International Journal of Automation and Computing 9(3), June 2012, 257-265
DOI: 10.1007/s11633-012-0642-4

An Efficient and Secure Authentication Protocol for RFID Systems

Md. Monzur Morshed Anthony Atkins Hong-Nian Yu
Faculty of Computing, Engineering and Technology, Staffordshire University, Stafford ST18 ODF, UK

Abstract: The use of radio frequency identification (RFID) tags may cause privacy violation of users carrying an RFID tag. Due to the unique identification number of the RFID tag, the possible privacy threats are information leakage of a tag, traceability of the consumer, denial of service attack, replay attack and impersonation of a tag, etc. There are a number of challenges in providing privacy and security in the RFID tag due to the limited computation, storage and communication ability of low-cost RFID tags. Many research works have already been conducted using hash functions and pseudorandom numbers. As the same random number can recur many times, the adversary can use the response derived from the same random number for replay attack and it can cause a break in location privacy. This paper proposes an RFID authentication protocol using a static identifier, a monotonically increasing timestamp, a tag side random number and a hash function to protect the RFID system from adversary attacks. The proposed protocol also indicates that it requires less storage and computation than previous existing RFID authentication protocols but offers a larger range of security protection. A simulation is also conducted to verify some of the privacy and security properties of the proposed protocol.

Keywords: Radio frequency identification (RFID), security, privacy, timestamp, authentication protocol

1 Introduction

Radio frequency identification (RFID) is going to be a part of our everyday life in near future. RFID tags are used in many applications such as in supply-chain management, logistics, waste management, automation of automobiles, animal tracking, healthcare industry and highway toll collection, etc.[1] Many large organizations like Wal-Mart, Procter and Gamble, and the United States Department of Defence are deploying RFID systems for proper control and management of their supply chains[2]. Due to the dropping cost and the improvement in the standardization of RFID tags it is emerging as the successors of optical barcodes in many places. RFID tags have some advantages over optical barcodes that make it more suitable in automation. A barcode indicates the type of the object on which it is printed but the RFID tag gives a unique serial number that distinguishes the object uniquely from many millions of similar types of products. Another advantage of an RFID tag is that it does not requires line-of-sight contact with the readers as in optical barcodes.

RFID is a technology to identify objects or people automatically. An RFID tag is standardized as an electronic product code (EPC) tag by the organization EPCglobal Inc.[3] An RFID system consists of three components: tag, reader, and back-end database[2, 4]. A typical RFID system is shown in Fig. 1. An RFID tag is a small and extremely low-priced device consisting of a microchip with limited functionality and data storage and antenna for wireless communication with the readers. It transmits data in the air in response to the interrogation by an RFID reader. RFID tags can be passive or active depending on the powering technique[5]. In general, passive tags are inexpensive. They have no on-board power; they get power from the signal of the interrogating reader[2]. Active tags contain batteries to power their transmission. Active tags can initiate communications and have read ranges of 100 m or more. Active tags are expensive and physically larger and hence not suitable for many applications. RFID readers are devices used to read or write data from or to RFID tags. A back-end database has information about the tags.

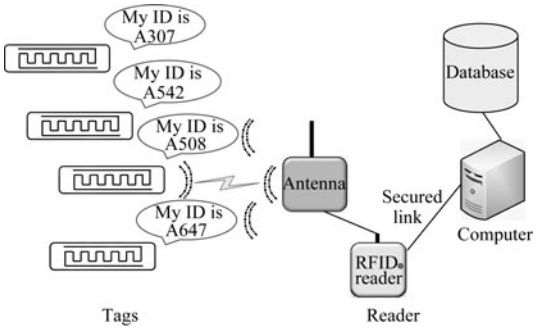

Fig. 1 A typical RFID System

Each RFID tag contains a unique identifier to serve as object identity so that this identity can be used as a link to relate information about the corresponding object. Due to this unique serial number in an RFID tag it is possible to track the tag uniquely and the information in it is vulnerable to an adversary. Products labelled with RFID tags contain unique identifiers. It allows tracking of persons through the tags they carry without their knowledge[1]. Moreover, implementation of conventional cryptography is not possible in a low-cost RFID tag due to its limited processing capability and memory limitations[6]. The major privacy and security issues in a RFID system to be investigated in this paper are as follows:

Information leakage: In a typical RFID system, a tag has a unique identifier that is transmitted to the reader. So it can be easily identified with this unique serial number. Due to this unique serial number, the information in it is

Manuscript received June 15, 2011; revised September 18, 2011

vulnerable to an adversary. For the protection from information leakage, an RFID system needs to provide privacy control so that unauthorized readers cannot access the tags.

Location privacy: If any value can be related or linked to a tag then it is possible to track the tag. If a tag transmits any fixed response to a reader, an adversary may try to distinguish it from other response. If an adversary can do it, he can find the location of the user.

Impersonation and replay attack: The communication between the tag and the reader is insecure. If an adversary can collect the information during communication from the tag and the reader they can impersonate the tag to explore more information. An adversary can use this information and perform replay attack in the future.

Message interception or denial of service (DoS): An adversary may try to block or prevent authentication between a valid reader and tags. If the adversary can successfully block the transmission, this can cause the server and the tag to lose synchronization. The RFID system should be able to handle this to keep the synchronization of the tag and the reader.

Backward and forward traceability: If the internal state of the tag is known then it can help to identify the tag interactions of past and future communications.

Many researchers have proposed efficient protocols for RFID systems authentication. These protocols can be classified into two categories. First is the hash function based security protocols[4, 7−15]. Second is the lightweight XOR based security protocols[16−24].

