Journal of Computing and Information Technology - CIT 23, 2015, 4, 295–302
doi:10.2498/cit.1002549

Analysis on the Performance of Server-less RFID Searching Protocol

Ping Huang, Haibing Mu and Fei Zeng

Beijing Key Laboratory of Communication and Information Systems, School of Electronic and Information Engineering, Beijing Jiaotong University, Beijing, China

Radio frequency identification (RFID) has spread into many fields. Its security and privacy has received more and more attention. Based on traditional authentication protocols, some other branches related to practical applications have been introduced including server-less authentication and searching protocols. The server-less searching protocol is extended from server-less authentication protocol and both of them are executed without the support from the backend servers. Through analyzing some proposed protocols, we found that the probabilistic tracking attack is one of the major threats on the server-less RFID security protocols. The probability of being tracked and the cost on computation are related with the probability of the undesired tag's response. Based on the analysis, a practical conclusion is given which can be used in most of the server-less RFID systems.

Keywords: RFID, server-less, authentication, searching, security

1. Introduction

Radio frequency identification (RFID) has been widely used in many fields, such as pharmaceuticals industry and logistics management. At present, RFID has been embedded into daily life. However, there is still hidden trouble in the security and privacy of RFID systems. Hence the authentication protocols have been presented by many researchers to guarantee the security and privacy involved in RFID systems.

At the beginning, the RFID security protocols were only used to check whether the tag is legal, i.e. one-way protocol. Afterwards, with deepening of understanding on the RFID system by malicious adversaries or users, readers can be utilized by them to violate the legal users' privacy. Considering this situation, a large amount of mutual authentication protocols were proposed. Based on these works, the grouping proof protocols were presented to ensure that some of the entities are scanned simultaneously. It is obvious that the security of these protocols is totally based on the central database. In other words, there has to be a central server connected with the readers constantly to realize a secure system. However, steady connection between the back-end database and the readers cannot be guaranteed in many practical scenarios, especially in the remote areas. Therefore, server-less security protocol is necessary. Among these server-less security protocols, the server-less RFID searching protocol is extended from the authentication protocol. The RFID searching protocol is used by the reader to determine whether the desired tag is in the group of tags.

The main contributions of this paper are: (i) the requirements for server-less RFID searching protocols are studied, (ii) the analysis of the relationship between the probabilistic tracking attack, the cost on computation and the parameter λ, and (iii) a conclusion is put forward in this section that can be used in most of the server-less RFID systems to optimize the performance of the systems.

2. Related Work

RFID technology firstly appeared during the World War II. Since then, it has been used in many practical fields. With its wide usage, RFID security is of the popular interest. The first approach to protect RFID users' privacy is

the implementation of "Kill" [5]. That means the Reader sends a command of kill the tag and the tag will be inactive forever. In this way, privacy can be well protected from an adversary's scanning the tag illegally. But the tag will never work anymore. Afterwards, according to the thought of cryptography presented by Shannon, a number of researchers came up with many RFID protocols for privacy and security of RFID system. Such is the Hash-Lock protocol [12, 13]. Weis S. A. et al. (2002) also described a new research direction in RFID for researchers with cryptography. A randomized Hash-Lock protocol [17] was put forward, and the authors said that low-cost Radio Frequency Identification (RFID) systems would become pervasive in our daily lives when affixed to everyday consumer items as "smart labels". It predicts that low-cost is important for RFID system's being applied in our daily life. The hash-chain protocol [10] can ensure forward-secure privacy, because hash-function has one-way property. In some of the early protocols, both of the parties might use security schemes with static IDs [8]. However, these security schemes have been proved to be insecure. Tsai et al. [16] presented their own dynamic ID scheme to achieve security and anonymity based on the work of Yoon et al. [18]. With the help of central database, most security requirements are realized by many protocols. In this section, a detailed introduction on sever-less protocols will be presented.

