International Journal of Information Technology and Knowledge Management
July-December 2011, Volume 4, No. 2, pp. 549-553

A FORWARD SECURED AUTHENTICATION PROTOCOL FOR MOBILE RFID SYSTEMS

M.Sandhya[1] & T.R.Rangaswamy[2]

The integration of RFID technology and mobile smart device stimulates the daily increasing popularity of mobile RFID-based applications, which makes its way to become a new hot zone for research and development. Current RFID authentication schemes are not viable to use in mobile RFID environment. The authentication schemes result in computing load to the low cost tag and provide insufficient protection to the information privacy. In this paper, an authentication protocol in mobile RFID environment is proposed which effectively achieves forward security with preventing replay, eavesdropping, and counterfeit tag attacks.

Keywords: Mobile RFID, Authentication, Eavesdropping.

1. Introduction

Radio frequency identification (RFID) has been regarded as the main driver of the future ubiquitous technology. It is also claimed as the core technology to realize internet of things environment where large amount of items are connected seamlessly anytime and anywhere [1]. RFID offers simplicity for people to object (P2O) and object to object (O2O) communications. It is believed that it will play a significant role for future ubiquitous society [2].

Generally, RFID systems consist of Radio Frequency Identification (RFID) tags and RFID readers. While RF tags operate as transponders, RF readers act as transceivers. In case of a more complex application, a database server is required to store information which comes from both transponders and receivers sides [3]. The process of RFID communication can be described as follows, RFID reader request access to the RFID tag and return the reply to the database server. After identification and authentication on server side, then server will return the information of RFID tag to the reader [3][4].

Automatic identification is the basic characteristic of RFID. In its simplest form, identification can be binary, e.g., paid or nor paid which is useful for alerting. Therefore, alerting is become the next powerful feature of RFID. Also, RFID enable real time monitoring to a large number in a short time. In addition, RFID has ability to perform on-chip computation, accordingly it support cryptographic protocol for authentication. In general, RFID has four basic capabilities, identification, alerting, monitoring, and authentication [5].

RFID has become a new and exciting area of technological development, and is receiving increasing amounts of attention. There is tremendous potential for applying it even more widely, and increasing numbers of companies have already started up pilot schemes or successfully used it in real-world environments. Although generally it is assumed that communication between RFID tag and the readers is secure, yet since it is basically wireless based communication, a number of security and privacy issues could not be avoided. Fundamental information security objectives, such as confidentiality, integrity, availability, authentication, authorization, non repudiation and anonymity are often not achieved unless special security mechanisms are integrated into the system [6].

However, this paper proposes an authentication protocol based on the assumption that, as opposed to what is assumed by existing approaches, the communication between a database and a reader also uses communication channels that are not secure. The structure of this paper is as follows. In Section 2 the risks involved in the use of RFID technology and the issues related to it that need to be addressed are discussed. In Section 3 the concept of Mobile RFID is explained Section 4 describes the related work in security of Mobile RFID. Section 5 presents the proposed system. Security of the proposed system is analyzed in Section 6. Finally, Section 7 presents the conclusion of the work.

2. Security Issues of RFID Systems

Several common types of attacks can be applied to RFID systems; eavesdropping, replay attack, man-in-the middle attack, and denial of service (DoS) attack. In eavesdropping, communication channel between the tag and the reader can

[1]Department of Computer Science & Engineering, B.S.Abdur Rahman University, Chennai, INDIA.
[2]Department of Information Technology, B.S.Abdur Rahman University, Chennai, INDIA.
E-mail: [1]sandhyamagesh1997@yahoo.com, [2]raamy 49 @ bsauniv.ac.in.

be observed by an adversary. In the replay attack, the adversary successfully eavesdrops a conversation between the tag and the reader, retransmits these conversations to query the tag or the back-end server to impersonate the valid tag or the valid reader. In the man-in-the-middle attack, the adversary monitors a conversation between the tag and the reader, alters the messages and sends them to the reader or the tag to obtain information. DoS attack can be implemented by placing a large number of fake tags for identification by the reader or corrupting large batch of tags [7]. Moreover, the adversary can prevent the tag or the reader from reading messages. This results in some synchronization problems between the tag and the server.

