Scalable authentication protocol in RFID-based systems

Xuping Ren[1*], Haiping Zhang[1], Yunfa Li[2], Xindong You[2]

[1]*School of information engineering, HangZhou Dianzi University, Hangzhou, China*

[2]*Institute of Software and Intelligent Technology, HangZhou Dianzi University, Hangzhou, China*

Received 1 May 2014, www.cmnt.lv

Abstract

Because of vast highly sensitive business information within RFID system, there is an urgent need for an effective and secure protocol to ensure the interests of various stakeholders. In this paper, we propose a scalable authentication protocol to provide classification protection. GNY logic formal approach is used to verify the design correctness of the protocol. The performance is evaluated and compared with other related protocols in three aspects: storage, computation requirement and communication overload. The analysis shows that the proposed protocol need less computation requirement and memory with acceptable communication overload. The conclusion indicates that the protocol is reliable and more scalable in RFID-based sensor systems.

Keywords: RFID security, authentication protocol, scalable

1 Introduction

Radio frequency identification (RFID) is an automatic identification technology. The tag communicates with a reader via wireless channels where neither visual nor physical contact is needed. RFID systems, thanks to their low cost and their convenience in identifying an object, have found many applications in manufacturing, supply chain management (SCM), parking garage management, and inventory control [1]. The wireless communication is more vulnerable to malicious adversaries. RFID system pays more attention to the tagged item's information because tags usually contain some sensitive or personal data. It is critical that the tag data can access only by authorized readers.

RFID is especially useful for SCM, whose goal is to manage all the steps involved in product manufacturing, distributing, and retailing, in order to minimize the operating expenses by managing the stock [2]. There are various stakeholders (e.g. manufacturer, material supplier, carrier and retailer) in SCM. Each stakeholder is permitted to access the authorized tag data, whereas any irrelevant sensitive data of other groups is not disclosed [3]. The RFID-based SCM systems are faced with two threats: internal attacks and external attacks. Both attacks may lead to security threats and privacy disclosure. We refer the internal attacks to internal legal entities, who may impersonate as other legal entities to do authority-exceeding violation. For example, a manufacturer's reader personates retail's reader to access a tag. We refer the external attacks to external illegal entities (such as adversaries or business competitors), who may do spoofing attack, replay attack, Denial of server attack and so on.

Many schemes have been proposed to address the potential security and privacy problems in RFID systems. These schemes can be categorized in three main types (traditional protocols, ownership transfer protocols and classification protection protocols) for RFID-based SCM systems.

Traditional protocols [4-6] use many methods to achieve the security goals. Those protocols may not be efficient or robust enough owing to various security vulnerabilities [7]. Most protocols have been designed without strict formal proof, which may detect design flaws and security vulnerabilities. Some protocols [8, 9] lack the idea of classified security protection for an overall management. Other schemes [10, 11] focus on the external illegal attacks, but ignore the forgery attacks from the internal legal entities. So such protocols are difficult to directly apply to the RFID-based SCM system.

The second type is ownership transfer protocols. Many ownership transfer protocols are proposed to fulfill security requirements of those stakeholders. The security requirements include the secure ownership, exclusive ownership and secure ownership transfer [12]. Some transfer protocols [13] adopt the asymmetric key authentication. Some RFID ownership transfer protocols are based on the symmetric key authentication schemes. According to the current ownership of the tag, a user can be a previous owner, current owner or new owner of the tag [14]. Such protocols have classified protection of ideas. However, there are many situations that are not the owner transfers in supply chain management. For instance, carrier is not the owner of anything, is only responsible for the goods delivered. In order to facilitate the management, it needs to gather some information from the tags, rather than the overall information.

[*] ***Corresponding author*** e-mail: renxp@hdu.edu.cn

Fore-mentioned schemes allow all the authorized readers can access all entire identifiers of all legal tags. Based on the previous analysis, it is essential for authenticated entities to access the specified field areas of a tag identifier (TID) [3].

To solve this problem, H. Ning et al. proposed a distributed key array authentication protocol (KAAP) [3] for RFID-based sensor systems to realize classified security protection and resist attacks. The authors declared the protocol is reliable and scalable in advanced RFID-based sensor systems. But the reader groups are predetermined. Meanwhile those grouping information need to write into tags. These features limit the protocol scalability.

Md Monzur Morshed et al. proposed three secure ubiquitous authentication protocols SUAP1, SUAP2 and SUAP3 for RFID systems. The final version of SUAP1 is improved over the preliminary version with privacy and security enhancement. SUAP2 and SUAP3 are the extension of SUAP1 and work in a large group-based system where RFID tags are divided into several groups. SUAP3 is proposed to provide a larger range of privacy and security protections for low storage and computations. It aimed at ubiquitous computing environment. But it is not suitable to be used directly on the common RFID system.