The hash function h is defined as $y = h(x)$, where $h(x)$ is a cryptographic one-way function. Ideally, besides the function being difficult to invert, the output y should not reveal any substantial information on its pre-image x [25]. Hash function based protocols mostly use random numbers to make the response anonymous. To make the response more anonymous and reliable two random numbers are used in many protocols. One is from the reader side and the other is from the tag side.

Lightweight encryption protocols require an XOR based binary operation for authentication. In most of the XOR based protocols, it requires many rounds to authenticate each other.

Some researchers have proposed hash-based privacy and security protocols for RFID systems using varying identifiers[4, 7, 16]. These are secured from most of the attacks. Due to varying identifiers, they include the recovery from desynchronization due to incomplete authentication process. However, due to the hash function of the constant identifier during this period it gives a fixed value. If one authentication process is unsuccessful, an adversary can use the response later in the subsequent phases to break the security. In this case, the adversary can use the response for impersonation and replay attack and also can break the location privacy. Many current available hash based protocols[8−10] used static identifiers and secret values to ensure privacy and security.

To address the above issues, this paper proposes an efficient and secure authentication protocol (ESAP) based on the challenge-response method using a one-way hash function, a static identifier, a random number and a timestamp in the RFID systems. The objective of this protocol is to overcome the privacy and security problems of the existing protocols with less storage and computations. In this protocol, a monotonically increasing timestamp ensures anonymity of the response. The purpose of the hash function is to give a one-way hash result so that an adversary cannot figure out the input from the output. The purpose of the random number is also to make the response anonymous. The monotonically increasing timestamp ensures unique combination of the hash input that makes the function output more anonymous. This protocol protects the privacy and security of RFID systems of the issues outlined above.

The paper is organized as follows. Section 2 reviews the related works. In Section 3, a new protocol is proposed. In Section 4, the privacy, security and efficiency of the protocol are evaluated. In Section 5, the simulation results and evaluations are presented. The Section 6 shows the application of the proposed protocol. Finally, in Section 7 conclusions are given.

2 Related works

There are varieties of RFID authentication protocols for the privacy and security of the RFID systems. Some protocols work with a varying identifier and some works with a static identifier.

2.1 Protocols with varied identifiers

To protect the RFID tags and the reader in an efficient and effective way varying identifiers are used in many authentication protocols[4, 7, 11−14, 16, 17]. This paper focuses on two protocols using varying identifiers and secret numbers for the authentication and is outlined as follows.

Henrici and Muuer[7] proposed a scheme which is called the hash-based identifier variation scheme (HIDV). The notations used in this protocol are shown in Table 1.

Table 1 Notations used in HIDV

Notations	Descriptions
$DB-ID$	Database-identifier
ID	Current ID
HID	Hash of ID acting as a primary index of the table
TID	Transaction number
LST	Last successful transaction number
ΔTID	$=TID-LST$
AE	Associated DB entry
$DATA$	A reference to tag data / user data
RND	A random number

The operations of the HIDV protocol are shown in Fig. 2. It uses a one-way hash function h 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 tracking and location privacy[11]. In addition, this scheme is not secure against impersonation attack[10].

Lee et al.[4] proposed a low-cost authentication protocol (LCAP) shown in Fig. 3 which simplifies and enhances the HIDV scheme in both efficiency and security. The notations and symbols used in LCAP operation are as follows:

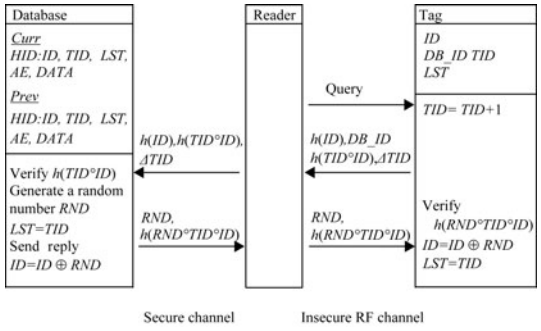

Fig. 2 The HIDV message exchange[6]

h: $\{0, 1\}^* \rightarrow \{0, 1\}^l$ is a one-way hash function. h_R is the right half and h_L is the left half of h. A hash function is infeasible to invert and the output hides the information of the input[7, 16].

ID: *ID* denotes identity of a tag and is a random value in $\{0, 1\}^l$.

r: A random number in $\{0,1\}^l$.

HaID: The *HaID* value is the hash value of *ID* used for identifying or addressing the tag.

TD: The *TD*-entry is used to trace previous data information of a tag when loss of message occurs in the current session.

DATA: *DATA* stores the information about an accessible tag.

Data fields of a tag and a reader are initialized to the following values:

Tag: The data field of a tag is initialized to its own *ID*.

Reader: A reader picks uniformly a random number r.

Database: The data fields of a back-end database are initialized to *HaID, ID, TD* and *DATA*.

The back-end database maintains two rows; *Prev* for the previous session and *Curr* for the current session. Each row contains *HaID, ID, TD,* and *DATA* fields.

The operations of the LCAP protocol are shown in Fig. 3.

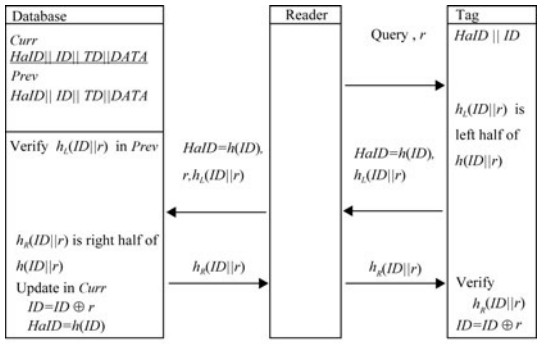

Fig. 3 The LCAP protocol[4]

The steps in LCAP are as follows:

1) A reader selects a random number r and sends a *Query* and r to the tag.

