DUJASE Vol. 2(2) 153-159, 2014 (January)

A Group-based Authentication Protocol using Varying Identifiers for RFID Systems

Md. Monzur Morshed[1], Anthony Atkins[2] and Hongnian Yu[3]

[1]Department of Accounting and Information Systems, University of Dhaka, Dhaka-1000

[2]Faculty of Computing, Engineering and Sciences, Staffordshire University, Beaconside, Stafford, UK

[3]School of Design, Engineering and Computing, Bournemouth University, Poole, UK

E-mail: mmmorshed@yahoo.com, a.s.atkins@staffs.ac.uk, yuh@bournemouth.ac.uk

Received on 24. 07. 2012. Accepted for publication on 16. 09. 2013.

Abstract

The use of RFID tags may cause various privacy and security problems of users carrying the tag. The possible privacy threats are information leakage of a tag, traceability of the consumer, denial of service attack, and impersonation of a tag. To enhance the privacy and security of the RFID systems some RFID systems authentication protocols protect privacy and security by changing its identifier and other secret numbers. These protocols do not consider a large system that may divide the tags in many groups. This paper proposes a new group-based authentication protocol which provides the privacy and security in a more efficient manner using varying identifiers. The protocol recovers from unexpected lack of synchronization due to incomplete authentication process or abnormal termination of communication. The proposed protocol requires lower computations which is suitable for RFID systems and offers larger ranges of security protection.

Keywords: RFID, security, privacy, varying identifier, recovery, authentication protocol.

1. Introduction

Radio Frequency Identification (RFID) tags are used in many applications such as in supply-chain management, automation of automobiles, animal tracking, highway toll collection etc [1]. Each RFID tag contains a unique identifier to serve as object identity so that this identity can be used to relate information about the corresponding object. The unique serial number in an RFID tag causes privacy and security problems for the tag holder. The RFID tag can be tracked by an adversary without the knowledge of the tag holder [1]. The RFID systems should be designed to keep the data secret and to protect the communication between the reader and the tag from various attacks. The identified privacy and security threats to the RFID systems are information leakage of a tag, traceability and location privacy, Denial of Service attack and impersonation of a tag etc. Implementation of conventional cryptography is not possible in a low-cost RFID tag due to its limited processing capability and memory. It is a challenging problem to construct an efficient authentication protocol for RFID systems since an RFID tag with approximately 4000 gates is considered low-cost which is limited in computation power, storage and communication capabilities [2-5]. Recently authentication protocols for the RFID systems received attention to protect the systems from privacy and security attacks due to the increasing uses in various applications.

There are varieties of authentication protocols using hash functions to protect the RFID systems from various privacy and security attacks [6-19]. Some protocols use static identifiers to ensure that it can work suitably in ubiquitous environment. Some researchers have proposed privacy and security protocols for RFID systems using varying identifiers to enhance privacy and security specially location privacy [6, 7, 8, 12, 13]. Due to varying identifiers they include the recovery from desynchronization due to incomplete authentication process. However, due to the hash function using the identifier if one authentication process is unsuccessful it is not changed and an adversary can use the fixed response in the subsequent authentication process to break the security. These protocols suggested to store all the tag information in one group and did not classify the tags to reduce the search time.

This paper proposes a new Group-based Authentication Protocol using Varying Identifiers (GAPVI) to address these issues and to present an efficient and secure protocol for RFID systems which can recover from unexpected lack of synchronization due to incomplete authentication process for abnormal termination. The protocol uses varying identifier, one-way hash function, two random numbers to make the response unpredictable and to enhance the location privacy of the RFID systems. The paper is organized as follows. Section 2 reviews the related works. In Section 3 the new protocol is presented. Section 4 presented the simulation results. In Section 5 the privacy, security and efficiency of the protocol is evaluated. In Section 6 the conclusion is given.

2. Related Works

There are varieties of hash-based RFID authentication protocols for the privacy and security of the RFID systems using a one-way hash functions. The protocols work with static identifiers to protect privacy and security so that they can work better in pervasive computing environment [9, 10,

11]. However, the protocols with static identifiers either using computationally expensive hash functions and large storage areas or are suffering from privacy and security problems [10, 11, 18].

