http://ansinet.com/itj

ITJ

ISSN 1812-5638

INFORMATION TECHNOLOGY JOURNAL

ANSInet
Asian Network for Scientific Information
308 Lasani Town, Sargodha Road, Faisalabad - Pakistan

Information Technology Journal 10 (10): 1917-1925, 2011
ISSN 1812-5638 / DOI: 10.3923/itj.2011.1917.1925

Prevention of Tampering Attacks in Mobile Radio Frequency Identification Environment

[1]M. Sandhya and [2]T.R. Rangaswamy
[1]Department of CSE, B.S.A. Crescent Engineering College, Chennai, India
[2]Department of IT, B.S.A. Crescent Engineering College, Chennai, India

Abstract: This study describes the characteristics of data tampering in RFID-based information systems and a method addressing it is proposed using hashing techniques in mobile RFID environment. The proposed method requires only hash, XOR and simple calculations but can provide good security and privacy protection features. Mobile RFID-enhanced applications ("Mobile RFID") offer a unique way of interacting with the physical world by using the touch paradigm. They offer an intuitive way to interact with physical objects to which RFID transponders are attached. However, the development of mobile RFID applications is not well supported yet, in contrast to stationary RFID applications because of security and privacy related issues. A critical threat for Mobile RFID based information systems is represented by data tampering which corresponds to the malicious alteration of data recorded in the tag memory.

Key words: RFID security, mobile RFID, mutual authentication, RFID transponders, pseudo random, constrained environment

INTRODUCTION

RFID systems, owning to their low cost and their convenience in identifying an object without physical contact, have been found in many applications such as manufacturing and supply chain management. An RFID system consists of three parts: tags, the reader and the back-end database. Tags are composed of a microchip for memory and logical operations and an antenna coil for receiving and transmitting wireless signals. The reader interrogates tags for their contents through RF antenna and interface to back-end databases for more functions. The back-end database associates records with tag data collected by the reader (Sarma *et al*., 2003).

RFID technology and products come into the commercial application stage during 1980-2000. The standardization of RFID technology tend to get attention, RFID products has been wide spreadly adopted and has become a part of people's lives. Zhang *et al*. (2011) proposed the design and implementation of a dynamic RFID data driven supply chain management which showed the importance and the usefulness of such an artifact for businesses seeking to optimize the performance of their supply chains. The RFID technology is effectively used in Smart Parking System (Idris *et al*., 2009) to help the users to locate their vehicle even if they use other exits. The integration of RFID (Lo *et al*., 2009) with intelligent agents in billing systems improves the process, reduces the management cost and provides more flexible stable systems. RFID based clinical decision support system (Al-Safadi and Al-Sulaiman, 2011) was introduced and the health care providers had a chance to track fast and accurate patient, staff and medical records in real time. Zahrani (2010) conducted an investigation regarding the optimization of effectiveness and efficiency in Ubiquitous learning environments through the integration of RFID and wireless technologies (2010) in a sole service network.

Mobile RFID service is defined as a special type of mobile service using RFID tag packing objects and RFID readers attached to mobile RFID terminals. The mobile RFID system is applied in various fields such as retail, bank and supply chain because it has advantages of a RFID system and a mobile device (Zhu *et al*., 2005). In such applications, RFID readers are installed in intelligent terminals such as PDA or mobile phone and other mobile devices. RFID readers can be mobile while RFID tags are relatively static. In mobile systems, the mobile device plays the role as a reader of the RFID systems. It transmits a query to a tag and identifies the received information from the tag and forwards to the database. The database is given the largest trust in the current mobile environment because it stores all related information with the tags. The information exchange between the mobile readers and the database is responsible for maintaining detailed information of users.

