backend server and the tag, if this RFID system search for this specific tag at that time, the search process maybe fail, so the design of a search protocol should solve this problem.

(6)Privacy of search result

The other privacy requirement to be considered is the search result of a mobile reader. It is undesirable to reveal the search result of a mobile reader. In some circumstances to an adversary, it might be useful information whether a mobile reader holder found a particular tag or not [8]. So a well designed search protocol should protect privacy of search result from an illegal user.

3. Related work

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 wildly.

To solve the security and privacy problems in RFID tag search systems, many search protocols have been proposed recently [8-17].

3.1 Review of Tan *et al.*'s RFID search protocol

In 2008, Tan *et al.* proposed server-less RFID search protocol [16].

However, there are two shortcomings of security and performance in Tan *et al.*'s mechanism as follows:

(1)In the step1 of Tan *et al.*'s server-less RFID search protocol request message from a reader always contains a changeless value R_i, namely an adversary can recognize and locate the reader by intercepting and analyzing. That is to say, the location privacy of the user that attached by the reader could be traced.

(2)Low-cost passive tags have constraint requirements of limited resources, using less hardware cost is an important research object, we can see that using pseudo random number generator in tags leads to extra hardware cost, usually, about 700-800 logic gates is needed to implementing a pseudo random number generator. More seriously, these two protocols use two hash functions each. So it is unpractical for low-cost RFID systems.

3.2 Review of Ji *et al.*'s RFID search protocol

In 2008, Ji *et al.* proposed server-less RFID search protocol [17].

However, there are two shortcomings of security and performance in Ji *et al.*'s mechanism as follows:

(1)In Ji *et al.*'s server-less RFID search protocol, request message from a reader always contains a changeless value R_i, namely an adversary can recognize and locate the reader by intercepting and analyzing. That is to say, the location privacy of the user that attached by the reader could be traced.

(2)Low-cost passive tags have constraint requirements of limited resources, using less hardware cost is an important research object, and we can see that using pseudo random number generator in tags leads to extra hardware cost.

A typical server-less search protocol [8] in 2011 is introduced as follows:

3.3 Review of Chun *et al.*'s RFID search protocol

Table 1. The notations used in 3.3 section

Symbol	Meaning
$\oplus$	XOR operator
ID	The unique identifier of a tag (The length is l)
RID	The unique identifier of a reader (The length is l)
PRNG()	The pseudo random number generator (The length of output is l_R, $l_R < l$)
N_T	Random number of tag
N_R	Random number of reader
Ti	Secret value between server and tag
SE= (E,D)	A symmetric encryption algorithm
$E_K(m)$	An encryption algorithm associated to a key K
$D_K(m)$	A decryption algorithm associated to a key K

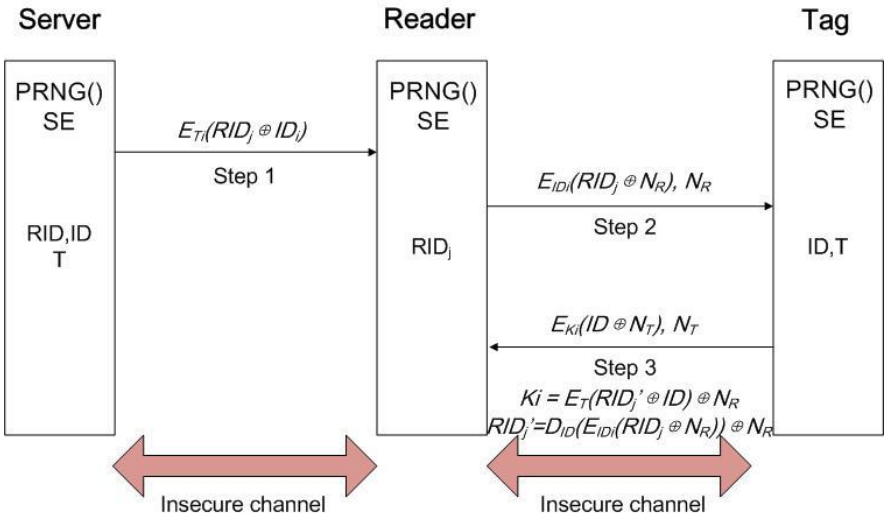

Figure 2. The original search protocol

The execution access of the original search protocol:

Step1: Server→Reader: $E_{Ti}(RID_j \oplus ID_i)$

The server chooses the ID of specific tag(ID_i) and calculates $E_{Ti}(RID_j \oplus ID_i)$, then sends $E_{Ti}(RID_j \oplus ID_i)$ to the reader (RID_j).