The general idea for changing the identifier after each authentication process is to enhance the privacy and security by making the response more unpredictable. To protect the RFID tags and the reader in an efficient and effective way varying identifiers are used in many authentication protocols. Chien and Chen [12] proposed a challenge-response based authentication protocol to prevent a replay attack. This protocol uses a database in a server which maintains new and old tag keys to protect a DoS attack. To prevent a traceability authentication key and access keys are updated. However, this scheme is still vulnerable to backward and forward traceability. If an active adversary can compromise a tag it can identify the tag's past interactions from previous transactions and the fixed identifier of the tag. Using the past transaction and fixed identifier it would be able to identify any future transaction. Ohkubo et al. [13] proposed a RFID privacy scheme using a hash chain (HC) mechanism. This method used two hash functions to protect the privacy and security. It is also not suitable in practical use because the back-end database requires a large number of hash chains. Henrici et al. [6] proposed a scheme which is called the hash-based identifier variation scheme (HIDV). It uses one way hash function to protect location privacy by changing the ID after each session. However, if any authentication session is unsuccessful it replies with the same hashed ID again for which it opens up the vulnerability for impersonation attack like spoofing. Lee et al. [7] proposed a low-cost authentication protocol (LCAP) which simplifies and enhances the HIDV scheme in both efficiency and security. It also has the similar problem as in HIDV that is a tag always replies with the same hashed *ID* before the next successful authentication which allows tag tracking and breaks the location privacy of the tag [12].

The protocols with varying identifiers have the privacy and security problems since these cannot eliminate all the threats [6-8, 12-15]. Another problem is that the protocols did not consider the groups of the tags and require considerable search time and hash computations. To enhance the privacy and security protection of the RFID systems we propose a new protocol in the next section with the following features:

1. It is a group-based authentication protocol using varying identifier that reduces computation and search time.
2. It uses one-way hash functions and two random numbers to make the response secure and unpredictable.
3. It eliminates the existing privacy and security problems.
4. It requires low storages, computation and communication costs that are suitable for low-cost RFID tags.

3. A Group-based Authentication Protocol using Varying Identifiers (GAPVI)

In this section, a new protocol GAPVI is proposed which is based on the challenge-response method using the one-way hash function and random numbers in the RFID systems. This supports recovery in case of desynchronization due to incomplete authentication process with less computation and protects the systems from location privacy effectively.

3.1 Notations

The notations used in this protocol are as follows:

h	A one-way hash function, $h:\{0,1\}^* \rightarrow \{0,1\}^l$
l	The length of an identifier
r_1	Random number in $\{0,1\}^l$
r_2	Random number in $\{0,1\}^l$
ID	Tag identifier
ID_{Prev}	Previous tag identifier
HID	Hash address
HID_{Prev}:	Previous value of the hash address
GI	Secret group index
$\oplus$	XOR operator
$\|\|$	Concatenation operator
$\leftarrow$	Assignment operator

3.2 System Set-up

Tag: Each tag contains the following fields: *ID*, *GI*
Reader: Reader does not contain any fields.
Back-end Database: Back-end database contains the following fields: *ID*, *HID*, *GI*, HID_{Prev}, ID_{prev}

3.3 GAPVI Operations

When a tag enters into the range of the reader, this can initiate the authentication protocol. The protocol is shown in Fig. 1.

The steps in the authentication protocol are as follows:

1. A reader selects a random number r_1 and sends a request with r_1 to the tag.

2. After receiving the random number r_1 the tag will generate another random number r_2.

The tag computes $A \leftarrow GI \oplus r_2$

$B \leftarrow h(ID) \oplus (GI + (r_1 \oplus r_2))$

$C \leftarrow h(ID \| r_1 \| r_2)$, and sends the value of A, B, C_L to the reader.