2) The tag computes $HaID = h(ID)$ and $h(ID||r)$ using r and its ID and sends $h_L(ID||r)$ and $HaID$ to the reader, where $h_L(ID||r)$ is the left half of $h(ID||r)$.

3) The reader sends $h_L(ID||r)$, r, and *HaID* to the back-end database.

4) The back-end database then compares if the value of *HaID* in *Prev* is same as the value of *HaID* received from the reader. If successful, then the back-end database computes $h_R(ID||r)$ using r received from the reader and ID in *Prev*, where $h_R(ID||r)$ is a right half of $h(ID||r)$. For the next session, the back-end database computes and stores $HaID = h(ID \oplus r)$ and $ID = ID \oplus r$ in *Curr*. *TD*-field of *Prev* is filled with current $HaID = h(ID \oplus r)$. Finally the back-end database sends $h_R(ID||r)$ to the reader.

5) The reader forwards $h_R(ID||r)$ to the tag.

6) The tag checks $h_R(ID||r)$. If it matches with the computed right part of $h(ID||r)$, the tag updates its ID to $ID \oplus r$.

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[11].

2.2 Protocols with static identifiers

The protocols use static identifiers to protect privacy and security so that they can work better in ubiquitous computing environment[8−10]. Molnar and Wagner[8] proposed a private authentication scheme for a library RFID system. It uses a pseudorandom number and a shared secret key by the tag and the reader for efficient authentication. This scheme does not ensure forward security since the tag′s identifier and the secret key is static and the random number forwarded is in plain text which can be captured by an adversary.

Rhee et al.[9] proposed a challenge-response based RFID authentication protocol (CRAP) which was designed for use in ubiquitous computing. However, this scheme requires to compute $(N/2 + 1)$ hash functions which is impractical for a large number of tags in ubiquitous computing.

Choi et al.[10] proposed a one-way hash based low-cost authentication protocol (OHLCAP), which is suitable for ubiquitous environment. Now, the OHLCAP protocol will be outlined in details since it is the most important work in this area. Notations used in this protocol are shown in Table 2.

Table 2 Notations used in OHLCAP

Notations	Descriptions
h	A one-way hash function, $h : \{0, 1\}^* \rightarrow \{0, 1\}^l$
l	The length of an identifier
r	Random number in $\{0, 1\}^l$
ID	Tag identifier
GI	Group index
GI_i	i-th group index
K	Secret in all tags
S	Tag secret
BL	Left half of the message B
BR	Right half of the message B
c	Counter
$\oplus$	XOR operator
$\|\|$	Concatenation operator

The OHLCAP protocol is shown in Fig. 4. It has the following steps.

Step 1. A reader selects a random value r and sends a query with r to a tag.

Step 2. The tag checks whether the random value r is all zero value or not.

1) If r value is all zero, the tag sends "stop" message to the reader and stop the protocol.

2) Otherwise, the tag performs the following

The tag computes $A^1 = K \oplus c$, $A^2 = ID + (GI_i \oplus r \oplus c) \mathrm{mod}(2^l - 1)$, $B = h(ID||(S \oplus GI_i)||(r \oplus c))$ and sends A^1, A^2 and B_R to the reader, where B_R is a right half of B.

Then, the tag increases the counter c which should not exceed $2^l - 1$.

If the counter c exceeds $2^l - 1$, it is initialized by initial c.

Step 3. After receiving from the tag,

1) The reader forwards A^1, A^2, B_R and r to the back-end database.

2) The back-end database computes $c' = A^1 \oplus K$ and $ID'_j = A^2 - (GI_j \oplus r \oplus c') \bmod (2^l - 1)$ using all group indices GI_j , $j \in \{1, \cdots, n\}$.

3) The Back-end database checks if one of computed $ID'_{j(\in\{1,\cdots,n\})}$ is matching to one of the stored IDs in the back-end database. If this process succeeds, the back-end database checks if the GI_j used to compute equals to the group index GI_i that contains the matching ID'_j.

If this is successful, the back-end database computes $h(ID||(S \oplus GI_i)||(r \oplus c))$ using the matched ID.

Otherwise, the back-end database stops this process.

4) Then, the back-end database authenticates the tag by matching the received value B_R.

5) The back-end database sends B_L to the reader, where B_L is a left half of B. The reader forwards B_L to the tag.

Step 4. The tag authenticates the reader by comparing the received value B_L.

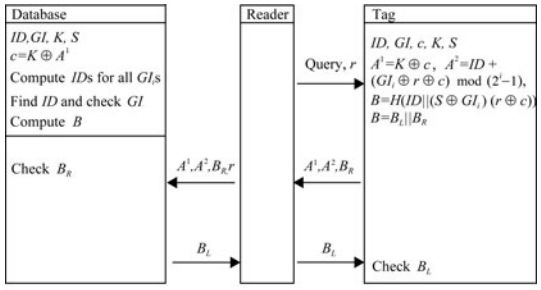

Fig. 4 The OHLCAP protocol[10]

OHLCAP is a novel approach in ubiquitous environment that uses one-way hash function for privacy and security. However, Ha et al.[15] found its security weakness and proposed an enhanced OHLCAP (EOHLCAP) scheme. The authors pointed out that this protocol is vulnerable to traceability attack and impersonation attack because of its special property, namely, $c_{i+1} = c_i + 1$. The adversary eavesdrops the messages transmitted between the tag and reader and obtains the successive A^1_{pre} and A^1_{cur} where $A^1_{\mathrm{pre}} = K \oplus c_i$, $A^1_{\mathrm{cur}} = K \oplus c_{i+1}$. Afterwards, it computes $A = A^1_{\mathrm{pre}} \oplus A^1_{\mathrm{cur}} = c_i \oplus c_{i+1} = c_i \oplus (c_i + 1)$ and removes the secret key K in this equation. In this way, the adversary can trace the tag′s holder. Similarly, the adversary can implement impersonation attack by selecting a special random number r. To overcome the security weakness, Ha et al.[15] added a pseudo random number generator (PRNG) to generate a random number and removes the counter in the tag to prevent traceability attack.