Corresponding Author: M. Sandhya, Department of CSE, B.S.A. Crescent Engineering College, Chennai, India

The RFID system causes security and privacy problems such as impersonation, traceability and reply attack because it uses wireless communication with RF signals. For this reason, the mobile RFID system has these problems which are similar to the RFID system and they are more serious than the RFID system because anyone has the mobile device as a reader and obtains information of tagged objects (Konidala and Kim, 2006). Traditionally, it is believed that the communication channel between the reader and the database is safe. However, in the mobile RFID system, the communication between the reader and the database is using wireless channel, thus, the communication channel between the reader and the database is not assumed to be safe (Wu *et al*., 2009).

Tsudik (2006) proposed a scheme called YA-TRAP (Yet Another Trivial RFID Authentication Protocol). In YA-TRAP, tag T_i shared a unique key k_i with the reader. T_i also stored a timestamp t_i that records the last time at which it was interrogated. Collins (2004) proposed that the tags can be saved either by destroying them or just by partially disabling them. The approach named "Minimalist cryptography" was introduced by Juels (2005) which was also a kind of renaming approach in which tags can change their identity on their own. Juels and Pappu (2003) proposed an approach, re-encryption in which some cryptographic techniques were applied to generate the cipher text but this method was not generalized. Ateniese *et al*. (2005) made some changes in the re-encryption approach, generalized and named it as Universal re-encryption.

Among existing Two-Factor Authentication mechanisms (Bindu *et al*., 2008; Chang and Lee, 2008; Hsiang and Shih, 2009; Shieh and Horng, 2008; Wang *et al*., 2009), mostly used active smart card as authentication tool which consists of hash function, exclusive or random number and timestamp. These methods met the demands of security but they all adopt active smart card of higher cost and secure channel assumption which was a condition unnecessarily, provided in actual environment.

Wang *et al*. (2010) proposed a low-cost RFID mutual authentication protocol based on the method of HMAC under the assumption that the Hash function was secure, the property that the new protocol can achieve mutual authentication between reader and tag. Lei *et al*. (2010) proposed a one-way Hash based low-cost authentication protocol with forward security and analyzed its efficiency but the computation load was not taken into consideration. Yeh and Lo (2010) developed a robust EPC GEN-2 conformed protocol, called TRAP-3, to pursue stronger anonymity property and security feature. Unfortunately, TRAP-3 still suffered from the de-synchronization attacks. Lei *et al*. (2009) proposed an improved lightweight authentication protocol using substring functions and analyzed its property. The previous protocols (Wong *et al*., 2006; Tuyls and Batina, 2006) for RFID security were scalable but traceable. Randomized hash lock scheme (Weis *et al*., 2003) was untraceable but unscalable.

There is scant published research on the feasible rogue-scanning and eavesdropping ranges for mobile RFID (Juels, 2006). Such research would benefit both mobile RFID security analyses and public policy formulation. The importance of mobile RFID privacy in restricted environment such as military operations reinforces an oft-neglected point: Privacy is not just a consumer concern. The enhanced supply-chain visibility that makes mobile RFID so attractive to industry can also, in another guise, betray competitive intelligence. Enemy forces monitoring or harvesting mobile RFID communications in a military supply chain could learn about troop movements. In civilian applications, similar risks apply. For example, many retailers see item-level RFID tagging as a means to monitor stock levels on retail shelves and avoid out-of-stock products. Individually tagged objects could also make it easier for competitors to learn about stock turnover rates; corporate spies could walk through shops surreptitiously scanning items (Melski *et al*., 2007).

Wang and Chin (2009) modified some of the vulnerabilities. To prevent replay attacks, the tag generated a random nonce as soon as it receives the query from the Reader. In Dimitriou's protocol (Dimitriou, 2008) the new owner updated the secret key in a private environment (e.g., home) where adversaries are assumed to be absent. This assumption is questionable because there is no need to encrypt any of the messages between tag and reader in such 'private' environments. The protocol proposed by Chen *et al*. (2008) had some fundamental vulnerabilities such as transmission of the tag's ID, EPC, the serial number of the product and the brand signature in clear text from tag to reader.