Where C_L=Left half of C and C_R=Right half of C

3. The reader then sends A, B, C_L, r_1 to the back-end database.

4. The database computes $r_2 \leftarrow GI \oplus A$,

$HID \leftarrow B \oplus (GI + (r_1 \oplus r_2))$ for all GI values

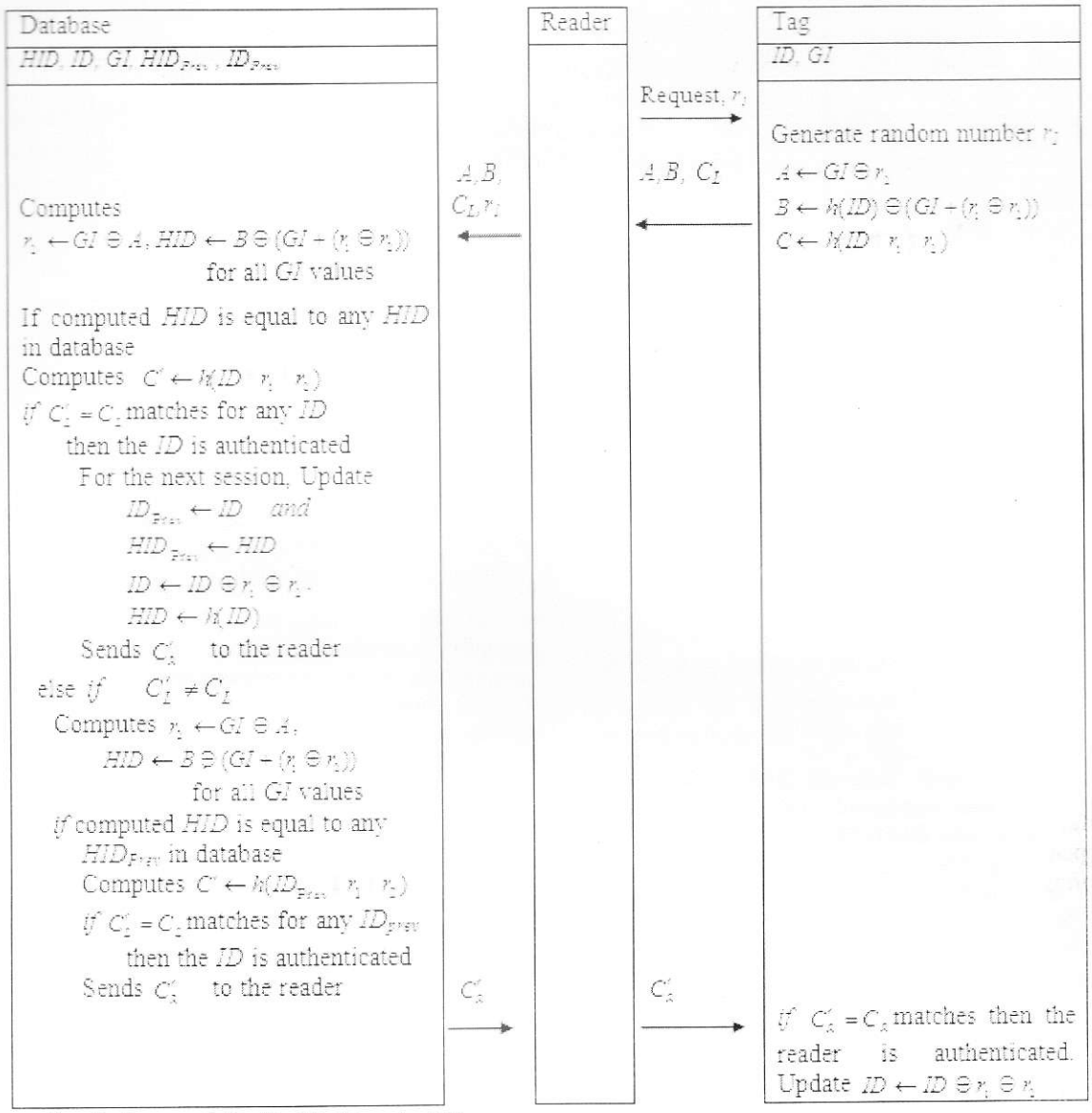

Fig. 1. GAPVI Protocol

If computed HID is equal to any HID in the database then pick the ID and computes $C' \leftarrow h(ID \| r_1 \| r_2)$

if $C'_L = C_L$ matches for any ID then the ID is authenticated,

where C'_L=Left half of C' and C'_R=Right half of C'