The aim of this paper is to design a classification protection and better scalable protocol for RFID-based SCM system. All readers and tags are divided into several groups. One reader can change its role successfully without tags' intervention. All the information about groups is stored in the back-end database. The main contributions of our work are as follows:

1) One-way hash function is adopted to protect PID_{Tj} and PID_{Rj} to realize no reversibility without revealing any sensitive data.

2) The authentication key array K_{MN} and the role array K_S are used to realize the classified security protection and resist internal and external attack.

3) Pseudorandom identifiers are transmitted instead of the real identifiers.

4) Access lists (L_R, L_T,) store all the pseudorandom identifiers and they are used to retrieve a certain reader or a certain tag for quick search. The hash values of the pseudorandom identifiers use to index certain reader or tag.

5) Mutual authentication procedure is performed to realize access control.

The organization of the paper is as follows. In section II, related RFID protocols are reviewed and analysed. Section III describes the proposed protocol. In next section, formal analysis of the protocol with GNY logic has been given. Performance analysis has been discussed in section V. Finally, section VI draws a conclusion.

2 Related works

In this section, two prominent protocols KAPP [3] and SUAP3 [10] will be discussed in more detail as they are more related to the proposed work. Two protocols both work in large group-based system where RFID tags are divided into several groups.

2.1 KAPP SCHEME

KAPP scheme uses distributed key array to realize classified security protection and resist both external and internal attacks, uses pseudorandom identifiers to resist the forward traceability, and adopts access lists to conserve memory and improve scalability. The notations and symbols used in KAPP operation are as follows in Table 1 [3]:

TABLE 1 The notations and symbols used in KAPP operation

Notation	Description
G_{Rm}, G_{Tn}	the mth reader group and the nth tag group in the RFID based sensor system, (m =1,2,…,M; n =1,2,…,N).
R_i	the ith reader who belongs to G_{Rm}, (i =1,2,…,I; I ≥ M).
T_j	the jth tag who belongs to G_{Tn}, (j =1,2,…,J; J ≥N).
PID_{R_i}, PID_{T_j}	the pseudorandom identifiers of R_i and T_j, which have special flags to mark R_i and T_j .
L_R	the access list for tags to retrieve a certain reader.
L_T	the access list for the database to retrieve a certain tag
r_{R_i}, r_{T_j}	the general formats of random numbers for R_i and T_j.
$r_{R_{igen}}, r_{T_{jgen}}$	the random numbers generated by R_i and T_j in one session.
r_{Ricom}, r_{Tjcom}	the random numbers computed by R_i and T_j in one session.
k_u	the shared key is pre shared between legal readers and tags, and it is a secure value without being revealed to the third entity.
$k_{m,n}$	the authentication key owned R_i and T_j, which is assigned to G_{Rm} and G_{Tn}.
$\|\|$	concatenate operator.
$\rightarrow$	transition operator.
$\{.\}_k$	encryption with key k.

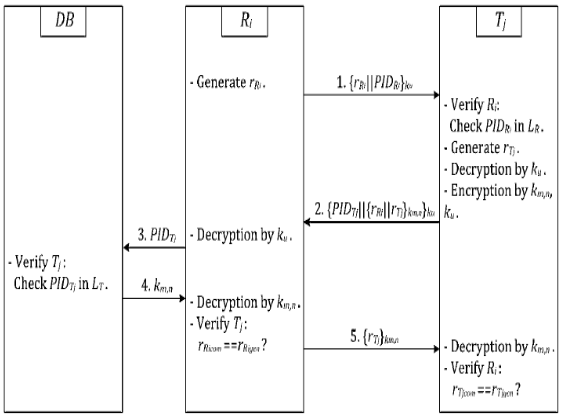

FIGURE 1 KAPP

The protocol is shown in Figure 1. All legal readers and tags are divided into different groups in the protocol. However, the reader groups are predetermined. Meanwhile those grouping information need to write into tags. These features limit the protocol scalability.

2.2 SUAP3 SCHEMES

Md Monzur Morshed et al. proposed three secure ubiquitous authentication protocols SUAP1, SUAP2 and SUAP3 for RFID systems. These protocols are low-cost and secured based on challenge-response method using a one-way hash function, hash address as a search index. The proposed protocols combine the features of the hash address and hash function of the LCAP protocol and the ubiquitous property of OHLCAP protocol. The detail about SUAP1and SUAP2 can be found in [10]. Here we focus on SUAP3.

The notations and symbols used in SUAP3 are as follows Table 2 [10].