Tsudik[26] described an RFID identification protocol T1 that provides a basic level of tag identification using time-stamps. Tsudik also proposed two further schemes T2 and T3 (known as YA_TRAP*) to provide tag authentication[27]. The schemes use monotonically increasing time-stamps for tracking-resistant tag authentication, and employ a keyed hash function f. The T1 and T2 schemes are susceptible to DoS attacks. The DoS vulnerability of the T1 and T2 schemes is overcome in T3 scheme by using a hash-chain to generate a so-called epoch token, which allows a tag to establish that a time-stamp is not too far into the future[27].

It is an important research consideration to develop a privacy and security protocol for the RFID system that addresses these privacy and security issues and overcomes these problems with the limited storage and computational capacity of an RFID tag. The next section presents the proposed efficient and secure authentication protocol (ESAP) to overcome the present privacy and security problems.

3 The proposed efficient and secure authentication protocol

In this section, a new protocol (ESAP) is proposed. This is based on the challenge-response method using a static identifier and a one-way randomized hash function for the RFID systems. This protocol uses a monotonically increasing timestamp to make the response more unidentifiable and anonymous. This timestamp with the random number from the reader side make the response unpredictable and secure.

3.1 Notations

The notations used in this protocol are shown in Table 3.

Table 3 Notations used in proposed ESAP

Notations	Descriptions
h	A one-way hash function, $h : \{0,1\}^* \rightarrow \{0,1\}^l$
l	The length of an identifier
r_1	Random number in $\{0,1\}^l$
ID	Tag identifier
X	Shared secret value stored in all tags
IDX	$ID \oplus X$; it is the search index of the records
T_r	Time stamp generated by the reader
T_t	Last timestamp stored in a tag
f_t	Tag response
f_r	Reader response
$\oplus$	XOR operator
$\|\|$	Concatenation operator
$\leftarrow$	Assignment operator

3.2 System set-up

The system set-up for the tag, reader and database is given as follows:

Tag: Each tag contains the following fields:

ID: Tag identifier.

X: Shared secret value.

T_t: Last timestamp.

Reader: Reader does not contain any fields.

Back-end database: Back-end database contains the following fields:

IDX: $ID \oplus X$; search index.

ID: Tag identifier.

3.3 ESAP operations

When a tag enters into the range of the reader, this can initiate the authentication protocol. The protocol is shown in Fig. 5.

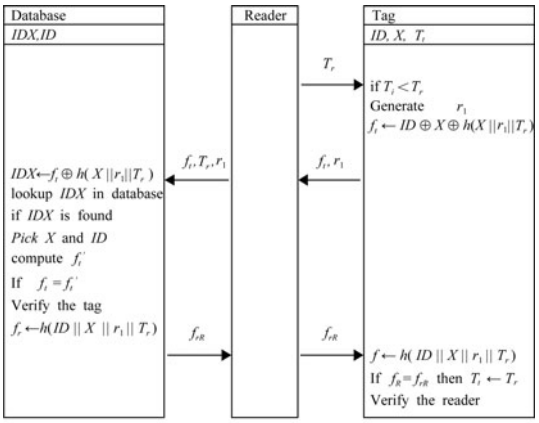

Fig. 5 The proposed ESAP protocol

The steps in the authentication protocol are as follows:

Step 1. Reader: The reader generates a time stamp T_r and sends a query with the timestamp to the tag.

Step 2. Tag: If $T_t < T_r$ then

The tag generates a random number r_1.

The tag computes $f_t \leftarrow ID \oplus X \oplus h(X||r_1||T_r)$.

It sends the value of r_1 and f_t to the reader. The reader then sends r_1, T_r and f_t to the back-end database.

Step 3. Database: The back-end database then can find X and computes $h(X||r_1||T_r)$ and then it finds $IDX \leftarrow f_t \oplus h(X||r_1||T_r)$.

Lookup IDX, ID in the database.

Compute $f_t' \leftarrow ID \oplus X \oplus h(X||r_1||T_r)$.

If $f_t = f_t'$ match, then authenticate the tag.

Compute $f_r \leftarrow h(ID||X||r_1||T_r)$.

Finally, the back-end database sends f_{rR} to the reader.

f_{rR} is the right half part of the f_r.

Step 4. Reader: The reader forwards f_{rR} to the tag.

Step 5. Tag: The tag also computes f_r and checks f_{rR}. If it matches with the response f_{rR} received from the tag, it authenticates the reader and updates $T_t \leftarrow T_r$.