For the next session, update

$$ID_{\text{Prev}} \leftarrow ID\ ,\quad HID_{\text{Prev}} \leftarrow HID\ ,$$
$$ID \leftarrow ID \oplus r_1 \oplus r_2,\ HID \leftarrow h(ID)$$

Sends C'_R to the reader

else *if* $C'_L \neq C_L$

Computes $r_2 \leftarrow GI \oplus A$,

$HID \leftarrow B \oplus (GI + (r_1 \oplus r_2))$ for all GI values

if computed HID is equal to any HID_{Prev} in database computes $C' \leftarrow h(ID_{\text{Prev}} \| r_1 \| r_2)$

if $C'_L = C_L$ matches for any ID_{Prev} then the ID is authenticated.

Sends C'_R to the reader

5. The reader forwards C'_R to the tag.

6. *if* $C'_R = C_R$ matches then the reader is authenticated. Update $ID \leftarrow ID \oplus r_1 \oplus r_2$

Table 1: Attacker's Success Table

Exp No	Number of Queries to the Tag	Data/ Secret Size (bits)	Number of Matches		
			EOHLCAP[18] (Static ID)	LCAP (Varying ID)	GAPVI (Varying ID)
1	10^{11}	16	1539054	1528976	1511114
2	10^{11}	16	1536078	1527463	1505568
3	10^{11}	32	0	0	0
4	10^{11}	32	43	0	0
5	10^{11}	32	0	0	0
6	10^{11}	32	0	0	0
7	10^{11}	64	0	0	0
8	10^{11}	64	0	0	0
9	10^{11}	64	0	0	0

Table 2: Summary of the Experiment

Data/Secret size	EOHLCAP[18]	LCAP	GAPVI
16 bits	Not secured	Not secured	Not secured
32 bits	Not secured	**Secured**	**Secured**
64 bits	**Secured**	**Secured**	**Secured**

The analysis and description of the proposed protocol will be presented in the Section 5.

4. Simulation Result

To validate the proposed protocol GAPVI, simulation experiments have been conducted. The objective of the simulation program was to check the anonymity of the response for one tag. The output of a hash function is the same for the same random number pair. The objective is to ensure unique response for different inputs of random number pair so that an adversary is unable to use any responses at later stage to access the tag or the reader. The program picks a response from a tag and checks it to match with the responses for different sets of random numbers. The randomness of the numbers is tested for uniform random distribution using Monte Carlo Simulation method. Table 1 demonstrates some simulation results to show the number of matches of a response which also indicates the attacker's success to access the tag. We selected EOHLCAP which uses static identifier to protect the privacy and security of the RFID systems to compare with our proposed protocol. The simulation is conducted for 16, 32 and 64 bits of secrets, random number and data. The results shown in Table 1 indicates that for 32 and 64 bits there is no matching response and the responses are always unique for the proposed protocol but for EOHLCAP this unique response is obtained only for 64 bits. The proposed protocol ensures better security protections for 32 bits as it updates the *ID* after each authentication process which makes the response more unpredictable. The secure zones for the two protocols are shown in the shaded cells. For 16 bits there were some recurrences of the same response for both the protocols. The recurrence of the same response is due to two reasons. Firstly it produces the same random number pairs and secondly it produces similar responses for some other combination of random number pairs.

Table 2 shows the summary of the evaluation. For each data/secret size we conduct 20 experiments each of which attempts 10^{11} times. For each protocol the possible security zone is identified. It is determined by the size of the secret size or length where the match is not found. It is assumed secured if the same tag response is not generated during 10^{11} attempts.

This experiment shows that the proposed protocol is secure for 32 and 64 bits in 10^{11} attempts shown in shaded cells in Table 2. For 16 bits there were some recurrences of the same response that can be used by an adversary. However, the EOHLCAP is not secure for 32 bits of data and secret values.