Although, mobile RFIDs provide relevant opportunities, they involved considerable information security threats (Juels, 2006), such as cloning of original tags and privacy violation. A critical threat is represented by data tampering which consists in the malicious changing of data recorded in the tag memory. The tampering has many dangerous effects, such as incoherence in the information system, exposure to opponent attacks and mistakes in the production flow. Several solutions to various security issues in mobile (Zhong and Yang, 2006) and pervasive technologies have

been provided but problems as tampering in RFID still represent a critical threat for data security. Potdar and Chang (2006) introduced fragile watermark in RFID tags to prevent tampering but the scheme was insecure and it cannot discriminate which part of RFID tags was tampered.

Yamamoto *et al*. (2008) proposed a tamper detection solution which was based on a technique known as a digitally signed journal (Suzuki and Harrison, 2006); this proposal was promising but it required modification in the existing EPC-C1G2 tags. Madan *et al*. (2006) proposed watermarking based tamper detection solutions for RFID tags where the Serial Number field was used as the cover medium to detect any modification occurring either in the EPC Manager (EM) or in the Object Class (OC) but not for both at the same time.

To deal with the tampering problems in mobile RFID environment, the use of cryptographic protocols is required. However, designing cryptographic protocols for RFID tags is challenging as an RFID tag is a low-cost device with limited computational power (Garfinkel and Rosenberg, 2005). It is infeasible to implement public key cryptographic primitives and block ciphers. As a result, a new approach to design cryptographic protocols for RFID tags which employ an only lightweight primitive is required. The most popular lightweight primitive used in designing cryptographic protocols for Mobile RFID is hash function. Therefore, this study aims at filling the gap in mobile RFID security study, analyzing the characteristics of data tampering in RFID-based information systems and surveying the state-of-the-art of RFID tampering protection, in order to provide readers with an exhaustive overview on risks and on proposed defenses against tampering. This study is specially focused on tampering with data in tag memories, since this threat represents a critical open issue. Furthermore, the most recent and effective general purpose security approaches for RFID tags are analyzed, evaluating their ability to effectively protect against tampering.

SECURITY REQUIREMENTS OF RFID

The RFID system consists of the tag, reader and database. User information or item information is sent to the database after the tag receives power from the reader. The database compares the tag information and stored information and sends authorization data to the tag after authorization. For this procedure to be processed properly, fabrication of data transfer must be prevented. However, the communication channel between the tag and reader is wireless, thus exposed to third parties. Therefore, this chapter deals with security requirements of RFID systems.

Authentication: All components of the system should go through an authentication process. The RFID is comprised of a tag, reader and database. Each part should provide authentication to each other. The tag should send secret values which have been previously agreed upon, to each component to become authorized.

Anonymity: Even if data is acquired from a tag, it should not be trackable to a tag. If identification values are set, anonymity cannot be guaranteed.

Confidentiality: Values used in security protocol should not be exposed and only authorized users may share them. All components should share a secret value to authenticate each other.

TAMPER ATTACKS IN RFID NETWORK

The greatest threat for RFID Information System is represented by data tampering. The most well-known data tampering attacks control data and the main defense against it is the control flow monitoring for reaching tamper-evidence. However, tampering with other kinds of data such as user identity data, configuration data, user input data and decision-making data, is also dangerous (Chen *et al*., 2005).

Some solutions were proposed, such as a tamper-evident compiler and micro architecture collaboration framework to detect memory tampering (Zhang *et al*., 2006). A further threat is the tampering with application data, involving mistakes in the production flow, denial of service, incoherence in the information system and exposure to opponent attacks. This kind of attack is especially dangerous for RFID systems, since one of the main RFID applications is the automatic identification for database real-time updating.