TABLE 2 The notations and symbols used in SUAP3

Notation	Description
ID	tag identifier
GID	group identifier
Had	hash address h(ID)
h	a one way hash function, h: $\{0,1\}^* \rightarrow \{0,1\}^l$
r_1, r_2	random number in $\{0,1\}^l$
l	the length of an identifier
$\oplus$	XOR operator
||	concatenation operator
$\leftarrow$	assignment operator
h_L	the left half of $h(ID \| r_1 \| r_2 \| GID)$
h_R	the right half of $h(ID \| r_1 \| r_2 \| GID)$

SUAP3 is shown in Figure 2. SUAP3 only requires two one-way hash function operations and avoids large number of hash computations in the database. The tag search time in the database is reduced by using the hash value as the address of the corresponding tag. The authors declare that SUAP3 ensures privacy and security protections from all the identified threats. The analysis shows that the storage requirements in SUAP3 are also less than other related protocols. The comparison shows that the proposed protocol SUAP3 is both secure and efficient than other related schemes, and has practical advantages over them because it is simple and provides a larger range of privacy and security protections for low storage and computations.

However, SUAP3 is not suitable to be used directly on the common RFID system. Furthermore, whether the reader who launches a query is legal or not, the tag must give a reply. This feature will cause the occurrence of denial of service (DOS): the tag may have no time to answer the inquiry from a legitimate reader.

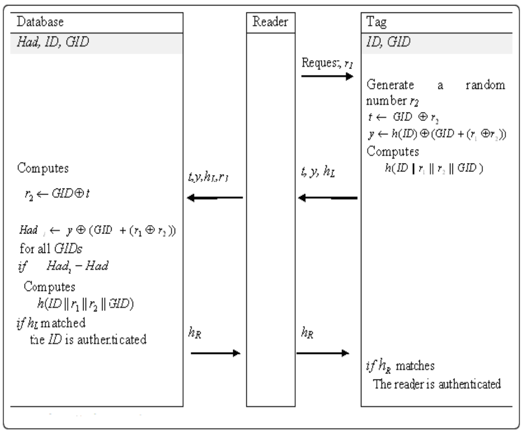
Database
Had, ID, GID
Reader
Tag
ID, GID
Request, r_1
Generate a random number r_2
$t \leftarrow GID \oplus r_2$
$y \leftarrow h(ID) \oplus (GID + (r_1 \oplus r_2))$
Computes
$h(ID \mid r_1 \| r_2 \| GID)$
t, y, h_L
t,y,h_L,r_1
Computes
$r_2 \leftarrow GID \oplus t$
$Had_i \leftarrow y \oplus (GID + (r_1 \oplus r_2))$
for all GIDs
if $Had_i - Had$
Computes
$h(ID \| r_1 \| r_2 \| GID)$
if h_L matched
the ID is authenticated
h_R
h_R
if h_R matches
The reader is authenticated

FIGURE 2 SUAP3

3 Protocol descriptions

Table 3 shows the notations applied in the protocol.

TABLE 3 Notation

Notation	Description
R	The reader in the RFID system
T	The tag in the RFID system
DB	The database in the RFID system
L_R	the access list for tags to retrieve a certain reader
L_T	the access list for the database to retrieve a certain tag
r_R ,r_T,	the random numbers generated by *R*, *T*
PID_R, PID_T	The pseudonym of *R*,*T*
h( )	A one-way hash function
[ ]	The rounding operation
$\oplus$	XOR bitwise logic operator
||	Concatenate operator
K_S	the role array which stores in DB
k_{ij}	the authentication key owned R_i and T_j, which is assigned to G_{Rm} and G_{Tn} $k_{ij}=a_1,a_2,\ldots a_s$. $a_x \in \{0.1\}$, x=1,2,…*s*. s is the number of TID fields. a_x=1 represents R_i is authorized to access the xth filed of T_j. Otherwise, R_i can not access the xth filed
K_{MN}	the key array which stores all the authentication keys in DB

3.1 INITIALIZATION

The system set-up of the new protocol is as follows:

Tag: each tag contains the following fields L_R, PID_{Tj} and can perform one-way hash function.

Reader: each reader contains PID_{Ri}.

Database: the back-end database contains L_T, L_R, the role array K_S and the key array K_{MN}.

3.2 AUTHENTICATION PROCESS

The protocol is summarized in Figure 3. The authentication process includes five phases: challenge messages; response messages; forward messages; authenticate the tag and authenticate the reader. Figure 3 describes the protocol in detail according to the sequence of message exchanges.