5. Privacy Security and Efficiency Analysis

To evaluate the proposed protocol privacy, security and efficiency will be analysed. The attack model is defined as Γ:An adversary, *R*: Reader, *T*: Tag.

It is assumed that the adversary disguises as a reader R_Γ and ID_Γ, GI_Γ will be used by the adversary as fake *ID* and secret *GI* respectively.

5.1 Privacy and Security Analysis

The privacy and security of the proposed protocol is analysed against various threats such as information leakage of a tag, location privacy, impersonation of a tag, Denial of Service attack and traceability and are outlined as follows:

Information Leakage: In this protocol to be able to obtain any sensitive information from a tag the adversary Γ must be authenticated. To authenticate the system an adversary Γ must know *ID, GI* and the hash function to get any

information from the tags. The combination of r_1 and r_2 with GI and ID makes the response C so unpredictable that the adversary can only guess the value or use a brute-force technique with an advantage of only $\frac{1}{2^l}$, which is negligible. From the responses $B \leftarrow h(ID) \oplus (GI + (r_1 \oplus r_2))$ and $C \leftarrow h(ID \| r_1 \| r_2)$ of the tag the adversary cannot extract the value of ID.

Location Privacy: The value of B and C cannot be linked with any particular tag. The protocol ensures location privacy by using new values of r_1, r_2 each time. The identifier ID is also updated after each authentication session. Even if a malicious reader sends the same random value r_1 all the times, a tag transmits the refreshed value using r_2 and GI. The adversary Γ can receive the response from the tag in one session.

$$T \Rightarrow \Gamma : h(ID \| r_1 \| r_2)$$

In the next session the adversary Γ will receive a different response from the tag since the ID, r_1, and r_2 are all changed, hence the responses are not matched. In subsequent all sessions the responses from the tag are anonymous hence location privacy is protected and tracking is not possible.

Impersonation and Replay Attack: When a tag reaches within the range of a reader, the reader queries with a random value to the tag. An adversary may disguises as a reader R_Γ and may make a request to a tag with a random number. However, without knowing the ID, the hash function, secret GI an adversary is unable to impersonate. After each session the ID is updated internally to a new value. The value of secret GI is passed always secretly. The adversary can only guess the value of ID and GI and use the fake ID_Γ and GI_Γ to authenticate the tag. However, for each session the tag generates a new value of the responses A, B *and* C with new ID and random numbers which are totally indistinguishable and different from other session and subsequently the impersonation and replay attacks are not possible.

Message Interception: The protocol recovers from the abnormal interruption of the authentication process. If the adversary is able to prevent the last transmission to the tag from the reader then the tag will not authenticate the reader in that session. In the next authentication phase it will use a new random number to authenticate and the database will use the previous ID_{prev} to authenticate and synchronous the system. For example the database will use HID_0, ID_0 instead of HID_1, ID_1 to authenticate the tag as shown as follows:

Database($HID, ID, GI, HID_{Prev}, ID_{prev}$)	**Tag**(ID, GI)
$HID_1, ID_1, GI, HID_0, ID_0$	ID_0, GI

Traceability: An adversary is unable to identify the tag from its response because each time it gives a different value which is non traceable from other responses. This scheme is fully protected from the future forward and backward traceability. The adversary has no control over r_2, and the combination of r_1, r_2 and hash function and also does not know the ID and group secret value GI. Consequently, the previous, present and future interactions are all indistinguishable.

The summary of the privacy and security properties is given in Table 3. The privacy and security properties of GAPVI are compared with four other schemes HIDV, LCAP, RoAP and EOHLCAP. The three schemes HIDV, LCAP, RoAP were chosen because all of these protocols involved tag authentication and involve secret update process after each successful authentication. The protocol EOHLCAP was chosen from static ID group since it offers better privacy and security options. The table shows that the proposed protocol provided protections from all the identified privacy and security threats. Some of the privacy and security properties are further tested by simulation program and outlined in section 4.