Tamper attacks may occur anywhere in the EPC network which include tags, readers, middleware, EPCIS (Electronic Product Code Information Services) repository, EPCIS accessing application, local ONS (object name service) and enterprise application database. The possible tamper attacks on RFID system can be classified into four categories based on the locations where they may be attacked:

RFID tag tampers: Tampering attacks on RFID tags can be divided into three types:

- **Tag data manipulation:** Malicious RFID reader can either corrupt or manipulate the data contained in a tag. Using a reader one can write data into the memory banks of a tag to suit the adversary's requirements. Equipped with the misleading security

features, the fake products can avoid closer inspection

- **Tag spoofing:** Spoofing which imitates the behavior of a genuine label, presents a serious threat to an RFID system as it adds a new dimension to thieving. A thief may replace a valid item with a fake label or replace the label of an expensive item with that of a fake label with data obtained from a cheaper item. Fake labels may also be used to create imitation items. However, because removing and reapplying authentic labels is costly, this attack does not threaten RFID system in a large scale
- **Tag cloning:** The ability to create clones of tags can be used as a means to overcome counterfeit protection (e.g., in passports and drug labels) and as a preparatory step in a large scale theft scheme

RFID stream tamper: In RFID applications, data are treated as a continuing stream instead of static datasets, delivered over a wireless network. Since streaming data are usually transmitted over unreliable networks, malicious parties can easily inject offensive data into the stream. Van Le *et al*. (2007) revealed a replay attack during RFID communications which the attacker uses a tag's response to a rogue reader's challenge to impersonate the tag to destroy stream integrity. In such applications, RFIDs can be more vulnerable than other mechanisms, due to their ability to be read at a distance by covert readers.

Electronic pedigree tamper: Some regulatory agencies have implemented provisions requiring pedigree for products in an attempt to ensure only authentic products are distributed through the supply chain (Guo *et al*., 2007). Clearly an item's electronic pedigree plays a vital role through counterfeit and gray market detection, shrinkage avoidance and accurate and autonomous unit level inventory management but if this electronic pedigree was accessed unauthorized, illegally modified, or fabricated, most of the aforementioned advantages may be lost.

Object naming service data tamper: ONS (Object Naming Service) can be considered as a DNS (Domain Name System) server; therefore, the security threats related to DNS server are also applicable to ONS (EPCglobal, 2007). Threats in this category include file corruption, unauthorized updates, ONS cache poisoning, IP address spoofing and data interception.

PROPOSED METHOD

The purpose of proposed protocol is that the information communicated between tag and reader is secure. Also, this protocol use lightweight operation for efficiency of reader and tag to provide security against tampering attacks.

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
R	Secret key shared between the reader and the server
$\oplus$	XOR operation
r	A random number generated through the use of a Pseudo random number generator (PRNG) by the reader
ID_{Tnew}	Updated ID information of the tag
PRNG	Pseudo random number generator
H	Hash function

The proposed method can be used in a mobile environment. In the mobile environment, the reader and database can be applied in a wireless environment and can therefore be perceived as insecure channels. The proposed method is based on the insecure communication channel between the tag and the reader. This method provides mutual authentication between the tag and database and therefore provides anonymity to the tag user.

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 R to the reader. The proposed method is illustrated in Fig. 1.

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

- The reader generates and saves a pseudo random number r by utilizing Pseudo Random Number Generator (PRNG) and sends a query request to the tag
- After receiving the query message the tag computes $H(ID_T \oplus K_I)$ and forwards it to the reader
- The reader generates $H(ID_R)$ and forwards it along with the message $H(ID_T \oplus K_I)$ to the server
- 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 encrypts the identity information of the tag ID_T using the key R known between the server and reader. It forwards the encrypted information to the reader.