Device designed specially can impersonate the tags with the data obtained from the valid tag. This attack is called as "cloning attack". The reader can not verify that whether it is communicating with the valid or the fake tag [7]. For example, a thief may replace an expensive item attached to the valid tag with a cheap item attached to the fake tag. RFID tags offer no tamper resistance; therefore a strong adversary can compromise the valid tag to retrieve its stored secrets. The content of the tags is vulnerable to physical attacks because tamper-proofing is an expensive option for low cost tags [7]. In [8], the concept of forward security is introduced. Forward security means that the adversary compromising the tag at time t cannot trace the past interactions of the tag that occurred at time t' < t. The forward security is referred as backward untraceability in [9, 10]. In [9] the concept of forward untraceability is introduced. Forward untraceability means that the strong adversary compromising the tag at time t cannot trace the future interactions of the tag that occurred at time t' > t. In [10] the concept of server impersonation is introduced. In this attack, the strong adversary knowing the internal state of the tag can impersonate the valid server to the tag.

3. MOBILE RFID

Mobile RFID enables unique RFID use-cases not possible with fixed readers. Mobile data collection devices such as scanners tethered to mobile comput-ers, integrated handheld readers, and vehicle mount-ed readers from companies such as Intermec, LXE, and Motorola, allow the reader to be brought to the asset instead of the asset having to pass by the reader. These devices and custom appli-cations running on them can leverage existing wire-less networks to communicate continuously with the rest of the system, and can often be used offline to collect data for transmission to the rest of the system at later time.

Today's deployments that use mobile RFID tech-nology —from workers carrying integrated handheld readers to the mounting of specialized readers on forklifts—benefit from more flexible interaction with tagged assets and broader location coverage [11]. The additional read opportunities enable greater asset visibility and allow for the recording of asset entry, movement, and placement around a facility. New ap-plications are being built every day to leverage these unique capabilities.

In order to truly capitalize on the benefits of mobile RFID, application developers must understand the unique requirements and challenges of mobile application development, deployment, and usage. A flexible architecture provides a rich foundation for mobile application development to extend the software across platforms and readers. Although the mobile RFID system has various applications in recent time and it has the advantages of both mobile technology and RFID system, it raises some serious privacy and security problems. By nature mobile RFID inherits all the problems present in the RFID system, such as, information leakage, traceability and impersonation, but the severity of these problems increase because of the mobility and higher reading range of the mobile RFID reader.

4. RELATED WORK

Researchers have attempted to resolve the security concerns related to the use of RFID tags and have proposed protocols that claim either to achieve secure authentication or to prevent unauthorized traceability. The approach named "Minimalist Cryptography" was introduced by Juels [12], a kind of renaming approach in which tags can change their identity on their own. Juels and Pappu [13] proposed a new approach called the re-encryption in which they applied some cryptography and used keys and cipher text, but were not generalized. So, to generalize it they made changes in it and named it "Universal re-encryption" [14].

A Faraday Cage [15] approach was also proposed to get rid of some security issues which are nothing but an extra device added approach. There is a similar kind of approach named Proxying approach in which Floerkemeier et.al [16] introduced a prototype named "Watchdog Tag". Yong Ki Lee and Ingrid Verbauwhede [17] propose two protocols SRAC and A-SRAC. The first protocol SRAC (Semi-Randomized Access Control) is designed using only a hash function as security primitives in tags. In spite of very restricted functionality, SRAC resolves not only security properties, such as the tracking problem, the forward secrecy and the denial of service attack, but also operational properties such as the scalability and the uniqueness of metaIDs. The second protocol ASRAC (Advanced SRAC) resolves the replay attack in the cost of a random number generator in tags. Moreover, these schemes have significantly reduced the amount of tag transmissions which is the most energy consuming task.

Another invention is a 'RFID blocker tag' [18] which exploit tag singulation (anti-collision) protocols in order to interrupt the communication with all tags or tags within a specific ID range. The blocker works for the most relevant

anti-collision protocols (tree walking and ALOHA) and may be used for privacy protection but it can also be misused for mounting denial-of-service attacks. Y. C. Lee et al. [19] proposed an improved protocol which can avoid tracking and spoofing attack through the different hash value during each authentication.