The idea of "server-less" was firstly shown by Tan et al. [15]. It was introduced in a practical scenario where a truck driver was dispatched to pick up some merchandise attached with RFID tags. Nevertheless the driver only has a PDA (Personal Digital Assistant) as a reader, without connection with central database for his remote location. Alternatively, it is to download the list of necessary information of the tags. But whether the PDA is stolen cannot be guaranteed. So an authentication protocol implemented only by readers is the best way to solve the problem. Tan et al. proposed several mutual authentication protocols and searching protocols without central database. Besides, they created a contact list which has been used in subsequent works. In 2008, some excellent protocols were presented by Ahamed et al. Some researchers put forward a server-less searching protocol and a server-less authentication protocol separately [1, 2]. These researches indicated that RFID security protocols without servers would be very meaningful for the development of RFID system [4]. The development of server-less RFID security scheme, analysis on security, privacy, anonymity, etc. has raised people's attention [11]. Then, in 2011, Myneni et al. [9] proposed an anonymous protocol while Kim et al. [6] added untraceability in their own protocol. Sundaresan et al. [14] combined server-less searching protocols with low-cost RFID tags, which can narrow the range of research and enhance practicability of protocols. Lee et al. [7] analyzed some previous works on the numerical values firstly. Then, they proposed their own protocols to try to enhance security and privacy.

Through analyzing the existing server-less protocols, we find that probabilistic tracking attack is a serious threat. We find out the key of probabilistic tracking attack and provide an effective solution to resist this attack.

3. Security Requirements on Sever-less RFID Searching Protocol

Server-less RFID protocol is usually operated in some remote area where the connection between the reader and the backend server may be not steady. This problem could influence the security of RFID systems which need continuous support from the servers

Besides forward security, privacy, anonymity and some other existing security targets for all RFID security protocols, some other requirements should be reached for server-less RFID searching protocol:

1. Higher stability of the reader. It means that to perform server-less RFID searching protocols, the readers' ability has to be much more robust to keep the systems steady.
2. Limited scalability of the system. A tag cannot join the process of operation of RFID searching protocol until the reader communicates with the trusted party, which means the scalability is strictly limited.
3. Limited recoverability of the tag. When a tag does not pass through the authentication between itself and its corresponding reader for a threshold times, the reader will keep the tag in record and it will not communicate with the tag. Only after the reader has

connected with the trusted party can the tag be authenticated by its reader.

Overall, high efficiency and security is the ultimate goal for a server-less RFID searching protocol.

4. Analysis of the Probabilistic Tracking Attack

Most of the server-less RFID searching protocols can be summarized to the framework below (Figure 1). The protocol proposed by Lee et al. (Figure 2) is taken as an example to demonstrate our analysis more clearly in this paper.

1. The reader broadcasts the active information which includes a random number, its identity and an encryption result of the fresh information and the shared keys with the desired tag to all the tags.
2. The desired tag will give a response with probability of 1 while the undesired tags will reply with a probability of λ.
3. When the reader receives the responses from the tags, it will check and reply to the tags.
4. The desired tag will check the message from the reader to authenticate it.

4.1. Notations in Lee et al.'s Server-less Protocols

In the paper, we created some new notations besides the ones used in Lee et al.'s server-less authentication and searching protocols. The notations are shown in Table 1.

4.2. Lee et al.'s Server-less Searching Protocol

Lee et al.'s protocol is used in the scenario when there is no continuous support from the server, which is shown in Figure 2 in details.

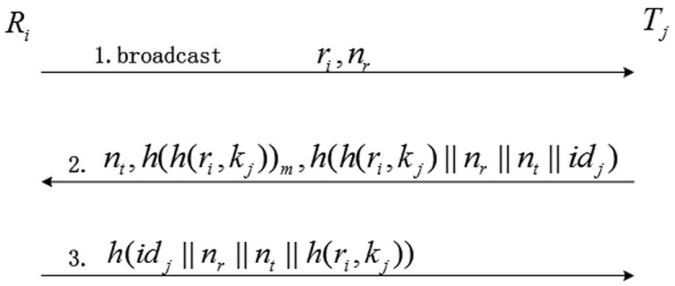

Figure 1. Framework for most of the server-less RFID searching protocols.