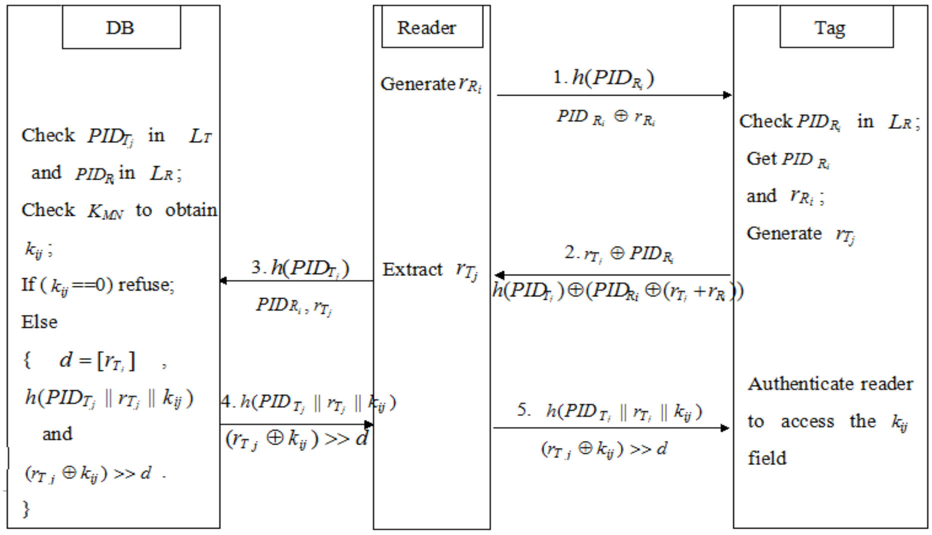
DB
Reader
Tag
Generate r_{R_i}
1. $h(PID_{R_i})$
$PID_{R_i} \oplus r_{R_i}$
Check PID_{R_i} in L_R;
Get PID_{R_i}
and r_{R_i};
Generate r_{T_j}
Check PID_{T_j} in L_T
and PID_{R} in L_R;
Check K_{MN} to obtain
k_{ij};
If (k_{ij}==0) refuse;
Else
{ $d = [r_{T_i}]$,
$h(PID_{T_j} \| r_{T_j} \| k_{ij})$
and
$(r_{T_j} \oplus k_{ij}) >> d$.
}
3. $h(PID_{T_i})$
PID_{R_i}, r_{T_j}
Extract r_{T_j}
2. $r_{T_i} \oplus PID_{R_i}$
$h(PID_{T_i}) \oplus (PID_{R_i} \oplus (r_{T_i} + r_{R_i}))$
4. $h(PID_{T_j} \| r_{T_j} \| k_{ij})$
$(r_{T_j} \oplus k_{ij}) >> d$
5. $h(PID_{T_i} \| r_{T_i} \| k_{ij})$
$(r_{T_j} \oplus k_{ij}) >> d$
Authenticate reader
to access the k_{ij}
field

FIGURE 3 The proposed protocol

The proposed protocol based on a key array and a role array adopts lightweight mechanisms to realize security, efficiency and reliability for low-cost and large group-based RFID system. The main approaches include:

1) Mutual authentication procedure is performed to realize access control. The reader needs to be verified by the tag and *DB*. *DB* authenticates T_j and R_j, then transmits messages to R_j before the tag indeed authenticates the reader. If and only if both authentications succeed, communication between R_j and T_j is secure and will continue.

2) Pseudorandom identifiers are transmitted instead of the real identifiers. In each session, T_j and R_j generate their random numbers r_{Tj} and r_{Ri}, which are to ensure dynamic refreshment. If a new query arrives with the same data within certain time, it will be neglected. This will help the system resist the replaying or jamming attacks.

3) The role array K_S and the authentication key array K_{MN} are used to realize the classified security protection and resist attacks. The role array K_S describes the rights of various types of readers. Because any reader may change its role during the system operating, the contents of K_{MN} may be changed, that is the value of the authentication key k_{ij} owned R_j and T_j can be varied. The tag needs to do nothing in the procedure. This enables the system to be more scalable.

4) One-way hash function is adopted to protect PID_{Tj} and PID_{Rj} to realize no reversibility without revealing any sensitive data.

5) Access lists (L_R, L_T) store all the pseudorandom identifiers and they are used to retrieve a certain reader or a certain tag for quick search. Each tag maintains L_R and *DB* maintains both. The hash values of the pseudorandom identifiers use to index a certain reader or tag. The access lists effectively reduce the time complexity of search operation and enable better scalability for dynamic systems.

In general, the proposed protocol is based on a dynamic key array and its TID is never exposed in plain form. It is meaningful for ranking diversified authorities to realize classified security protection. In next section, GNY Logic [16] is applied to analyse the design correctness of the proposed protocol.

4 Formal analysis of the protocol with GNY logic

Most authentication protocols have been designed and demonstrated in informal ways. Design flaws and security errors may be ignored by informal analysis [11]. With the formal method, a protocol can be demonstrated to reasonably achieve its goals using logical postulates [3].

We do the GNY formal logic analysis like [3], and the analysis involves four steps:

1) formalization of the protocol messages;

2) declaration of initial assumptions;

3) definition of anticipant goals;

4) verification by logical rules and formulae.

4.1 FORMALIZATION OF MESSAGES

We express each exchanged message as a logical formula and formalization of the messages in the language of GNY Logic. For the sake of clarity, we use the same statements as [11,15]. Table 4 shows those statements.