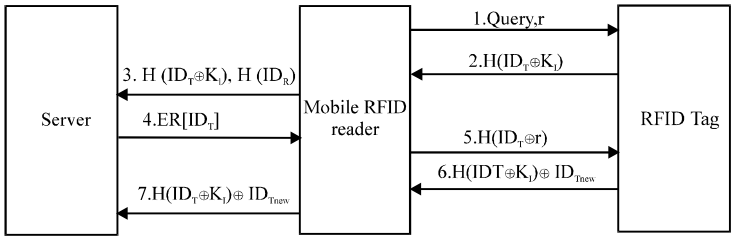

Fig. 1: Proposed Method

- The reader decrypts and obtains the tag information ID_T. It then utilizes the XOR algorithm to generate H (ID_T⊕ r) and forward it to the tag
- The tag verifies the authenticity of the reader by using the random number r. The reader is an authenticated one and now it has the right to access the tag memory and modify the information stored on the tag. The reader performs the modifications on the tag and the tag information is updated. The modified information details of the tag ID_{Tnew} should also be updated in the database. The tag computes H (ID_T⊕ K_I) ⊕ ID_{Tnew} and forwards the information to the reader
- The reader forwards the message H (ID_T⊕ K_I) ⊕ ID_{Tnew} to the server. The server checks whether H (ID_T⊕ K_I) forwarded by the reader matches with the stored hash code of the tags. If it matches the server updates the identity information of the tag ID_T to ID_{Tnew}

IMPLEMENTATION

In this section, focus is on the security module implementation cost for the RFID tag because the passive RFID tag is hardware constrained device. The implementation of the complex encryption schemes such as public key encryption or the symmetric key encryption is currently very rough task in that type of devices. Although, the complex encryption scheme equipped tag could be implemented, the tag would cost more. Therefore, the implementation cost should be considered very carefully before implementing the security module into the Active or Passive tag.

Excluding the basic need for RFID tag fabrication such as antenna, IC and memory area, only 1,000 ~ 3,500 gates can be assigned for security module implementation. To verify whether the proposed scheme can be implemented practically, experiment is made on the total number of gates for the proposed scheme. It has been designed in such a way that the data and pseudonym may be implemented in parallel. Therefore, 128 XOR modules are needed and the register which stores

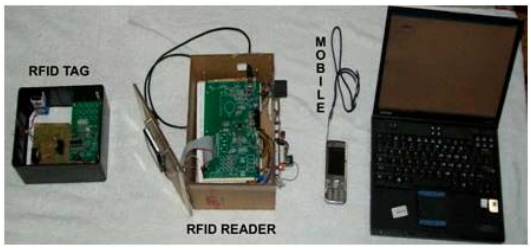

Fig. 2: Complete Setup

the 128 bit-length temporal data for implementation of the nonce or the ID of tag is also needed. However, these basic needs can be reduced by reducing the bit-length of data which the implementation module takes for input.

For example, if the implementation module takes 64 bit-length data as the input then the number of XOR module for the data padding and register size for the temporal input/output data storage can be reduced almost by half. In the proposed work, this module can be implemented within 5,208 gates if it is assumed that the implementation module is designed to take 32 bit-length data as input data. The total gates of the work are even smaller than those of the AES module or MD-4. Through experiment, especially in security and performance viewpoint, it is found that the work has the advantage of composition of hash and exclusive-or than just applying the hash function or the exclusive-or.

The proposed method is implemented and tested on a RFID reader prototype model. Wireless mode of communication is used in between the RFID reader and mobile phone to make it act as a Mobile RFID reader. The objective of the experiment is to validate various aspects introduced in the proposed method and display the results.

The complete setup used for testing the proposed system is shown in Fig. 2. The Mobile RFID reader has to first register to obtain a username (ID_R) and password (R). The login screen of the reader is shown in Fig. 3. The

Fig. 3: Mobile Reader login

Fig. 4: Mobile Reader querying the tags

reader forwards a query and gets a response from the tag and it is displayed in Fig. 4. The complete details about the tag will be obtained by the reader after the authentication process and the result of it is shown in Fig. 5.

To test the effectiveness and security of the proposed system, testing is conducted from various aspects. On hardware, a reader is selected and on

Fig. 5: Server returns details to Mobile Reader

software, programs are designed to conduct testing from various aspects such as accessing, decryption, modifying tag data, damaging and copying tag.