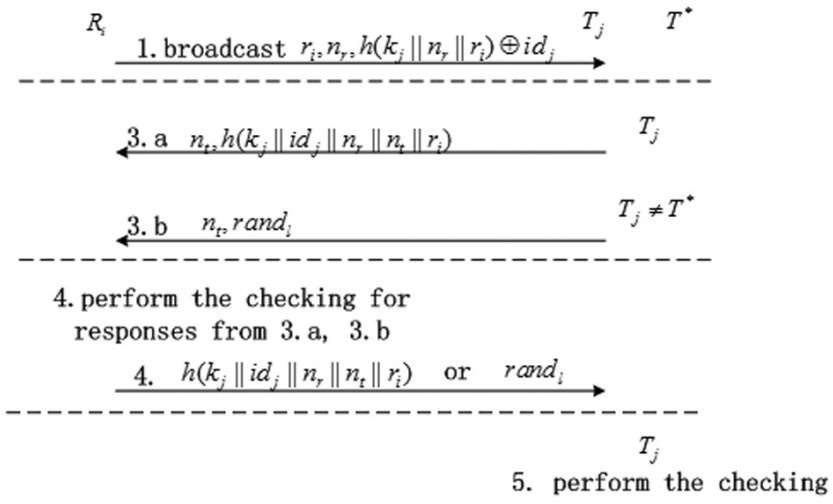

Figure 2. Lee et al.'s server-less searching protocol.

R_i, r_i	r_i is the identity of an RFID reader R_i
T_i, id_i	id_i is the identity of the i th tag T_i
$rand_l$	A random number with length l
$rand_l^j$	The j th random number with length l
n_r	The random number generated by the reader
n_t	The random number generated by the tag
S	The trusted back-end server
k_i	The i th secret key shared by T i and S
h(),f()	Two one-way hash functions
$h()_m$	The m bits in the left of h()
L_i	The reader-specific access list downloaded from S
id_j	Id for RFID tag T_j
i, j	different indexes of tags or readers
CA	Trusted party, responsible for authenticating readers and deploying tags
L_{ij}	The j th item for T_j in contact list L_i, i.e. the j th line in L_i
L_{ij}^{old}	The value of L_{ij} before refreshing
L_{ij}^{new}	The value of L_{ij} after refreshing
N	The total number of tags in the group
C_{hash}	The cost of one hash operation

Table 1. Notations in the protocol.

1. The reader broadcasts $n_t, h(k_j||id_j||n_r||n_t||r_i)$ to the tags.

2. When $T*$ receives the message from the reader, $T*$ will compute the value $h(k_{T*}||n_r||r_i)$ and check whether the value of $h(k_{T*}||n_r||r_i)_l \oplus h(k_j||n_r||r_i)_l \oplus id_j$ equals its identity; if so, it will go to 3a, otherwise, it will go to step 3b.

3a. The desired tag T_j will send the message $n_t, h(k_j||id_j||n_r||n_t||r_i)$ to the reader.

3b. The undesired tag $T*$ will send the message $n_t, rand_l$ with probability λ.

4. After receiving the response from the tags, the reader will send $h(r_i||id_j||n_r||n_t||k_j)$ to the T_j or $rand_l$ to the T*.

5. T_j computes and checks whether $h(r_i||id_j||n_r||n_t||k_j)$ equals the value received in step 4. If so, it will accept the reader. Otherwise, it will terminate the session.

5. Analysis of the Searching Protocol

5.1. Definition

The protocols presented by Lee et al. would suffer from probabilistic tacking.

In searching protocol, when a tag is not the desired one, it will reply to the reader with a probability λ. Thus, the probability of some tags' response can be calculated.

There are two circumstances where we calculated the values of the tracking probability and the overhead of computing hash function on the verifier.

We make a detailed definition on the variables mentioned above.

Definiton 1: the random event that there is the desired tag among the N tags is denoted as C. C's opposite event that there is no desired tag among the N tags is denoted as $\bar{C}$.

When N is very large, that can be seen as infinity, we define the probability of event C and

event $\bar{C}$ as below:

$$P(C) = P(\bar{C}) = \frac{1}{2} \tag{1}$$

We will analyze the two different circumstances from two aspects, as following. We make detailed description for these two cases.