Shang-ping Wang et al. proposed a low-cost RFID mutual authentication protocol [20] based on the method of HMAC under the assumption that the Hash function is secure, the property that the new protocol can achieve mutual authentication between reader and tag. He Lei et al. proposed a one-way Hash based low-cost authentication protocol [21] with forward security and analyze its efficiency but the computation load was not taken into consideration. K.H.Yeh and Lo developed a robust EPC GEN-2 conformed protocol, called TRAP-3, to pursue stronger anonymity property and security feature [22]. Unfortunately, TRAP-3 still suffers from the de-synchronization attacks. He Lei et al. proposed an improved lightweight authentication protocol [23] using substring functions and analyzed its property. Allen Y.Chang et al. proposed an effective and secured certificate mechanism using mobile devices as RFID readers together with the credit cards containing RFID tags [24]. The result shows it can improve the existing RFID security issues under the premise of safety, efficiency and compatibility of the EPC network. Sun et al. [25] showed a desynchronization attack on SASI with at most 96 trials.

5. PROPOSED METHOD

According to the problems in the literature review outlined above, an improved protocol is proposed which is also based on the hash function, and it can prevent illegal access, eavesdropping, tracking, impersonation and replay attacks. The protocol is illustrated in Figure 1.

The notations used in the proposed method are summarized in Table 1. Mobile RFID reader has to register and authenticate itself to the server. The server authenticates the reader and sends an ID_R and a password s to the reader.

Table 1
Notations of Proposed Protocol

Symbol	Meanings
ID_t	Unique Identifier of the tag
ID_R	Unique Identifier of the reader
K_i	Secret key shared between the tag and the server
K_{i+1}	Updated Secret key used in between the tag and the server
s	Secret key shared between the reader and the server
$\oplus$	Exclusive OR operation
r	A random number generated through the use of a PRNG within the reader
g	A random number generated through the use of a PRNG within the server for updating K_i
D	Detailed Information about the tag in the database
H	Hash function

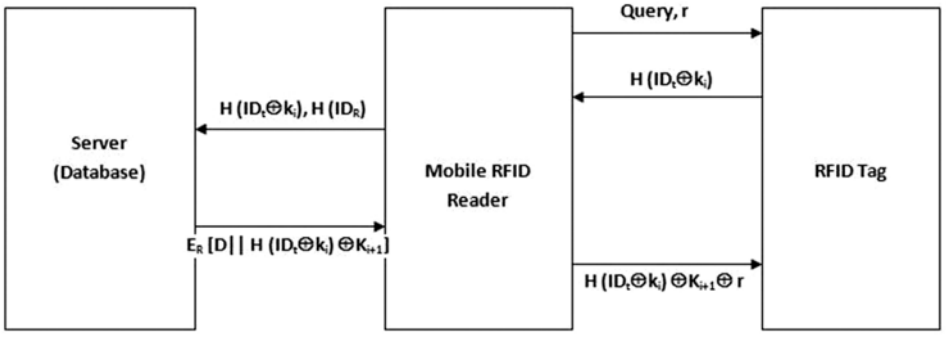

Fig.1: Proposed Method

The details of the proposed method are described in following steps.

1. The reader generates and saves a pseudo random number r by utilizing PRNG and sends a query request to the tag.
2. After receiving the query message the tag computes $H(ID_t \oplus K_i)$ and forwards it to the reader.
3. The reader generates $H(ID_R)$ and forwards it along with the message $H(ID_t \oplus K_i)$ to the server.
4. The server checks whether $H(ID_t \oplus K_i)$ forwarded by the reader matches with the stored hash code of the tags. If it matches then the database authenticates the tag as a legitimate one. Then it verifies the authenticity of the reader by matching the received hash code of the reader $H(ID_R)$ with the stored hash code. If they are equal, the reader passes the authentication; otherwise, the reader is not authenticated.

The server updates the confidential information K_i to K_{i+1} where K_{i+1} = PRNG (K_i).g is the random number used to update the secret key K_i. The server performs XOR algorithm of K_{i+1} with $H(ID_t \oplus K_i)$. This message along with the detailed information

of tag D is forwarded in encrypted form to the reader using the reader password K_R.

5. The reader decrypts and obtains the tag data D. It then utilizes the XOR algorithm to generate $H(ID_t \oplus K_i) \oplus K_{i+1} \oplus r$ and forward it to the tag.