Next, we discuss how the protocol works. In this protocol, the reader starts authentication by generating a new timestamp T_r and sends it to the tag. If the timestamp is $T_t < T_r$ then the tag generates a random number r_1 to make the authentication process reliable. The tag then computes the response $f_t \leftarrow ID \oplus X \oplus h(X||r_1||T_r)$ and sends f_t and r_1 to the reader. The reader sends the response and the random number r_1 to the database. The reader at first computes $h(X||r_1||T_r)$ and then computes $IDX \leftarrow f_t \oplus h(X||r_1||T_r)$. If IDX is found in the database, it picks the X and ID to calculate $h(X||r_1||T_r)$. The database then calculates f_t with this values. If it matches with the f_t received from the tag then authenticates the tag. The database then computes $f_r \leftarrow h(ID||X||r_1||T_r)$ and sends the right half f_{rR} to the reader. The protocol uses one monotonically increasing timestamp to keep the response unidentifiable or anonymous. The tag then computes the $f \leftarrow h(ID||X||r_1||T_r)$. If the right half of this value matches with the received one then the reader is authenticated. The proposed protocol uses a random number for the tag side and a timestamp from the reader side. It makes the response more unpredictable. Moreover, the monotonically increasing timestamp also makes the input combination unique and intractable.

4 Analysis of the proposed protocol

To evaluate the proposed protocol privacy, security and efficiency will be analysed.

4.1 Privacy and security analysis

The privacy and security of the proposed protocol are analysed against the threats discussed in Section 1.

Information leakage: To be able to obtain any sensitive information from a tag, a protocol must be authenticated. In this protocol, to authenticate the system an adversary must know *ID, X* and the hash function to receive any information from the tags. If the secret X is not compromised, it is not possible for any information leakage of *ID*. The combination of r_1, T_r and ID makes the responses so unpredictable that the adversary can only guess the value or use a brute-force technique with an advantage of only $(1/2^l)$, which is negligible for data length of 96 bits or more.

Location privacy: The value of f_r and f_t cannot be linked with any particular tag. The protocol ensures location privacy by using new values of r_1, T_r each time. Even if a malicious reader sends the same timestamp T_r all the times, a tag transmits the refreshed value using r_1, X and *ID*.

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 also make a request to a tag with a timestamp. However, without knowing the *ID*, X, the hash function an adversary is unable to impersonate. For each session, the tag generates a new value of f_t which is totally indistinguishable and different from other session and subsequently the impersonation and replay attacks are not possible.

Message interception or DoS attack: It is not possible to detect all the types of DoS attacks. The objective of the protocol is to take action against the vulnerability of a DoS attack and the system should not be desynchronized. The proposed protocol uses a static identifier for 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 reader will send a new timestamp and the process will be continued.

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_1, and the combination of r_1, T_r and hash function and also does not know the *ID* and secret X. Consequently, the previous, present and future interactions are all indistinguishable.

4.2 Efficiency analysis

Storage, communication and computation cost were considered for efficiency analysis. Two existing authentication protocols OHLCAP[10] and YA_TRAP*[27] were compared with the proposed ESAP authentication protocol. These protocols were selected for efficiency comparison since all of them work in ubiquitous environment. OHLCAP and YA_TRAP* require a larger storage and computations than an ESAP protocol. OHLCAP is also vulnerable to impersonation attack. The ESAP protocol shows improved performance as shown in Table 4 because it requires less tag side and database side storage than other protocols.

Table 4 Efficiency analysis

Efficiency criteria		OHLCAP	YA_TRAP*	ESAP
Storage	Tag	$5l$	$4l$	$3l$
	Reader	–	–	–
	Database	$4l$	$5l$	$2l$
Computation	Tag	$1h + A$	$2h$	$2h$
	Reader	–	–	–
	Database	$1h + \varepsilon$	$(N/2+1)h$	$2h$
Communication	Tag-to-Reader	$2.5l$	$3l$	$2l$
	Reader-to-tag	$0.5l$	$3l$	$0.5l$

A, ε: Operations in a tag and a database respectively except for hash operation

The storage requirement for the tag and the database are $3l$ and $2l$, respectively. The protocol requires less hash function in both tag and database. YA_TRAP* cannot give protections from some of the attacks and it requires $(N/2+1)$ complex functions operations which is costly because the value of N may be very high and it requires many function computations that will make the protocol slower[27]. Table 4 gives an overall comparison of the different protocols compared to the proposed ESAP. Another advantage of the proposed protocol is that it requires less data to be communicated from the reader to the tag.

5 Simulation results and evaluation

To validate the proposed protocol ESAP, simulation work has been conducted. The privacy and security protections are ensured with the hash functions, timestamp and random number. A hash function is a one-way function for which information leakage is not possible from the hash response. The simulation is to further verify the protection for impersonation attack, replay attack and location privacy. It is assumed that the adversary will capture a response from the tag or the reader and then subsequently use this response 10^{11} times to impersonate the tag or the reader. It checks the responses f_t and f_r if any of them recur more than once for one tag during the attacks by an adversary. If the same response is generated, it can be used by the adversary for impersonation and replay attack and the location privacy of the tag may be broken. A simulation program in Turbo C++ compiler is developed. It runs in a desktop computer of Intel (R) Core 2 Duo. Processor speed is 2.93 GHz and memory 3.46 GB. The operating system was Windows XP professional. The objective of the simulation program was to check the response for one tag if the response is anonymous. The output of a hash function is the same for the same random number and timestamp. Our objective is to practically ensure unique response for different inputs of random number and timestamp so that attacker cannot use any response it collected and attack later to access the tag or the reader.

The program checks to match a response with subsequent responses for a set of random number and time stamp. The number of times the same response generated for the tag response f_t and the reader response f_r is given in Table 5. It represents the success of the adversary for 10^{11} attempts for different sizes of secret numbers and data. The simulation was conducted for 16 bits, 32 bits, 64 bits and 96 bits secret and data length. In this simulation, there was no match of the response for 64 bits and 96 bits. For 16 bits and 32 bits, there were some recurrences of the same response. The reason is that it produced the same response for some other combination of random number and the timestamp. The recurrence of the response for 16 bits, 32 bits, 64 bits and 96 bits are shown in the Table 5 for 10^{11} attempts.