Situation 1: it is a special case. It is certain that there is the desired tag in the group in many circumstances, such as the reader queries for a tag for a second time before updating.

Situation 2: it is uncertain whether the desired tag is in the group of tags or not. This is the most frequent case.

5.2. Probabilistic Tracking

Tracking means distinguishing one tag from the others by obtaining the same or related information from different sessions about the tag. As we all know, an unmatched tag will reply with probability λ and not reply with probability $(1-\lambda)$. In this way, when there is only one response in the wireless channel, it maybe comes from the undesired tag with the probability of λ Suppose that a malicious adversary has already recorded the query of the response and he is patient enough to send the same query over and over again. At the same time he keeps monitoring the number of responses transmitted in the wireless channel. When there is only one response again, the adversary tracks successfully with some probability. We will denote the probability as p_t. Suppose M is the random event that when there is only one response in the channel, it comes from the desired tag and p_m is the probability of the random event. U represents the random event that none of the undesired tags gives any response. p_u is the probability that the other unmatched tags do not answer the query from the reader.

We can get an equation:

$$p_t = p_m \cdot p_u \tag{2}$$

Situation 1: from the definition of situation 1, we will get:

$$p_m = 1 \tag{3}$$

$$p_u = (1-\lambda)^{N-1} \tag{4}$$

So,

$$p_t = p_m \cdot p_u = (1-\lambda)^{N-1} \tag{5}$$

In this way, the average number of times that the adversary replays the same query (set as n) is,

$$n = \frac{1}{p_t} = \frac{1}{(1-\lambda)^{N-1}} \tag{6}$$

Situation 2: in this situation, whether the desired tag is in the group of tags or not is not certain. $P(U_i)$ $(i = 1, 2)$ is the probability that the other unmatched tags do not answer the query from the reader under random event C or $\bar{C}$. $P(M|C)$ means the probability of the case that there is only one response and it comes from the desired tag when the desired tag is in the group. $P(M|\bar{C})$ represents the probability of the case that there is only one response and it comes from the desired tag when the desired tag is not in the group.

$$\begin{aligned} p_t &= P(T_{track}|C) \cdot P(C) + P(T_{track}|\bar{C}) \cdot P(\bar{C}) \\ &= P(M|C) \cdot P(U_1) \cdot P(C) \\ &+ P(M|\overline{C}) \cdot P(U_2) \cdot P(\overline{C}) \end{aligned} \tag{7}$$

Where,

$$P(M|C) = 1 \tag{8}$$

$$P(M|\bar{C}) = 0 \tag{9}$$

$$P(U_1) = (1-\lambda)^{N-1} \tag{10}$$

$$P(U_2) = (1-\lambda)^{N} \tag{11}$$

So,

$$p_t = \frac{1}{2}(1-\lambda)^{N-1} \tag{12}$$

In this situation, the average number of times that the adversary replays the same query (set as n) is,

$$n = \frac{1}{p_t} = \frac{2}{(1-\lambda)^{N-1}} \tag{13}$$

Since the scale of tags may be very great, i.e. N is large, n is rather large, which means the adversary has to replay the same query many times to reach success with some probability. But it is feasible because of computer technology. So the probability p_t cannot be negligible.

In a server-less RFID system, the probability of being tracked and the cost on authentication are both influenced by the value of λ. With an increasing λ, the probability of being traced

will be reduced while the cost on authentication adds up The property associated with λ mentioned before is one of the characteristics of the framework. Because of this property, x is introduced as the weight of security in the comprehensive assessment of the system performance. Besides, a parameter S can be used to evaluate the performance of the system, and S can be expressed as the following equation

$$S = 1 - (x \cdot p_t + (1 - x) \cdot m) \tag{14}$$

where m represents the normalized performance of computation on authentication, ie:

$$m = \frac{1}{N} \cdot \left(\frac{1}{2} \cdot N \cdot \lambda + \frac{1}{2} \cdot (1 + (N-1)\lambda) \right) \tag{15}$$