Step2: Reader→Tag: $E_{IDi}(RID_j \oplus N_{R)}$, N_R

After receiving $E_{Ti}(RID_j \oplus ID_{i)}$ from the server, the reader would store $E_{Ti}(RID_j \oplus ID_i)$ in its memory and generate a random N_R, then calculate $E_{IDi}(RID_j \oplus N_R)$ and send $E_{IDi}(RID_j \oplus N_R)$, N_R to tags.

Step3: Tag→Reader: $E_{Ki}(ID \oplus N_R)$, N_T

After receiving $E_{IDi}(RID_j \oplus N_R)$, N_R from the reader, each tag near the reader should calculate $RID_j' = D_{ID}(E_{IDi}(RID_j \oplus N_R) \oplus N_R$, then calculate $K_i = E_T(RID_j' \oplus ID) \oplus N_R$, subsequently generate a random N_T and calculate $\lambda = E_{Ki}(ID \oplus N_T)$, then send $E_{Ki}(ID \oplus N_T)$, N_T to the reader.

After receiving $E_{Ki}(ID \oplus N_T)$, N_T from each tag, the reader should calculate $K_i^* = E_{Ti}(RID_j \oplus ID_i) \oplus N_R$ and $ID' = D_{Ki*}(E_{Ki}(ID \oplus N_R)) \oplus N_R$. If $ID_i = ID'$, the specific tag is searched, or the tag is not the specific tag that the server would search.

This protocol is simple and clear, but there are two problems as follows:

(1)Losing synchronization between the server and a tag

In a execution access of corresponding authentication protocol of this RFID system, if an adversary disturbs the communications between a reader and a tag by means of intercepting or blocking messages transmitted, the secret value T that shared between the server and the tag maybe not be updated successfully in this authentication access, it could cause losing synchronization between the backend server and the tag, so in this search protocol, T_i in $E_{Ti}(RID_j \oplus ID_i)$ is not equal to T stored in the tag, the legitimate tag cannot be searched by the backend server again.

(2)Computation cost of a tag is high

In this search protocol, the encryption method between the server and a tag use symmetrical encryption function like AES. Usually, the one-way hash function has lower cost than symmetrical encryption function, so this search protocol and its corresponding authentication protocol are not suitable for the low-cost RFID system.

For solving these two problems, we propose a new RFID search protocol for mobile readers based on one-way hash function.

4. A New RFID Search Protocol based on One-way Hash Function

4.1 Notation

Table 2. The notations used in this protocol

Symbol	Meaning
$\oplus$	XOR operator
$\|\|$	Concatenation operator
ID	The unique identifier of a tag (The length is l)
RID	The unique identifier of a reader (The length is l)
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 $l_R < l$)
S_{old}	Old secret value
S_{new}	New secret value
N_T	Random number of tag
$N_{R(old)}$	Old random number of reader
$N_{R(new)}$	New random number of reader
N_{DB}	Random number of server databases

4.2 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 ageist brute exhaustive search from an adversary.

4.3 Initialization phase

In this phase, the backend server needs to have a one-way hash function H(), A pseudo random number generator PRNG(), and stores Table RID, Table ID; A reader needs to have a one-way hash function H(), A pseudo random number generator PRNG(), and stores its own RID; A tag needs to have a one-way hash function H(), A pseudo random number generator PRNG(), and stores its own ID and secret value S.

4.4 Search protocol

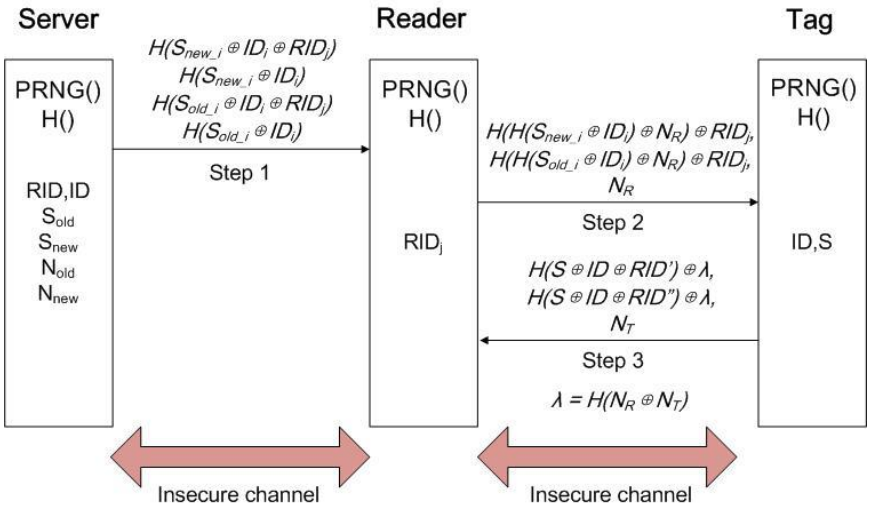

Figure 4. The proposed search protocol

The execution access of the proposed protocol:

Step1: Server→Reader: $H(S_{new\_i} \oplus ID_i \oplus RID_j)$, $H(S_{new\_i} \oplus ID_i)$, $H(S_{old\_i} \oplus ID_i \oplus RID_j)$, $H(S_{old\_i} \oplus ID_i)$

The Server chooses the ID of specific tag(ID_i) and calculates $H(S_{new\_i} \oplus ID_i \oplus RID_j)$, $H(S_{new\_i} \oplus ID_i)$, $H(S_{old\_i} \oplus ID_i \oplus RID_j)$, $H(S_{old\_i} \oplus ID_i)$, subsequently sends $H(S_{new\_i} \oplus ID_i \oplus RID_j)$, $H(S_{new\_i} \oplus ID_i)$, $H(S_{old\_i} \oplus ID_i \oplus RID_j)$, $H(S_{old\_i} \oplus ID_i)$ to the reader (RID_j).

Step2: Reader→Tag: $H(H(S_{new\_i} \oplus ID_i) \oplus N_R) \oplus RID_j$, $H(H(S_{old\_i} \oplus ID_i) \oplus N_R) \oplus RID_j$, N_R

After receiving $H(S_{new\_i} \oplus ID_i \oplus RID_j)$, $H(S_{new\_i} \oplus ID_i)$, $H(S_{old\_i} \oplus ID_i \oplus RID_j)$, $H(S_{old\_i} \oplus ID_i)$ from the server, the reader would store $H(S_{new\_i} \oplus ID_i \oplus RID_j)$ and $H(S_{old\_i} \oplus ID_i \oplus RID_j)$ in its memory and generate a random N_R, then calculate $H(H(S_{new\_i} \oplus ID_i) \oplus N_R) \oplus RID_j$, $H(H(S_{old\_i} \oplus ID_i) \oplus N_R) \oplus RID_j$ and send $H(H(S_{new\_i} \oplus ID_i) \oplus N_R) \oplus RID_j$, $H(H(S_{old\_i} \oplus ID_i) \oplus N_R) \oplus RID_j$, N_R to tags.

Step3: Tag→Reader: $H(S \oplus ID \oplus RID') \oplus \lambda$, $H(S \oplus ID \oplus RID'') \oplus \lambda$, N_T

After receiving $H(H(S_{new\_i} \oplus ID_i) \oplus N_R) \oplus RID_j$, $H(H(S_{old\_i} \oplus ID_i) \oplus N_R) \oplus RID_j$, N_R from the reader, each tag near the reader should calculate $H(H(S \oplus ID) \oplus N_R)$ firstly, then calculate $RID' = H(H(S \oplus ID) \oplus N_R) \oplus H(H(S_{new\_i} \oplus ID_i) \oplus N_R) \oplus RID_j$ and $RID'' = H(H(S \oplus ID) \oplus N_R) \oplus H(H(S_{old\_i} \oplus ID_i) \oplus N_R) \oplus RID_j$, subsequently generate a random N_T and calculate $\lambda = H(N_R \oplus N_T)$, $H(S \oplus ID \oplus RID') \oplus \lambda$, $H(S \oplus ID \oplus RID'') \oplus \lambda$, then send $H(S \oplus ID \oplus RID') \oplus \lambda$, $H(S \oplus ID \oplus RID'') \oplus \lambda$, N_T to the reader.

After receiving $H(S \oplus ID \oplus RID') \oplus \lambda$, $H(S \oplus ID \oplus RID'') \oplus \lambda$, N_T from each tag, the reader should calculate $H(N_R \oplus N_T)$, then calculate $\alpha = H(N_R \oplus N_T) \oplus (H(S \oplus ID \oplus RID') \oplus \lambda)$ and $\beta = H(N_R \oplus N_T) \oplus (H(S \oplus ID \oplus RID'') \oplus \lambda)$. If $\alpha = H(S_{new\_i} \oplus ID_i \oplus RID_j)$, the specific tag is searched, or the reader checks whether $\beta = H(S_{old\_i} \oplus ID_i \oplus RID_j)$ or not, if $\beta = H(S_{old\_i} \oplus$

$ID_i \oplus RID_j$), the specific tag is searched, but in the previous authentication access, the tag has not updated S successfully for some reason. If $\alpha <> H(S_{new\_i} \oplus ID_i \oplus RID_j)$ and$\beta <> H(S_{old_i} \oplus ID_i \oplus RID_j)$, then the tag is not the specific tag that the server would search.