TABLE 4 Basic statement

Notation	Description
$S < X$	*S* receives a message containing *X*, *S* can read and repeat *X*
$S < * X$	*S* receives *X*, *X* is a not-originated-here formula
$S \ni X$	*S* possesses, or is capable of possessing *X*
$S \mid\sim X$	*S* once conveyed *X*
$S \mid\equiv X$	*S* believes, or would be entitled to believe, that statement *X* holds
$S \mid\equiv \varphi X$	*S* believes, or is entitled to believe that *X* is recognizable
$S \mid\equiv \# X$	*S* believes, or is entitled to believe that *X* is fresh
$S \mid\equiv S \overset{v}{\longleftrightarrow} X$	*S* believes, or is entitled to believe, that *V* is a suitable secret for *S* and *X*
$\{X, Y\}$	Concatenation

According to the authentication phase, the formalized messages are as follows:

M1 $(R_i \to T_j): h(PID_{R_i}),(PID_{R_i} \oplus r_{R_i})$;

M2 $(T_j \to R_i): r_{Tj} \oplus PID_{R_i}, \mathrm{h}(\mathrm{PID}_{T_j}) \oplus (PID_{R_i} \oplus (r_{T_j} + r_{R_i}))$;

M3 $(R_i \to DB): h(PID_{T_j}), r_{T_j}, PID_{R_i}$;

M4 $(DB \to R_i): h(PID_{T_j} \| r_{T_j} \| k_{ij}),(r_{T_j} \oplus k_{ij}) >> d$;

M5 $(R_i \to T_j): h(PID_{T_j} \| r_{T_j} \| k_{ij}),(r_{T_j} \oplus k_{ij}) >> d$.

4.2 INITIAL ASSUMPTIONS

In order to specify the initial possessions and abilities of each participant, we assume the following statements:

(A1) $T \ni r_T$;

(A2) $T \mid\equiv \# k_{ij}$;

(A3) $T \ni PID_T, T \mid\equiv T \xleftrightarrow{PID_T} DB$

(A4) $T \mid\equiv \# PID_R, T \mid\equiv T \xleftrightarrow{PID_R} R$;

(A5) $R \ni r_R$;

(A6) $R \ni PID_R, R \mid\equiv \# PID_R, R \mid\equiv R \xleftrightarrow{PID_R} T$;

(A7) $R \mid\equiv DB \mid\Rightarrow (DB \mid\equiv *)$;

(A8) $DB \ni k_{ij}, DB \mid\equiv \# k_{ij}$;

(A9) $DB \ni PID_T, DB \mid\equiv \# PID_T, DB \mid\equiv DB \xleftrightarrow{PID_T} T$;

(A10) $DB \ni PID_R, DB \mid\equiv \# PID_R, DB \mid\equiv DB \xleftrightarrow{PID_R} R$.

Those statements show that each participator possesses its random number and the pseudorandom identifier. Each tag believes or is entitled to believe k_{ij} and PID_R are fresh. The database DB possess k_{ij}, PID_R and PID_T, and it believes that they are fresh. The communication channel between R and DB is considered to be secure; so R believes that DB has jurisdiction over all his beliefs.

4.3 ANTICIPANT GOALS

The objectives of the protocol are to mutually authenticate between R and T, and assure freshness of data among R, T and DB. The anticipant goal can be obtained as follows:

(G1) $T \mid\equiv R \mid\sim r_R$;

(G2) $T \mid\equiv R \mid\sim PID_R$;

(G3) $R \mid\equiv T \mid\sim r_T h$;

(G4) $R \mid\equiv T \mid\sim PID_T$;

(G5) $DB \mid\equiv T \mid\sim PID_T$;

(G6) $T \mid\equiv \# h(PID_R)$;

(G7) $DB \mid\equiv \# h(PID_T)$;

(G8) $T \mid\equiv \# h(k_{ij})$;

(G9) $T \mid\equiv DB \mid\sim k_{ij}$.

The first to the fifth goals show belief requirements. R believes T conveys r_T and PID_T. T believes R conveys r_R and PID_R. DB believes T conveys PID_T. The next two goals show that the messages are not used in the previous sessions and indicate freshness requirements. The eighth goal shows **T** believes that $h(k_{ij})$ is fresh. The last goal indicates T believes DB conveys k_{ij}.

4.4 LOGIC VERIFICATION

Logic verification is based on the assumption, the formalized messages and the related GNY Rules.

From M1, T is informed messages $(PID_R \oplus r_R)$ and $h(PID_R)$. T has not received or sent them in the previous sessions, we have

$$T < *(PID_R \oplus r_R), T < *h(PID_R). \tag{1}$$

Applying the Being-Told Rule T1: $(P \triangleleft (*X))/(P \triangleleft X)$ deduces

$$T < (PID_R \oplus r_R), T < h(PID_R). \tag{2}$$

T can retrieve PID_R from L_R, and applying the Being-Told Rule T2: $(P < X, Y)/(P < X)$ deduces

$$T < PID_R,\ T < r_R. \tag{3}$$

Thus, T is considered to have been informed r_R and PID_R.