Above all, performance of the system can be expressed as the equation below:

$$S = 1 - \left(x \cdot \left(\frac{1}{2}(1-\lambda)^{N-1} \right) + (1-x) \cdot \frac{1}{N} \cdot \left(\frac{1}{2} \cdot N \cdot \lambda + \frac{1}{2} \cdot (1 + (N-1)\lambda) \right) \right) \tag{16}$$

The empirical model is visualized by using matlab, as shown in Figure 3. From the figure, it can be seen that the performance of a system will reach the peak in the darkest place of the curve. Because λ and x are both variable, controlling variables method is adopted. With this method, we analyzed two different cases. They are the case where λ is fixed and the case where x is fixed.

Firstly, λ is fixed (λ is set as 0.5), and the probability of being tracked, cost on computation and the performance of the system are shown in Figure 4a. In this case, the operator of the system can adjust the system as he wants.

Secondly, x is fixed (x is set as 0.5) and the probability of being tracked, cost on computation and the performance of the system are shown in Figure 4b. It can be seen from the figure that the performance of the system rises to its peak rapidly and goes down with the increase of λ. The operator can adjust the system as he wants.

Above all, the tendency of the system's performance related to x and λ can be seen clearly from the figures above. The parameters can be adjusted by the system's owner according to the system's ability and requirements.

6. Conclusion

In our paper, a detailed analysis of the existing server-less RFID searching protocols proposed by Lee et al. is shown. From our analysis, we find that probabilistic tracking cannot be ignored. Especially with the help of high-tech computer, probability tracking may be a great security threat. In the future, we will do a deep research on server-less RFID searching protocols, to lower the existing security threat and reach the requirements on server-less RFID searching protocol.

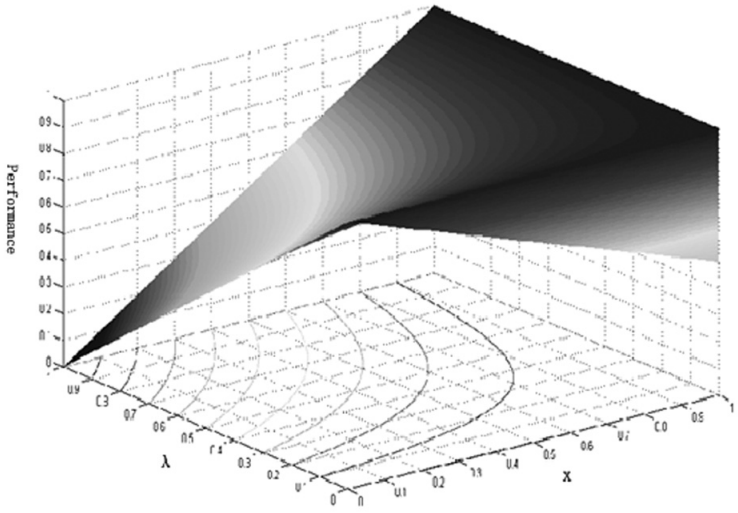

Figure 3. Performance of the system.

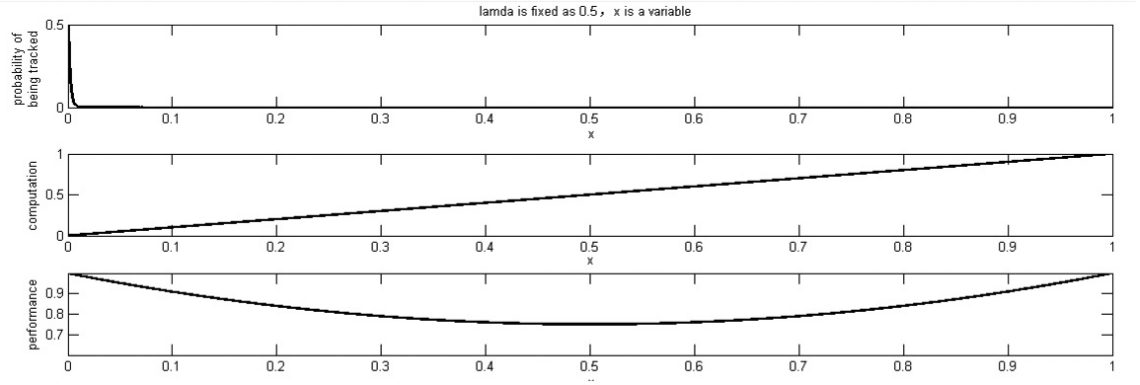

Figure 4a. λ is fixed.