5. Security Analysis

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 $H(H(S_{new\_i} \oplus ID_i) \oplus N_R) \oplus RID_j$, $H(H(S_{old\_i} \oplus ID_i) \oplus N_R) \oplus RID_j$, N_R 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 random number N_R during each access, so the adversary cannot differentiate which tag does the response from the message $H(H(S_{new\_i} \oplus ID_i) \oplus N_R) \oplus RID_j$, $H(H(S_{old\_i} \oplus ID_i) \oplus N_R) \oplus RID_j$, N_R. 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 N_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) is stored 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 N_R and a tag would generate a new random N_T, so replay attack can be prevented in this protocol due to the message transmitted for each access is different. Different value of $H(N_R \oplus N_T)$ is utilized in individual access and N_T plays a key role in providing different value of $H(N_R \oplus N_T)$ to conceal $H(S \oplus ID \oplus RID')$, $H(S \oplus ID \oplus RID'')$ of the tag. An adversary cannot acquire H() so as to calculate $H(N_R \oplus N_T)$, 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 a execution access of corresponding authentication protocol of this RFID system, the shared value S_{old} and S_{new} between the backend server and the tag should be considered, so $H(S_{new\_i} \oplus ID_i \oplus RID_j)$, $H(S_{new\_i} \oplus ID_i)$, $H(S_{old\_i} \oplus ID_i \oplus RID_j)$, $H(S_{old\_i} \oplus ID_i)$ have been calculated, $H(S_{new\_i} \oplus ID_i \oplus RID_j)$ and $H(S_{old\_i} \oplus ID_i \oplus RID_j)$ 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 searched 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 him 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.

Table 3 indicates a comparison of results among our search protocol and the related search protocols [8, 16, 17] in terms of security.

Table 3. Comparison of security

Security requirement	[8]	[16]	[17]	New
Tag untraceability	O	O	O	O
Reader untraceability	O	X	X	O
Tag information protection	O	O	O	O
Spoofing attack	O	X	X	O
Replay attack	O	O	O	O
DoS attack	X	O	O	O
Privacy of search result	O	X	X	O
Based on dynamic ID	X	X	X	O

'O' denotes satisfied, 'X' denotes not satisfied

6. Conclusion

Mobile RFID systems suffer from more privacy and security problems. Therefore, in this paper, we analyze security requirements for RFID search protocols firstly; then pointing out the shortcomings of one typical RFID search protocol; based on the analyzed result, a new RFID search protocol which meets the requirements for mobile readers is proposed. The careful security analysis shows that this protocol has well security properties.

Acknowledgements

This work was partially supported by Research Projects of State Ethnic Affairs Commission No.12DLZ001; Heilongjiang Province Science and Technology Research Grant of the Education Department No.12533002.

References

[1] A. 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.
[2] 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.
[3] 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.
[4] 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.
[5] 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.
[6] H. Jialiang, O. Dantong, B. Tian and Z. Liming, "A Lightweight RFID Authentication Protocol for Mobile Reader", International Journal of Digital Content Technology and its Applications, AICIT, vol. 6, no. 6, (**2012**) pp. 80-88.
[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, (**2011**) pp. 331-338.

[8] J. Y. Chun, J. Y. Hwang and D. H. Lee, "RFID tag search protocol preserving privacy of mobile reader holders", IEICE Electronics Express, Electronics Express, vol. 8, no. 2, (**2011**), pp. 50-56.
[9] 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, Int. J. Commun. Syst, vol. 25, (**2012**) pp. 376-385.
[10] Y. Zuo, "Secure and private search protocols for RFID systems", Information Systems Frontiers, Springer, vol. 12, (**2010**), pp. 507-519.
[11] Md. E. Hoque, F. Rahman, S. I. Ahamed and 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.
[16] 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.
[17] 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

He was born 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 Youjun

He was born in 1977, received the Master degree in computer application from Jilin University in 2005 and the PhD degree in computer software and theory from Jilin University in 2011. Now he is a lecturer at College of Computer Science and Information Technology, Daqing Normal University, China. His papers have been published in some well-known international Journals. His main interests include Automated Reasoning, Internet of Things.

Xu Zhiqiang

He was born in 1981, received the Master degree in Electronics & 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.