5.2 Efficiency Analysis

Storage, communication and computation cost are considered for efficiency analysis. Various existing authentication protocols are compared with the proposed GAPVI authentication protocol. HIDV [6] requires larger storages and computations than other protocols and suffers from location privacy issues. It is also vulnerable to impersonation attack. LCAP [7] appears to be better in performance however, it has location privacy problem. The GAPVI protocol shows improved performance as shown in Table 4 because it requires comparable tag side and database side storage with other protocols and gives protection from the all attacks discussed in Section 6.1. The storage requirement for the tag and the database are $2l$ and $5l$ respectively. The protocol requires low hash computations in both the tag and the database as shown in Table 4. RoAP [16] gives protections from all the attacks but it needs $\frac{N+1}{2}$ functions and 2 hash operations which is costly because the value of N may be very high and require many hash computations that will make the protocol slower. Table 4 gives an overall comparison of the different protocols compared to the proposed GAPVI. Due to the group-based searching it reduces the number of search operations to identify the tag. It also avoids hash computations using low-cost xor operations to reduce the computational overhead in the database side.

Table 3: Privacy and Security Comparisons

Property	HIDV[6] (Varying ID)	LCAP[7] (Varying ID)	RoAP[16] (Varying ID)	EOHLCAP[18] (Static ID)	GAPVI (Varying ID)
Information privacy	Y	Y	Y	Y	Y
Location Privacy	N	N	Y	Y	Y
Impersonation	N	A	Y	Y	Y
Replay attack	N	Y	Y	Y	Y
Message Interception	Y	Y	Y	Y	Y
Backward Traceability	N	Y	Y	Y	Y
Forward Traceability	N	Y	Y	Y	Y

*Y: Protected A: provided under assumption N: Not Provided

Table 4. Efficiency Analysis

Efficiency Criteria		HIDV[6] (Varying ID)	LCAP[7] (Varying ID)	RoAP[17] (Varying ID)	EOHLCAP[18] (Static ID)	GAPVI (Varying ID)
Storage	Tag	$3l$	$1l$	$2l$	$3l$	$2l$
	Reader	-	-	-	-	-
	Database	$10l$	$6l$	$3l$	$3l$	$5l$
Computation	Tag	$3h$	$2h$	$2h+f$	$1h+\mu$	$2h$
	Reader	-	-	-	-	-
	Database	$3h+\varepsilon$	$2h+\varepsilon$	$(\frac{N}{2}f+2h)+\varepsilon$	$(\frac{m_i+1}{2})h+\varepsilon$	$1h+\varepsilon$
Communication	Tag-to-Reader	$3l$	$1.5l$	$2l$	$2.5l$	$2.5l$
	Reader-to-tag	$2l$	$0.5l$	l	$0.5l$	$0.5l$

ε: Small operation in back-end database μ: small operation in the tag side h: hash operation f: Function operation
N: Total number of tags, m_i: number of tags in the ith group

6. Conclusion

A new efficient and secure authentication protocol GAPVI is proposed to protect privacy for low-cost RFID systems. The proposed group-based protocol uses a varying identifier to provide effective privacy and security with recovery of the identifier to maintain synchronization. Due to the group-based design it requires less computation and search time to authenticate a tag. The proposed protocol is protected from privacy and security threats which is evaluated by mathematical and logical analysis and is shown in Table 3. It enhances the location privacy of the tag by transmitting the hash address *HID* encrypting with a secret random number and a group secret value. The proposed scheme requires only two one-way hash functions in the tag and only one hash computation in the database making it highly efficient. The storage requirement for the tag and database is also cost efficient for an authentication protocol using varying identifiers. The comparison outlined in the analysis of Tables 3 and 4 shows that the proposed protocol is both secure and efficient compared to the other protocols for a large number of RFID tags. It has practical advantages over these protocols because it is simple and provides a larger range of privacy and security protections.