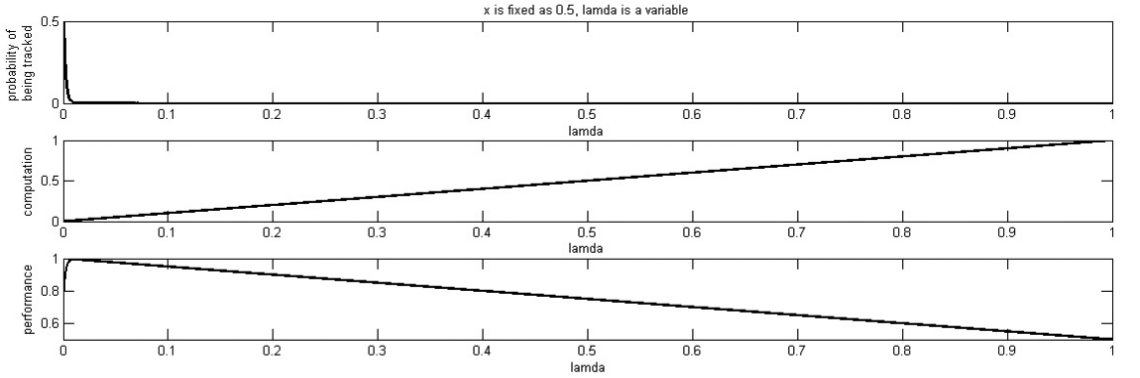

Figure 4b. x is fixed.

Acknowledgment

This work is supported by National Natural Science Foundation of China under Grant 61201159 and by Fundamental Research Funds for the Central Universities under Grant 2012JBM016. The authors also gratefully acknowledge the helpful comments and suggestions of the reviewers, which have improved the presentation.

References

[1] S. I. AHAMED, E. HOQUE, F. RAHMAN, ET AL. YA-SRAP: Yet another serverless RFID authentication protocol[J], 2008.

[2] S. I. AHAMED, F. RAHMAN, E. HOQUE, ET AL., S3PR: Secure serverless search protocols for RFID[C]//Information Security and Assurance, 2008. ISA 2008. *International Conference on. IEEE*, (2008) pp. 187–192.

[3] C. CHEN, D. HE, S. CHAN, ET AL., Lightweight and provably secure user authentication with anonymity for the global mobility network[J]. *International Journal of Communication Systems*, **24**(3), (2011), 347–362.

[4] M. E. HOQUE, F. RAHMAN, S. I. AHAMED, ET AL., Enhancing privacy and security of RFID system with serverless authentication and search protocols in pervasive environments[J]. *Wireless personal communications*, **55**(1), (2010), 65–79.

[5] JUELS, RFID security and privacy: A research survey. *IEEE Journal on Selected Areas in Communication*, **24**(2), (February 2006), 381–394.

[6] Z. KIM, J. KIM, K. KIM, ET AL., Untraceable and serverless RFID authentication and search protocols[C]. *Parallel and Distributed Processing with Applications Workshops (ISPAW), 2011 Ninth IEEE International Symposium on IEEE*, (2011) 278–283.

[7] C. F. LEE, H. Y. CHIEN, C. S. LAIH, Server-less RFID authentication and searching protocol with enhanced security[J]. *International Journal of Communication Systems*, **25**(3), (2012) 376–385.

[8] J. S. LI, K. H. LIU, A hidden mutual authentication protocol for low-cost RFID tags[J]. *International Journal of Communication Systems*, **24**(9), (2011) 1196–1211.

[9] S. MYNENI, S. MISRA, G. XUE, SAMA: Server-less Anonymous Mutual Authentication for Low-Cost RFID Tags[C]. *Communications (ICC), 2011 IEEE International Conference on IEEE*, (2011) 1–5.