Testing result could be concluded as following:

- The access of tag data through authentic or copied Reader is possible but it is difficult to analyze the tag information out successfully. In other words, even unauthentic user could read out tag data but they couldn't decrypt the information
- Unauthentic user might modify tag data through specific ways but such tag could not pass the validation of system
- Once tag is damaged or copied, it could not pass the validation of system

ANALYSIS AND COMPARISONS

Analysis and comparison in functionalities: To analyze the functionalities in the proposed mechanism, the symbols are defined in Table 2. In some related works (Bindu *et al*., 2008; Chang and Lee, 2008; Hsiang and Shih, 2009; Shieh and Horng, 2008; Wang *et al*., 2009), the user identification is applied with active RFID tags and the low-cost requirement (C2) is unable to accomplish. The detailed comparisons in functionalities are shown in Table 3.

Efficiency analysis: Besides security, care is also taken about how efficient a RFID system operates. The

Table 2: Notations for the analysis and comparisons

Notations	Statements
C_1	Mutual authentication is achieved
C_2	Low cost requirement is provided
C_3	The password guessing attack is resisted
C_4	The message integrity is guaranteed
C_5	Reader has to be authenticated to write messages into the assigned sector and block in tag
C_6	The secure channel is needless

Table 3: The functionalities of schemes compared

	Schemes					
Items	Bindu *et al.* (2008)	Chang and Lee (2008)	Hsiang and Shih (2009)	Shieh and Horng (2008)	Wang *et al.* (2009)	Proposed method
C_1	Yes	Yes	Yes	Yes	Yes	Yes
C_2	No	No	No	No	No	Yes
C_3	Yes	Yes	Yes	Yes	Yes	Yes
C_4	No	No	No	No	No	Yes
C_5	No	No	No	No	No	Yes
C_6	No	No	No	No	No	Yes

efficiency of a RFID system is measured by computation load on a tag, communication load and computation load on the back-end server.

- **Computation load on a tag:** This is measured by how many hash operations are needed on a tag for a complete interrogation. The proposed scheme involves only two hash operations
- **Communication load:** Seven messages are needed for a complete interrogation
- **Computation load on the server:** The proposed scheme can precompute the hash values before querying the tag and reader. During interrogation, the back-end server only needs to search the database. If appropriate searching algorithm is adopted, the server could find a matching value with complexity of O (1). In batch mode, the complexity is O (n)

CONCLUSION

A more comprehensive approach to address data tampering problem in mobile RFID environment is proposed in the hope to inspire more research in this field. It is very imperative to protect unauthorized access to the tag in order to prevent the violation of privacy and confidential information stored in it. Moreover, the proposed method is a mutual authentication system that will be able to protect unauthorized or malicious readers from accessing the information stored in the RFID tags. In conclusion, the mutual agreement protocol can offer data security enhancement and privacy protection capability at reader side under an insecure and wireless mobile RFID system.

REFERENCES

Al-Safadi, L. and Z. Al-Sulaiman, 2011. RFID based clinical decision support system using simulation modeling. J. Applied Sci., 11: 2808-2815.

Ateniese, G., J. Camenisch and B. de Madeiros, 2005. Uuntraceable RFID tags via insubvertible encryption. Proceedings of the 12th ACM Conference on Computer and Communication Security, October 2005, Washington, DC., pp: 1-10.

Bindu, C.S., P.C.S. Reddy and B. Satyanarayana, 2008. Improved remote user authentication scheme preserving user anonymity. Int. J. Comput. Sci. Network Security, 8: 62-66.

Chang, C.C. and C.Y. Lee, 2008. A friendly password mutual authentication scheme for remote-login network systems. Int. J. Multimedia Ubiquitous Eng., 3: 59-64.