References

1. Jules, A., Garfinkel, S., Pappu, R., 2005. 'RFID privacy: an overview of problems and proposed solutions', IEEE Security and Privacy, , May/June, 3(3): pp. 34-43.
2. Jules, A., 2006. 'RFID security and privacy: A research survey', IEEE Journal on Selected Areas in Communication, 24(2), February, pp. 1-19.
3. Sun, H.M., Ting, W.C., 2009. 'A Gen2-based RFID authentication protocol for security and privacy', IEEE Trans. Mob. Comput., 8, (8), pp. 1052–1062.
4. Want, R., 2005. 'An Introduction to RFID Technology', IEEE Pervasive Computing, vol 5, pp. 25 – 33.
5. Weis, S.A., Sarma, S.E., Rivest, R.L., Engels, D.W., 2004. 'Security and privacy aspects of low-cost radio frequency identification systems', Secur. Pervasive Comput., 2802, pp. 201–212.
6. Henrici, D., Muller, P., 2004. 'Hash-based enhancement of location privacy for radio-frequency identification devices using varying identifiers', In R. Sandhu and R. Thomas, editors, International Workshop on Pervasive Computing and Communication Security -PerSec 2004, Orlando, Florida, USA, March. IEEE Computer Society, pp. 149–153.
7. Lee, S.M., Hwang, Y.J., Lee, D.H., Lim, J.I., 2005. 'Efficient Authentication for Low-Cost RFID systems', ICCSA05, vol. 3480 LNCS, Springer-Verlag, pp. 619-629.

8. Song, B., Mitchell, C. J., 2008. 'RFID authentication protocol for low-cost tags', In *WISEC*, pp. 140-147.

9. Molnar, D., Wagner, D., 2004. 'Privacy and security in library RFID: Issues, practices, and architectures', In B. Pfitzmann and P. Liu, editors, Conference on Computer and Communications Security - ACM CCS, Washington, DC, USA, October. ACM Press, pp. 210–219.

10. Rhee, K., Kwak, J., Kim, S., Won, D., 2005. 'Challenge-Response Based RFID Authentication Protocol for Distributed Database Environment', SPC 2005, LNCS 3450, pp. 70-84.

11. Choi, E.Y., Lee, S.M., Lee, D. H., 2005. 'Efficient RFID Authentication Protocol for Ubiquitous Computing Environment', Embedded and Ubiquitous Computing, vol.3832, pp.945-954.

12. Chien, H., Chen, C., 2007. 'Mutual authentication protocol for RFID conforming to EPC class 1 generation 2 standards', Computer Standards & Interfaces, 29(2), February, pp.254–259.

13. Ohkubo, M., Suzki, K., Kinoshita, S.,2003. 'Cryptographic approach to "privacy-friendly" tags', In RFID Privacy Workshop, MIT, MA, USA, November. http://www.rfidprivacy.us/2003/agenda.php.

14. Dimitriou, T., 2005. 'A lightweight RFID protocol to protect against traceability and cloning attacks', In Conference on Security and Privacy for Emerging Areas in Communication Networks - SecureComm, Athens, Greece, September. IEEE, pp. 59–66.

15. Song, B., 2008, 'RFID Tag Ownership Transfer', In *4thWorkshop on RFID Security (RFIDsec 08)*, Budaperst, Hungary, July.

16. Hoque, M.E., Rahman, F., Ahamed, S.I., 2009. 'Supporting Recovery, Privacy and Security in RFID Systems Using A Robust Authentication Protocol', Proceedings of the 2009 ACM symposium on Applied Computing, *SAC'09*, Honlulu, Hawaii,USA. pp.1062-1066.

17. Cai, S., Li, Y., Li, T., Deng, R. H., 2009. 'Attacks and Improvements to an RFID Mutual Authentication Protocol and its Extensions', *WiSec'09*, March 16–18, Zurich, Switzerland, pp. 51-58.

18. Ha, J., Moon, S., Nieto, J.M.G., Boyd, C., 2007. 'Security Analysis and Enhancement of One-Way Hash Based Low- Cost Authentication Protocol', Emerging Technologies in Knowledge Discovery and Data Mining, vol.4819, pp.574-583.

19. Morshed, M.M., Atkins, A., Yu, H., 2012. 'Secure Ubiquitous Authentication Protocols for RFID Systems', Eurasip Journal on Wireless Communications and Networking, March, pp.1-13.