This simulation shows that during the attempt with 64 bits and 96 bits data and secret the tag and the reader produced unique response for a tag ID and the adversary cannot break the privacy and security of the RFID systems.

Table 5 Attacker's success table

Experiment Number	Number of queries to the Tag	Attacker's success for different data length		
		Data length	Number of matches	
			f_t	f_r
1	10^{11}	16	1 538 360	1 538 360
2	10^{11}	16	1 550 799	1 550 799
3	10^{11}	16	1 527 728	1 527 728
4	10^{11}	32	20	20
5	10^{11}	32	15	15
6	10^{11}	32	0	0
7	10^{11}	32	0	0
8	10^{11}	32	25	25
9	10^{11}	32	23	23
10	10^{11}	64	0	0
11	10^{11}	64	0	0
12	10^{11}	64	0	0
13	10^{11}	64	0	0
14	10^{11}	64	0	0
15	10^{11}	96	0	0
16	10^{11}	96	0	0
17	10^{11}	96	0	0
18	10^{11}	96	0	0
19	10^{11}	96	0	0
20	10^{11}	96	0	0

In this simulation the attacker only tries to track the response in a passive mode. It cannot use the previous timestamp and the response to attack the tag, since the tag always checks if the new timestamp is larger than its stored one. The tag does not modify its timestamp until an authentication process is successful. This experiment showed that the protocol is secure for at least 64 bits data and secrets in 10^{11} attempts. Table 6 shows the evaluation summary.

In this authentication system it is not possible to perform an active attack by the adversary to the tag by using the same timestamp. The reason is that the tag always stores the last timestamp and it does not allow any authentication process until it receives a timestamp greater than the previous one. Due to this monotonically increasing timestamp impersonation and replay attack is not possible. Another advantage of this protocol is that the adversary cannot be successful with arbitrary big fake timestamp since the tag does not update its timestamp unless a successful authentication is performed. This prevents the protocol from a DoS attack.

The summary of the privacy and security properties is given in Table 7. The privacy and security properties of ESAP are compared with four other schemes[4, 10, 11, 15, 27]. The four schemes were chosen because all of these protocols involved tag authentication. HIDV and LCAP involve secret update process and other two protocols OHLCAP and YA_TRAP* do not support secret update. ESAP is similar to OHLCAP and YA_TRAP* since ESAP does not support secret update and all these protocols support authentication in ubiquitous environment. Table 7 shows that the proposed protocol provided protections from all the identified privacy and security threats.

Fig. 6 shows the storage comparison with two other ubiquitous RFID privacy and security protocols. Storage requirement in ESAP is less than other protocols. Storage requirements are presented as l bits. The HIDV and LCAP protocols are not included in storage comparison since they update their *ID* after each authentication phase.

The simulation test successfully authenticates the tag and the reader without any privacy and security failure.

6 Applications

This protocol will be suitable for a hospital where the privacy of the patient is important. In this case, the patient identification number will be used as an *ID* for an RFID tag.

Through the tag *ID*, the private data of a person can be tracked[28]. The privacy issue with tagged patient cards involves the risk of exposing the information, such as trace of personal location and the information of their personal health and clinical treatment. Many security threats are identified in a RFID system that can also be threats in hospitals.

To protect the private data in the hospital environment the ESAP protocol can be used in the tag, reader and the database. A hospital database will keep information about the patient. The information contains personal detail of the patient. It is also linked with other information related to the patient like disease, medical history, medicine and diagnostic information. It will additionally keep secret number for the tag. In this case any unauthorised user cannot track a patient or cannot extract any information from the patient tag. The secure RFID system for patient data in a hospital environment is depicted in Fig. 7. It shows that the encrypted value f_t and f_r cannot be extracted by the unauthorised user as the secret value and *ID* are not known. The secret and *ID* are never transmitted in plaintext and in an environment like hospitals the information is fully secure.

The protocol can also be implemented to ensure the privacy and information security in medicine management. In this case, the medicine will be identified by *ID*. Since medicine information is also private and should be kept confidential the proposed protocol will also be suitable for this purpose. In this case, also any unauthorised user cannot track the medicine or cannot extract any information from the tag used in any medicine.

Table 6 Attacker's success summary

Number of Queries	Attacker's Success					
	Data length (16 bits)		Data length (32 bits)		Data length (64/96 bits)	
	f_t	f_r	f_t	f_r	f_t	f_r
10^{11}	>0	>0	$\geqslant 0$	$\geqslant 0$	0	0

f_t: Tag response, f_r: Reader response

Table 7 Privacy and security comparisons

Property	HIDV	LCAP	OHLCAP	YA_TRAP*	Proposed ESAP
Information privacy	Y	Y	Y	Y	Y
Location privacy	N	N	Y	Y	Y
Impersonation	N	A	N	Y	Y
Replay attack	N	Y	N	Y	Y
Message interception	Y	Y	Y	N	Y
Backward traceability	N	Y	N	N	Y
Forward traceability	N	Y	N	N	Y