Chen, C.L., Y.Y. Chen, Y.C. Huang, C.S. Liu, C.I. Lin and T.F. Shih, 2008. Anti-counterfeit ownership transfer protocol for low cost RFID system. Wseas Trans. Comput., 8: 1149-1158.

Chen, S., J. Xu, E.C. Sezer, P. Gauriar and R.K. Iyer, 2005. Non-control-data attacks are realistic threats. Proceedings of the 14th Conference on USENIX Security Symposium, (SSYM'05), USENIX Association Berkeley, CA, USA., pp: 12-12.

Collins, J., 2004. Marks spencer expands RFID retail trial. RFID Journal, February 2004, http:// www.rfidjournal.com/article/view/791.

Dimitriou, T., 2008. RFIDDOT: RFID delegation and ownership transfer made simple. Proceedings of the 4th International Conference on Security and Privacy for Communication Networks, (ICSPCN'08), ACM, New York, USA., pp: 370-376.

EPCglobal, 2007. Pedigree ratified standard. EPC Version 1.0.

Garfinkel, S. and B. Rosenberg, 2005. RFID: Applications, Security and Privacy. 1st Edn., Addison-Wesley Professional, USA., ISBN: 0321290968, pp: 608.

Guo, H.P., Y.J. Li and S. Jajodia, 2007. Chaining watermarks for detecting malicious modifications to streaming data. Inform. Sci., 177: 281-298.

Hsiang, H.C. and W.K. Shih, 2009. Weaknesses and improvements of the Yoon-Ryu-Yoo remote user authentication scheme using smart cards. Comput. Commun., 32: 649-652.

Idris, M.Y.I., E.M. Tamil, Z. Razak, N.M. Noor and L.W. Kin, 2009. Smart parking system using image processing techniques in wireless sensor network environment. Inform. Technol. J., 8: 114-127.

Juels, A. and R. Pappu, 2003. Squealing Euros: Privacy protection in RFID enabled banknotes. Financial Cryptography, 2742: 103-121.

Juels, A., 2005. Minimalist cryptography for low-cost RFID tags. Sec. Commun., 3352: 149-164.

Juels, A., 2006. RFID Security and privacy: A research survey. IEEE J. Select. Areas Commun., 24: 381-394.

Konidala D.M. and K. Kim, 2006. Mobile RFID applications and security challenges. Inform. Sec. Cryptol.-ICISC, 4296: 194-205.

Lei, H., G. Yong, C. Zeng-yu and L. Na-na, 2009. An improved lightweight RFID protocol using substring. Proceedings of the 5th International Conference on Wireless Communications, Networking and Mobile Computing, Sep. 24-26, China, pp: 1-4.

Lei, H., L. Xin-mei, J. Song-he and C. Zeng-yu, 2010. 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, March 6-7, Automation and Robotics, China, pp: 269-272.

Lo, S.K.C., H.C. Keh, Y.H. Lin and W. Jo-Chi, 2009. Integrated the intelligent agent behavior model and billing service into communication system. Inform. Technol. J., 8: 668-677.

Madan, M. and V. Potdar and E. Chang, 2006. Recovering and restoring tampered RFID data using steganographic principles. Proceedings of the IEEE International Conference on Information Technology, Dec. 15-17, Mumbai, pp: 2853-2859.

Melski, A., L. Thoroe and M. Schumann, 2007. Managing RFID data in supply chains. Int. J. Internet Protocol Technol., 2: 176-189.

Potdar, V. and E. Chang, 2006. Tamper detection in RFID tags using fragile watermarking. Proceedings of the International Conference on Industrial Technology, Dec. 15-17, Mumbai, India, pp: 2846-2852.

Sarma, S.E., S.A. Weis and D.W. Engels, 2003. RFID systems, security and privacy implications. Proceedings of the 4th International Workshop on Cryptographic Hardware and Embedded Systems, (IWCHES'02), Spring-Verlag, Berlin, pp: 454-469.