[10] M. OHKUBO, K. SUZUKI, S. KINOSHITA, Hash-chain based forward-secure privacy protection scheme for low-cost RFID. In: *Proceedings of the 2004 Symposium on Crytography and Information Security (SCIS 2004)*, Sendai, (2004) 719–724.

[11] J. H. PARK, Security analysis of mCrypton proper to low-cost ubiquitous computing devices and applications. *International Journal of Communication Systems*, **22**(8), (2009) 959–969.

[12] S. E. SARMA, S. A. WEIS, D. W. ENGELS, Radio-frequency identification: Secure risks and challenges. RSA Laboratories Cryptobytes, **6**(1), (2003) 2–9.

[13] S. E. SARMA, S. A. WEIS , D. W. ENGELS, RFID systems and privacy implications. In: *Proceedings of the 4th International Workshop on Cryptographic Hardware and Embedded Systems (CHES 2002). Lectures Notes in Computer Science 2523.* (B. S. KALISKI, C. K. KOC, C. PAAR EDS.), (2003) pp. 454–469. Springer-Verlag, Berlin.

[14] S. SUNDARESAN, R. DOSS, W. ZHOU, A serverless ultra-lightweight secure search protocol for EPC Class-1 Gen-2 UHF RFID tags[C]. *Computer & Information Science (ICCIS). 2012 International Conference on IEEE*, (2012) 580–585.

[15] C. C. TAN, B. SHENG, Q. LI, Severless search and authentication protocols for RFID[C]. *Pervasive Computing and Communications, 2007. PerCom'07. Fifth Annual IEEE International Conference on IEEE*, (2007) 3–12.

[16] J. L. TSAI, T. C. WU, K. Y. TSAI, New dynamic ID authentication scheme using smart cards[J]. *International Journal of Communication Systems*, **23**(12), (2010) 1449–1462.

[17] S. A. WEIS, S. E. SARMA, R. L. RIVEST, D. W. ENGELS, Security and privacy aspects of low-cost radio frequency identification systems. In: *Proceedings of the 1st International Conference on Security in Pervasive Computing. Lectures Notes in Computer Science 2802* (D. HUTTER, G. MULLER, W. STEPHAN, M. ULLMANN, EDS.), (2004) 201–212. Springer-Verlag, Berlin.

[18] E. J. YOON, K. Y. YOO, Improving the dynamic id-based remote mutual authentication scheme. *OTM Workshops. Lecture Notes in Computer Science*, **4277**, (2006) 499–507. Springer, Berlin.

Received: November, 2014
Revised: July, 2015
Accepted: August, 2015

Contact addresses:

Ping Huang
Beijing Key Laboratory of Communication and Information Systems
School of Electronic and Information Engineering
Beijing Jiaotong University
Beijing 100044
China
e-mail: 12120086@bjtu.edu.cn

Haibing Mu
Beijing Key Laboratory of Communication and Information Systems
School of Electronic and Information Engineering
Beijing Jiaotong University
Beijing 100044
China
e-mail: hbmu@bjtu.edu.cn

Fei Zeng
Beijing Key Laboratory of Communication and Information Systems
School of Electronic and Information Engineering
Beijing Jiaotong University
Beijing 100044
China
e-mail: 12125056@bjtu.edu.cn

PING HUANG received her Master's Degree in communication and information system from Beijing Jiaotong University in Apr. 2015. Her research area is RFID network security. She has published three papers during the last three years. After graduation, she has been working on GIS in Baidu.

HAIBING MU received her PH.D. Degree in communication and information system from Beijing Jiaotong University in Jan. 2008. She is a full-time associate professor in the Department of Communication at Beijing Jiaotong University. Her current research areas include computer network and communication, network and information security, Ad Hoc and RFID network security.

FEI ZENG has graduated from Beijing Jiaotong University in 2014 and did some research work in RFID authentication protocols. His research interests include the Internet of Things and RFID authentication protocols, and he published a paper titled "An Improved LMAP++ Protocol Combined With Low-cost and Privacy Protection" in an IE conference.