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

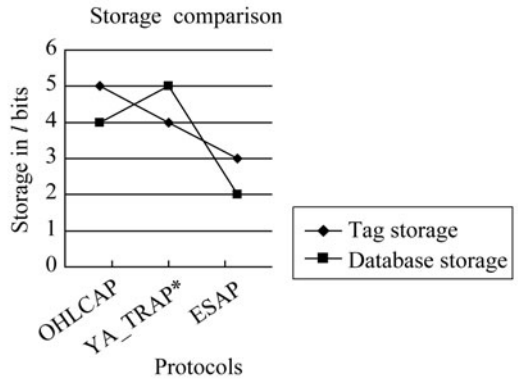

Fig. 6 Storage comparison

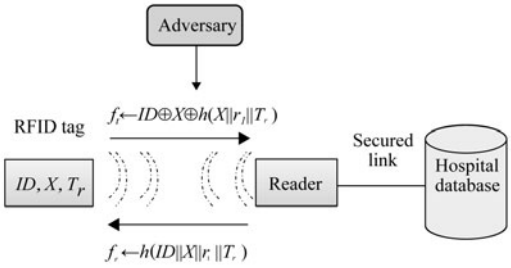

Fig. 7 Protection of the patient data

7 Conclusions

A new efficient and secure authentication protocol ESAP has been presented in this paper to protect privacy for low-cost RFID systems. The protocol uses a static identifier to provide effective privacy and security in a ubiquitous environment using hash functions, a timestamp and a random number. The strength of this protocol is the use of a monotonically increasing timestamp and a random number to make the response more unidentifiable. This protocol uses the search index IDX to search the tag records in the database. It reduces the tag search time substantially in the database. The simulation experiment also proved that, the responses during the experiment were unique for both the 64 and 96 bits long secret and data length. It is secured from an adversary from all the attacks discussed in Section 1. Specific privacy and security protections from an adversary appropriate to simulation experiment were tested and found to be satisfactory. The privacy and security protections were also analyzed and the analysis verified that this protocol is protected from the identified threats. The proposed scheme requires only two one-way hash functions making it highly efficient. The storage requirements for the tag and database are also cost efficient. The comparison outlined in the analysis and experiment result shows that the proposed protocol is secure and efficient in compared to the other protocols. It has practical advantages over these protocols because it is simple and provides a larger range of privacy and security protections. This protocol will be suitable in the RFID systems of healthcare system, shopping mall and automation in manufacturing industry, etc. However this protocol is suitable for a system where the tags are in one group and are not much distributed. In future, authentication protocol for multiple groups of tags will be considered.

References

[1] S. L. Garfinkel, A. Jules, R. Pappu. RFID privacy: An overview of problems and proposed solutions. *IEEE Security and Privacy*, vol. 3, no. 3, pp. 34–43, 2005.

[2] A. Jules. RFID security and privacy: A research survey. *IEEE Journal on Selected Areas in Communication*, vol. 24, no. 2, pp. 381–394, 2006.

[3] EPCglobal Web site, 2005. [Online], Available: http://www.EPCglobalinc.org, February 16, 2012.

[4] S. M. Lee, Y. J. Hwang, D. H. Lee, J. I. Lim. Efficient authentication for low-cost RFID systems. In *Proceedings of the 2005 International Conference on Computational Science and its Applications*, ACM, Berlin, Germany, vol. 3480, pp. 619–627, 2005.

[5] R. Want. An introduction to RFID technology. *IEEE Pervasive Computing*, vol. 5, no. 1, pp. 25–33, 2006.

[6] B. S. Prabhu, X. Su, H. Ramamurthy, C. Chu, R. Gadh. WinRFID — A Middleware for the Enablement of Radio Frequency Identification (RFID) Based Applications. [Online], Available: http: //www.techrepublic. com/ whitepapers/winrfid-a-middleware-for-the-enablement-of-radio-frequency-identification/2349745, February 19, 2012.

[7] D. Henrici, P. Muller. Hash-based enhancement of location privacy for radio-frequency identification devices using varying identifiers. In *Proceedings of the 2nd IEEE Annual Conference on Pervasive Computing and Communications Workshops*, IEEE, Orlando, USA, pp. 149–153, 2004.

[8] D. Molnar, D. Wagner. Privacy and security in library RFID: Issues, practices, and architectures. In *Proceedings of Conference on Computer and Communications Security*, ACM, Washington, USA, pp. 210–219, 2004.

[9] K. Rhee, J. Kwak, S. Kim, D. Won. Challenge-response based RFID authentication protocol for distributed database environmnet. In *Proceedings of International Conference on Security in Pervasive Computing*, Mendeley, Boppard, Germany, vol. 3450, no. 3, pp. 70–84, 2005.

[10] E. Y. Choi, S. M. Lee, D. H. Lee. Efficient RFID authentication protocol for ubiquitous computing environment. In *Proceedings of Embedded and Ubiquitous Computing*, vol. 3832, pp. 945–954, 2005.

[11] H. Chien, C. Chen. Mutual authentication protocol for RFID conforming to EPC class 1 generation 2 standards. *Computer Standards & Interfaces*, vol. 29, no. 2, pp. 254–259, 2007.

[12] M. Ohkubo, K. Suzki, S. Kinoshita. Cryptographic approach to "privacy-friendly" tags. [Online], Available: http://rfidprivacy.media.mit.edu/2003/papers/ohkubo.pdf, February 17, 2012.

[13] T. Dimitriou. A lightweight RFID protocol to protect against traceability and cloning attacks. In *Proceedings of the 1st International Conference on Security and Privacy for Emerging Areas in Communication Networks*, IEEE, Athens, Greece, pp. 59–66, 2005.

[14] M. E. Hoque, F. Rahman, S. I. Ahamed. Supporting recovery, privacy and security in RFID systems using a robust authentication protocol. In *Proceedings of the 2009 ACM Symposium on Applied Computing*, ACM, Honlulu, USA, pp. 1062–1066, 2009.

[15] J. Ha, S. Moon, J. M. G. Nieto, C. Boyd. Security analysis and enhancement of one-way hash based low-cost authentication protocol. In *Proceedings of the 2007 International Conference on Emerging Technologies in Knowledge Discovery and Data Mining*, ACM, Berlin, Germany, vol. 4819, pp. 574–583, 2007.