Applying the Possession Rule P1: $(P < X)/(P \ni X)$ deduces

$$T \ni PID_R, T \ni r_R. \tag{4}$$

Applying the Possession Rule P2:

$(P \ni X, P \ni Y)/(P \ni (X,Y), P \ni F(X,Y))$ deduces

$$T \ni (PID_R, r_R). \tag{5}$$

From A4, $T \mid\equiv \# PID_R$, and applying the Freshness Rule F1: $(P \mid\equiv \#(X))/(P \mid\equiv \#(X,Y), P \mid\equiv \# F(X))$ deduces

$$T \mid\equiv \#(PID_R, r_R). \tag{6}$$

From A4, we get

$$T \mid\equiv T \xleftrightarrow{PID_R} R\,. \tag{7}$$

Applying the Message Interpretation Rule I3:

$$\frac{P \triangleleft H(X, <S>), P \ni (X, S), P \mid\equiv P \xleftrightarrow{S} Q, P \mid\equiv \#(X, S)}{P \mid\equiv Q \mid\sim (X, <S>), P \mid\equiv Q \mid\sim H(X, <S>)}$$

deduces

$$T \mid\equiv R \mid\sim (PID_R, r_R)\,. \tag{8}$$

Finally, from I3 interpretation and applying the Message Interpretation Rule I7:

$(P \mid\equiv Q \mid\sim (X, Y) / P \mid\equiv Q \mid\sim X)$ deduces

$$T \mid\equiv R \mid\sim (PID_R)\,,\ T \mid\equiv R \mid\sim (r_R)\,. \tag{9}$$

As a result, *T* believes that *R* once conveyed *PID_R* and *r_R*. Goal G1 and G2 are achieved.

Hereinafter, for simplicity, we directly mark the applied logical rules and Equations behind the Equation.

For Goal 3:

$$R < *(r_T \oplus PID_R) \ \text{// by M2} \tag{1}$$

$$R < (r_T \oplus PID_R) \ \text{//by T1} \tag{2}$$

$$R < r_T \ \text{// by T5} \tag{3}$$

$$R \ni r_T \ \text{// by P1} \tag{4}$$

$$R \ni (r_T, PID_R) \ \text{//by P2} \tag{5}$$

$$R \ni H(r_T) \ \text{//by P4} \tag{6}$$

$$R \mid\equiv \varphi(r_T) \ \text{// by R6} \tag{7}$$

$$R \mid\equiv \# PID_R \ \text{//by A6} \tag{8}$$

$$R \mid\equiv \#(r_T, PID_R) \ \text{//by F1} \tag{9}$$

$$R \mid\equiv T \mid\sim r_T \ \text{//by I3} \tag{10}$$

According to I3, *R* is entitled to believe that *T* once conveyed r_T.

For Goal 5:

$$DB < *h(PID_T)\,, DB < *PID_R\,, DB < *r_T \ \text{//by M3} \tag{1}$$

$$DB < h(PID_T)\,, DB < PID_R\,, DB < r_T \ \text{//by T1} \tag{2}$$

$$DB \ni PID_R,\ DB \ni h(PID_T)\,, DB \ni r_T \ \text{//by P1} \tag{3}$$

$$DB \ni PID_T \ \text{// by P5} \tag{4}$$

$$DB \ni (r_T, PID_T) \ \text{//by P2} \tag{5}$$

$$DB \mid\equiv \# PID_T \ \text{//by A9} \tag{6}$$

$$DB \mid\equiv \#(r_T, PID_T) \ \text{//by F1} \tag{7}$$

$$DB \mid\equiv T \mid\sim (PID_T) \ \text{// by I3} \tag{8}$$

According to I3, *DB* is entitled to believe that *T* once conveyed PID_T.

For Goal 4:

$$R \mid\equiv DB \mid\Rightarrow (DB \mid\equiv *) \ \text{//by A7} \tag{1}$$

$$DB \mid\equiv T \mid\sim (PID_T) \ \text{// by Goal 5} \tag{2}$$

$$R \mid\equiv DB \mid\Rightarrow (T \mid\sim PID_T) \tag{3}$$

$$R \mid\equiv DB \mid\equiv (T \mid\sim PID_T) \ \text{//by J3} \tag{4}$$

$$R \mid\equiv (T \mid\sim PID_T) \ \text{//by J1} \tag{5}$$

As a result, *R* is entitled to believe that *T* once conveyed PID_T.