Shieh, G. and W.B. Horng, 2008. Efficient and complete remote authentication scheme with smart cards. Proceedings of the IEEE International Conference on Intelligence and Security Informatics, June 17-20, Taipei, pp: 122-127.

Suzuki, S. and M. Harrison, 2006. Data Synchronization Specification. Auto-ID Labs AEROID-CAM-007, 2006.

Tsudik, G., 2006. YA-TRAP: Yet another trivial RFID authentication protoco. Proceeding of the 4th IEEE International Conference on Pervasive Computing and Communications Workshops, March 13-17, IEEE Computer Society Press, IEEE Pisa, pp: 640-643.

Tuyls, P. and L. Batina, 2006. RFID-tags for anti-counterfeiting. Top. Cryptol. CT-RSA, 3860: 115-131.

Van Le, T., M. Burnmester and B. de Medeiros, 2007. Universally composable and forward secure RFID authentication and authenticated key exchange. Proceedings of the 2nd ACM Symposium on Information, Computer and Communications Security, (ASIACCS'07), ACM, New York, USA., pp: 242-252.

Wang, C.H. and S. Chin, 2009. A new RFID authentication protocol with ownership transfer in an insecure communication environment. Proceedings of the 9th International Conference on Hybrid Intelligent Systems, (ICHIS'09), IEEE Computer Society Washington, DC., pp: 486-491.

Wang, S.P., Q.M. Ma, Y.L. Zhang and Y.S. Li, 2010. HMAC-Based RFID authentication protocol. Proceedings of the 2nd International Symposium on Information Engineering and Electronic Commerce, July 23-25, Ternopil, China, pp: 1-4.

Wang, Y.Y., J.Y. Liu, F.X. Xiao and J. Dan, 2009. A more efficient and secure dynamic ID based remote user authentication scheme. Comput. Commun., 32: 583-585.

Weis, S., S. Sarma and R. Rivest, 2003. Security and privacy aspects of low-cost radio frequency identification systems. Int. Conf. Security Pervasive Comput., 3: 454-469.

Wong, K., P. Hui and A. Chan, 2006. Cryptography and authentication on RFID passive tags for apparel products. Comput. Ind., 57: 342-349.

Wu, K., E. Bai and W. Zhang, 2009. A hash based authentication protocol for secure mobile RFID systems. Proceedings of the 1st International Conference on Information Science and Engineering, Dec. 26-28, Nanjing, pp: 2440-2443.

Yamamoto, A., S. Suzuki, H. Hada, J. Mitsugi, F. Teraoka and O.A. Nakamura, 2008. Tamper detection method for RFID tag data. Proceeding of IEEE International Conference on RFID, April 16-17, Las Vegas, NV., pp: 51-57.

Yeh K.H. and N.W. Lo, 2010. Improvement of two lightweight RFID authentication protocols. Inf. Assur. Secur. Lett., 1: 6-11.

Zahrani, M.S., 2010. The benefits and potential of innovative ubiquitous learning environments to enhance higher education infrastructure and student experiences in Saudi Arabia. J. Applied Sci., 10: 2358-2368.

Zhang, K., T. Zhang and S. Pande, 2006. Memory protection through dynamic access control. Proceedings of the 39th Annual IEEE/ACM International Symposium on Microarchitecture, Dec. 9-13, Orlando, FL., pp: 123-134.

Zhang, X., J. Crabtree, Y. Huang and T. Hu, 2011. Building a dynamic RFID data-driven supply chain management system: imperatives and guidelines. Inform. Technol. J., 10: 703-709.

Zhong, S. and Y.R. Yang, 2006. Verifiable distributed oblivious transfer and mobile agent security. J. Mobile Networks Appl., 11: 201-210.

Zhu, W., D. Wang and H. Sheng, 2005. Mobile RFID technology for improving m-commerce. Proceedings of the IEEE International Conference on e-Business Engineering, Oct. 18-21, Beijing, China, pp: 118-125.