[16] B. Song, C. J. Mitchell. RFID authentication protocol for low-cost tags. In *Proceedings of the 1st ACM Conference on Wireless Network Security*, ACM, New York, USA, pp. 140–147, 2008.

[17] B. Song. RFID Tag Ownership Transfer. In *Proceedings of the 4th Workshop on RFID Security*, Budaperst, Hungary, 2008. [Online], Available: http://events.iaik.tugraz.at/RFIDSec08/Papers/Publication/15February 19, 2012.

[18] N. J. Hopper, M. Blum. Secure human identification protocols. In *Proceedings of the 7th International Conference on the Theory and Application of Cryptology and Information Security: Advances in Cryptology*, ACM, London, UK, vol. 2248, pp. 52–66, 2001.

[19] A. Juels, S. Weis. Authenticating pervasive devices with human protocols. [Online], Available: http://www.iacr.org/cryptodb/archive/2005/CRYPTO/1478/1478.pdf, February 17, 2012.

[20] H. Gilbert, M. Robshaw, H. Sibert. Active attack against HB^+: A provably secure lightweight authentication protocol. *Electronics Letters*, vol. 41, no. 21, pp. 1169–1170, 2005.

[21] J. Katz, J. S. Shin. Parallel and concurrent security of the HB and HB+ protocols. Cryptology ePrint archive, Report 2005/461, 2005. [Online], Available: http://eprint.iacr.org, February 17, 2012.

[22] J. Bringer, H. Chabanne, E. Dottax. HB++: A lightweight authentication protocol secure against some attacks. In *Proceedings of the 2nd International Workshop on Security, Privacy and Trust in Pervasive and Ubiquitous Computing*, IEEE, pp. 28–33, 2006.

[23] S. Piramuthu. HB and related lightweight authentication protocols for secure RFID tag/reader authentication. In *Proceedings of CollECTeR Europe Conference*, Basel, Switzerland, 2006. [Online], Available: http://www.avoine.net/rfid/download/papers/Piramuthu-2006-collecter.pdf, February 19, 2012.

[24] J. Munilla, A. Peinado. HB-MP: A further step in the HB-family of lightweight authentication protocols. *Computer Networks*, vol. 51, no. 9, pp. 2262–2267, 2007.

[25] A. J. Menezes, P. C. Oorshot, S. A. Vanstone. *Handbook of Applied Cryptography*, chapter 19, Boca Raton, USA: CRC Press, 1996.

[26] G. Tsudik. YA-TRAP: Yet another trivial RFID authentication protocol. In *Proceedings of the 4th IEEE Annual Conference on Pervasive Computing and Communications*, Pisa, Italy, pp. 640–643, 2006.

[27] G. Tsudik. A family of dunces: Trivial RFID identification and authentication protocols. In *Proceedings of the 7th International Conference on Privacy Enhancing Technologies* pp. 45–61, 2007.

[28] B. Lee, H. Kim. Ubiquitous RFID based medical application and the security architecture in smart hospitals. In *Proceedings of the 2007 International Conference on Convergence Information Technology*, ACM, Washington, USA, pp. 2359–2362, 2007.

Md. Monzur Morshed obtained M. Eng. degree in computer science and engineering from Bangladesh University of Engineering and Technology (BUET), Dhaka in 1999. He obtained his B. Eng. degree in computer science and engineering from BUET in 1996. He is an associate professor in the Department of Accounting and Information Systems, University of Dhaka, Bangladesh. He is now a Ph. D. candidate at Staffordshire University, UK. He obtained his M. Sc. degree in ICT from Waseda University, Japan in 2007. He published 14 research papers in various journals and proceedings on pattern recognition, human computer interaction, RFID privacy and security and other topics on computer science and engineering.

His research interests include the privacy and security of RFID systems, pattern recognition and Bangla text entry techniques in mobile phones.

E-mail: m.m.morshed@staffs.ac.uk

Anthony Atkins is a reader in applied computing in the Faculty of Computing, Engineering and Technology at Staffordshire University, UK. He is a Chartered Engineer and Professional Engineer (USA) in both computing, and mineral and petroleum engineering. He is also a Churchill Fellowship in bioengineering and environmental engineering and has several patents in bioengineering and waste recycling with embedded real time systems covering the UK, EU, Australia and USA. Other interests are in IT outsourcing in which he has published 6 book chapters, service management and knowledge management systems (KMS). He has published over 130 refereed publications consisting of journals, chapters in books, and conferences with his colleagues and research students.

His research interests include mobile and RFID technology in waste recycling in the construction industry and in medical waste, supply chain management (SCM) and mobile technological application to the ageing population.

E-mail: a.s.atkins@staffs.ac.uk

Hong-Nian Yu has held academic positions at Yanshan University, PRC, the Universities of Sussex, Liverpool John Moor, Exeter, Bradford and Staffordshire in the UK. He is currently professor of computer science at Staffordshire University, UK. He has published over 200 journal and conference research papers. He has held several research grants from the UK EPSRC, the Royal Society, and the EU, AWM, as well as from industry. Currently he is principal investigator on an EPSRC funded UK-Japan network grant on HAM and holds two EU funded projects. He was awarded the F.C. William Premium for his paper on adaptive and robust control of robot manipulators by the IEE Council.

His research interests include mobile computing, modelling, scheduling, planning, and simulations of large discrete event dynamic systems with applications to manufacturing systems, supply chains, transportation networks, computer networks and RFID applications, modelling and control of robots and mechatronics, and neural networks.

E-mail: h.yu@staffs.ac.uk (Corresponding author)