For Goal 6: From message M1 gets

$$T < *(PID_R \oplus r_R) \tag{1}$$

$$T < (PID_R \oplus r_R) \ \text{//by T1} \tag{2}$$

$$T < PID_R \ \text{//by T2} \tag{3}$$

$$T \ni PID_R \ \text{//by P1} \tag{4}$$

$$T \mid\equiv \# PID_R \ \text{//A4} \tag{5}$$

$$T \mid\equiv \# h(PID_R) \ \text{//by F10} \tag{6}$$

So *T* is entitled to believe that $h(PID_R)$ is fresh.

For Goal 7:

$$DB \ni PID_T \ \text{//A9} \tag{1}$$

$$DB \mid\equiv \# PID_T \ \text{//A9} \tag{2}$$

$$DB \mid\equiv \# h(PID_T) \ \text{// F10} \tag{3}$$

So Goal G7 is achieved.

For Goal 8:

$$T < *(r_{T_j} \oplus k_{ij}) >> d \ \text{//M5} \tag{1}$$

$$T < (r_{T_j} \oplus k_{ij}) >> d \ \text{// T1} \tag{2}$$

$$T \ni (r_{T_j} \oplus k_{ij}) >> d \ \text{// P1} \tag{3}$$

$$T \ni r_T \ \text{//A1} \tag{4}$$

So *T* possesses *d*, where $d=r_T$. Therefore we get

$$T \ni k_{ij} \tag{5}$$

$$T \mid\equiv \# k_{ij} \ \text{// A2} \tag{6}$$

$$T \mid\equiv \# h(k_{ij}) \ \text{// F10} \tag{7}$$

As a result, *T* is entitled to believe that $h(k_{ij})$ is fresh.

For Goal 9: From aforementioned Equation (5) gets

$$T \ni k_{ij} \tag{1}$$

$$T \ni PID_T \text{ , } T \mid\equiv T \xleftrightarrow{PID_T} DB \text{ // A3} \tag{2}$$

$$T \ni (PID_T, k_{ij}) \text{ // P2} \tag{3}$$

$$T \mid\equiv \# k_{ij} \text{ // A2} \tag{4}$$

$$T \mid\equiv \#(k_{ij}, PID_T) \text{ // F1} \tag{5}$$

$$T \mid\equiv DB \mid\sim (k_{ij}, PID_T) \text{ // I3} \tag{6}$$

$$T \mid\equiv DB \mid\sim (k_{ij}) \text{ // I7} \tag{7}$$

As a consequence, *T* is entitled to believe that *DB* once conveyed k_{ij}.

5 Performance analysis

In RFID systems, the performance is another important metric apart from the security issue, so that the optimization and balance between security and performance are necessary for RFID systems [16].

In this section, storage cost, communication load and computation of the proposed protocol are compared with other related protocol. For the sake of simple, KAPP and [11] are chose as the representative of the relevant protocols because of their good performance. The details about performance comparison of [11] can be found in [11]. The details about performance comparison with related protocols of KAPP can be found in [3].

During the entire authentication process of the protocol, each tag and each reader performs one random number generation (RNG) operation and one one-way hash function respectively, while the database performs one one-way hash function like [11]. In KAPP, each tag needs two encryption and two decryption besides generating one random number. Like [3] and [11], access list L_R and L_T are adopted to avoid exhaustive searches in the storage. So computation cost of the protocol is similar to [11] and less than KAPP.

The total authentication progress completed via five phase is acceptable in real sensor system [3]. The communication overhead refers to exchanged messages during each authentication session. In the protocol, there are two exchanged messages between tag and reader during one phase like [11], while KAPP only needs one.

In the protocol, each tag stores access list L_R, the TID ID_T, pseudorandom identifier PID_T and revisable values in the re-writable memory, while other cryptographic algorithms (such as KAAP) also need to store the secret keys. The database stores the role array K_S and the key array K_{MN}, while K_S points out one specific role has own access contents of the tag and K_{MN} indicates the different reader groups own different access authorities. The size of K_{MN} depends on the numbers of the tag groups and the reader groups in the sensor system. A reader group in the proposed protocol can play multiple roles, while a reader group in KAPP can only play one role for one specific tag group. On the whole, the storage requirement of the protocol is less than what it needs in KAPP. Additionally, the memory consumption on one-way hash function is another concern [11]. Standardized cryptographic hash functions such as SHA-1 are too expensive for today's low-cost RFID tags [16,17]. The implementation of the protocol will suitable for low-cost tags.

Above all, the computation cost and the storage requirement of the protocol are less than KAPP, and the communication overhead is similar to [11]. The protocol owns acceptable performance.

6 Conclusions

In the paper, a new distributed protocol is proposed for classified security protection in RFID-based sensor systems. The proposed protocol adopts challenge-response mutual authentication mechanism, random access control mechanism and access lists to strengthen security and privacy protection. As a formal analysis, GNY logic is used to verify the design correctness of the protocol.