   The tag verifies the authenticity of the reader by using the random number r. It then computes K_{i+1} by using the XOR operation of $H(ID_t \oplus K_i)$ with random number r. The computed value of K_{i+1} is the updated secret key information between the tag and the server. The tag updates the secret key information K_i to K_{i+1}.

6. Security Analysis of The Proposed Method

Eavesdropping: In the process of the proposed scheme the information has been encoded by hash function which makes the adversary to get the original value impossible because of the one-way characteristic. The attackers cannot know the detailed content of the information even they espionage the outputs; In the process of (4), the server forwards the tag detail in encrypted form to the reader so the attackers also cannot know the real information.

Denial of Service Attack: The proposed protocol needs synchronization between the server and the tag. The tag refreshes its secrets after taking confirmation from the server. An adversary can prevent the reader or the tag from receiving a message. If the adversary performs this attack on the last flow of the protocol, he can prevent the tag from taking confirmation. This breaks the synchronization between the tag and the server because the server refreshes the tag secrets but the tag does not. However, in the protocol, the server makes itself synchronize with the tag in such a situation because it stores old and new values of the tag secrets.

Tag Cloning: Tag cloning means that, the data on a valid tag is scanned and copied by a malicious RFID reader and the copied data is embedded onto a fake tag. Authentication of RFID reader prevents this cloning attack. In the protocol, a tag never generates genuine replies unless it verifies the reader first. This verification thwarts the cloning attack.

Forward Security: The forward-security property means that even if the adversary obtains the current secret key, he still cannot derive the keys used for past time periods. To ensure this, a forward-secure message authentication scheme which involves key-evolving is used. For each valid read operation, a tag uses the current key K_i for creation and verification of authentication tags. At the end of each transaction, the old key K_i is updated to a new secret key K_{i+1} and the previous K_i is deleted. An attacker breaking in gets the current key. But given the current key it is still not possible to derive any of the previous keys.

Privacy Attacks: In privacy attacks an adversary wants to learn the contents of the tag and queries the tags. In each session, the tag uses a hash function to generate $H(ID_t \oplus K_i)$ and responds the reader with the hash code. Only valid server can access the information associated with the tag, so it can only extract the correct information ID_t from the message. Thus, the protocol provides information privacy for the tag.

Replay Attack: The attackers can obtain outputs of the tag, and transmit the eavesdropped messages to the reader. But he cannot impersonate the legitimate tag since the outputs are different on every session. Therefore, the scheme is secure and against the impersonation and replay attack.

7. Conclusion

Mobile RFID system has advantages of a RFID system and a mobile device, but it also brings a series of new security and privacy problems. In the mobile RFID system, the communication channel between the reader and the database is not assumed to be safe. If the security and privacy problems are not appropriately solved, the applications of Mobile RFID will be greatly reduced. Therefore, this paper proposes an improved efficient Mobile RFID authentication protocol with confidential information updating mechanism in order to provide forward security and analyze its security. The result indicates that this protocol does not increase the calculation amount and the cost of tag obviously. Moreover, it can provide forward secrecy and protect from traceability attack, replay attack and cloning attacks.

References

[1] B, Violino, "Leveraging Internet of Things," RFID Journal November/ December, 2005, pp.1-2.

[2] R. Want, "Enabling Ubiquitous Sensing with RFID", IEEE Computer Magazine, 37, Iss. 4, 2004, pp. 84-86.

[3] S. Han, T.S. Dhillon, and E. Chang, "Anonymous Mutual Authentication Protocol for RFID Tag without Back-End Database," Mobile Adhoc and Sensor Networks 2007, LNCS 4864, pp. 623—632.

[4] S. Han, V. Potdar, and E. Chang, "Mutual Authentication Protocol for RFID Tags based on Synchronized Secret Information with Monitor", Computational Science and its Applications - ICCSA 2007, LNCS 4707, pp. 227 – 238.

[5] M.Langheinrich and R.Marti, "Practical Minimalist Cryptography for RFID Privacy," IEEE Systems Journal, 1, Iss. 2, Dec 2007.

[6] H. Knospe and H. Pohl, "RFID Security," Information Security Technical Report, 9, Iss. 4, pp 39-50, Dec 2004.

[7] P. H. Cole and D. C. Ranasinghe, "Networked RFID Systems and Lightweight Cryptography", Springer-Verlag, 2008.