Comparison with similar protocol KAPP, the protocol has better scalability because one reader can change its role easily and the tag does not need to store its authentication key. Moreover, the protocol just updates key array on the database side.

According to performance analysis, the protocol has acceptable communication overload, less storage requirements and computation load compared with other related protocol.

Therefore, the proposed protocol is suitable for large-scale RFID application (Such as SCM system). In the future, synchronization problem should be taken into consideration. In addition, RFID authentication protocols with anti-collision mechanism should be paid more attention to.

Acknowledgements

This work was supported in part by a grant from Zhejiang Provincial department of education of china (NO. Y201222937, Y201432390).

References

[1] Chien H, Chen C 2007 Mutual authentication protocol for RFID conforming to EPC class 1 generation 2 standards *Computer Standards & Interfaces* **29**(2) 254–9

[2] Lee Y, Park Y 2013 A New Privacy-preserving Path Authentication Scheme using RFID for Supply Chain Management *Advances in Electrical and Computer Engineering* **13**(1) 23-6

[3] Ning H, Liu H, Mao J, Zhang Y 2011 Scalable and distributed key array authentication protocol in radio frequency identification-based sensor systems *IET Communications* **5**(12) 1755-68

[4] Sun HM, Ting WC 2009 A *IEEE Trans Mob Comput* **8**(8) 1052-62

[5] Sakai K, Ku W, Zimmermann R, Sun M 2013 *IEEE Trans on computers* **62**(1) 112-23

[6] Wang B, Ma M 2012 *IEEE Trans On Industrial Informatics* **8**(3) 689-96

[7] Piramuthu S 2008 *IEEE Trans Syst Man Cybern C Appl Rev* **38**(3) 360-76

[8] Rahman F, Ahamed S I 2014 Efficient detection of counterfeit products in large-scale RFID systems using batch authentication protocols *Pers Ubiquit Comput* **18** 177-88

[9] Bu K, Liu X, Xiao B 2014 Approaching the time lower bound on cloned-tag identification for large RFID systems *Ad Hoc Networks* **13** 271–81

[10] Morshed Md M, Atkins A, Yu H 2012 Secure ubiquitous authentication protocols for RFID systems *EURASIP Journal on wireless communications and networking* **93**

[11] Ren X, Li Y, Xu X 2013 A one-way Hash Function Based Lightweight Mutual Authentication RFID Protocol *Journal of Computers* **8**(9) 2405-12

[12] Van Deursen T, Mauw S, Radomirovi'c S, Vullers P 2009 Secure ownership and ownership transfer in RFID systems *LNCS* **5789** 637–54

[13] Elkhiyaoui K, Blass E-O, Molva R 2012 ROTIV:RFID Ownership transfer with issuer verification *RFID sec 2011 LNCS* **7055** 163-82

[14] Nan Li, Yi Mu, Willy Susilo, Vijay Varadharajan 2013 Secure RFID Ownership transfer protocols *ISPEC 2013 LNCS* **7863** 189-203

[15] Gong L, Needham R, Yahalom R 1990 Reasoning about belief in cryptographic protocols *IEEE Computer Society Symp Research in Security and Privacy* 234–48

[16] Lehtonen M, Staake T, Michahelles F, Fleisch E 2006 From identification to authentication - a review of RFID product authentication techniques I*n Printed handout of Workshop on RFID Security - RFIDSec 2006*

[17] Weis S 2003 Security and privacy in radio-frequency identification devices *Master's thesis Massachusetts Institute of Technology (MIT) Massachusetts USA*

Authors

	Xueping Ren, born in 1978, Zhejiang Province, China **Current position, grades:** lecturer at the School of information engineering, Hangzhou Dianzi University. **University studies:** B.S. degree from Hanzhou Dianzi University, Hangzhou, China, in 2005. **Scientific interest:** RFID. **Publications:** 10 papers.
	Haiping Zhang, born in 1975, Zhejiang Province, China **Current position, grades:** an associate professor at the School of information engineering, Hangzhou Dianzi University. **University studies:** B.S. degree from Hanzhou Dianzi University, Hangzhou, China, in 2005. **Scientific interest:** on wireless security. **Publications:** 10 papers.
	Yunfa Li, China **Current position, grades:** an associate professor of the School of Computer Science and Technology, Hangzhou Dianzi University. **University studies:** PhD degree and the Master degree in Computing Science from Huazhong University of Science and Technology. **Scientific interest:** performance modelling, analysis of software, virtual machine, cloud computing, system security, network security. **Publications:** over 30 research papers.
	Xindong You, China **Current position, grades:** a lecturer of School of Computer Science and Technology, Hangzhou Dianzi University, China. **University studies:** PhD degree in Northeastern University in 2007. **Scientific interest:** distributed computing, cloud storage, energy management.