[8] M. Okhubo, K. Suzuki, and S. Kinoshita, "Cryptographic Approach to "Privacy-friendly" Tags", Proceedings of RFID Privacy WorkShop, 2003.

[9] C. H. Lim and T. Kwon, "Strong and Robust RFID Authentication Enabling Perfect Ownership Transfer", Proceedings of the 8th International Conference on Information and Communications Security, ICICS 2006.

[10] B. Song and C. J. Mitchell, "RFID Authentication Protocol for Low-cost Tags", Proceedings of the1st ACM Conference on Wireless Network Security, New York, NY, USA, 2008. pp 140–147.

[11] Mrs. M. Sandhya and Dr.T.R.Rangaswamy, "Buffer Overflow Prevention in Mobile RFID Environment Using Train Algorithm", Journal of Computing, 2, Issue 7, July 2010.

[12] A. Juels, "Minimalist Cryptography for Low-cost RFID Tags", Proceedings of the 4th International Conference on Security in Communication Networks, Springer-Verlag, vol 3352, 2004, pp. 149–164.

[13] A. Juels, R. Pappu, "Squealing Euros: Privacy Protection in RFID Enabled Banknotes. Financial Cryptography", Springer-Verlag, vol.2742, 2003, pp. 103–121.

[14] G. Ateniese, J. Camenisch, B. de Madeiros, "Untraceable RFID Tags via Insubvertible Encryption", Proceedings of the 12th ACM Conference on Computer and Communication Security, 2005, pp. 1-10.

[15] Zongwei Luo, Terry Chan, Jenny S. Li, "A Lightweight Mutual Authentication Protocol for RFID Networks", Proceedings of the IEEE International Conference on E-business Engineering, October 2005, pp. 620-625.

[16] C.Floerkemeier, R. Schneider, M. Langheinrich", Scanning with a Purpose - Supporting the Fair Information Principles in RFID Protocols", Proceedings of the 2nd International Symposium on Ubiquitous Computing Systems, 2004, pp. 1-9.

[17] Yong Ki Lee and Ingrid Verbauwhede, "Secure and Low-cost RFID Authentication Protocols", Proceedings of the 2nd IEEE International Workshop on Adaptive Wireless Networks, November 2005.

[18] A.Juels, R.L. Rivest and M. Szydlo, "The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy", Proceedings of the 10th ACM Conference on Computer and Communications Security, 2003.

[19] Y.C.Lee, Y.C.Hsieh, P.S.You and T.C.Chen, "An Improvement on RFID Authentication Protocol with Privacy Protection", Proceedings of the 3rd International Conference on Convergence and Hybrid Information Technology, South Korea: Busan, 2, 2008, pp.569–573.

[20] Shang-ping Wang, Qiao-mei Ma, Ya-ling Zhang and You-sheng Li, "HMAC-Based RFID Authentication Protocol", Proceedings of the 2nd International Symposium on Information Engineering and Electronic Commerce, China, 2010, pp.1-4.

[21] He Lei, Lu Xin-mei, Jin Song-he and Cai Zeng-yu, "A One-way Hash Based Low-cost Authentication Protocol with Forward Security in RFID System", Proceedings of the 2nd International Asia Conference on Informatics in Control, Automation and Robotics, China, 2010,pp.269-272.

[22] K.H. Yeh and N.W. Lo, "Improvement of Two Lightweight RFID Authentication Protocols", Information Assurance and Security Letters 1, 2010, pp.6-11.

[23] He Lei, Gan Yong, Cai Zeng-yu and Li Na-na, "An Improved Lightweight RFID Protocol Using Substring", Proceedings of the 5th International Conference on Wireless Communications, Networking and Mobile Computing, China, 2010, pp. 1-4.

[24] Allen Y. Chang, Dwen-Ren Tsai, Chang-Lung Tsai and Yong-Jiang Lin, "An Improved Certificate Mechanism for Transactions Using Radio Frequency Identification Enabled Mobile Phone", Proceedings of the 43rd Annual International Conference on Security Technology, Taiwan, 2009,pp.36-40.

[25] H.M. Sun, W.C. Ting, and K.H. Wang, "On the Security of Chien's Ultra lightweight RFID Authentication Protocol", IEEE Transactions on Dependable and Secure Computing, 2011, pp.315-317.