Journal of Network and Computer Applications 42 (2014) 135–142

Contents lists available at ScienceDirect

Journal of Network and Computer Applications

journal homepage: www.elsevier.com/locate/jnca

RFID seeking: Finding a lost tag rather than only detecting its missing

Wei Xie [a,*], Lei Xie [b], Chen Zhang [a], Qiang Wang [c], Jian Xu [d], Quan Zhang [a], Chaojing Tang [a]

[a] School of Electronic Science and Engineering, National University of Defense Technology, China
[b] State Key Laboratory for Novel Software Technology, Nanjing University, China
[c] School of Communication and Computer Science, Swiss Federal Institute of Technology, Lausanne, Switzerland
[d] Department of Electrical and Computer Engineering, University of Illinois at Chicago, USA

ARTICLE INFO

Article history:
Received 19 May 2013
Received in revised form
30 October 2013
Accepted 8 January 2014
Available online 22 January 2014

Keywords:
RFID
Server-less
Searching
Security
Privacy

ABSTRACT

This paper proposes a novel type of RFID application, i.e., RFID seeking. Several existing types of RFID applications such as monitoring, searching, locating/navigating, are similar with RFID seeking. However, they are either inapplicable or vulnerable for RFID seeking scenarios, in which a user is to find a lost tagged item in a blind spot, or to find a wanted item among a mass of similar ones.

In this paper, detailed requirements for RFID seeking are suggested. The first secure RFID seeking protocol is proposed, meeting all the given requirements. Its security is formally verified by using the AVISPA tool. The proposed protocol is server-less, lightweight, privacy-friendly to both RFID readers and tags, and is secure against common attacks such as eavesdropping, manipulating, replaying, tracing, Denial of Service (DoS), etc.

1. Introduction

Radio Frequency Identification (RFID) (Sheng et al., 2011) is a wireless technology that uses radio signal to identify tagged items remotely. An RFID system is usually composed of RFID readers, tags, and a centralized database. Tags are either active, requesting a reader; or passive, responding to a reader's request. An RFID reader identifies tags according to the centralized database which is usually stored in a backend server. RFID technology has been widely used in a series of real-life applications, such as supply chain management, contactless credit card, inventory control, etc. However, there are still many security and privacy concerns about RFID applications (Di Pietro and Molva, 2011; Hancke, 2011; Rizzo et al., 2011; Avoine et al., 2012; Kardas et al., 2012; Li et al., 2012; Sakai et al., 2013).

In daily life, people often suffer from item-seeking problems, i.e. to find a lost item in a blind spot, or to find a specified item among lots of similar ones. For instance, a man tried to find his car key when he was leaving home. After a long time seeking, the key was finally found under the sofa; however, he had been late for his date. For another instance, a professor had a personal library with a huge collection of books. There were so many books on different shelves that the professor had to spend quite a lot of time to find a wanted book.

The above problems can be solved in a world of Internet of Things (IoT) where everyday items are expected to be tagged with RFID tags. A person can be enabled to quickly find a wanted item by using an RFID reader. This kind of RFID applications is termed “RFID seeking” in this paper. To our knowledge, there is no current works specially designed for RFID seeking. Related works are either inapplicable or vulnerable to RFID seeking scenarios.

RFID Monitoring protocols (Tan et al., 2008a; Zhang et al., 2011; Li et al., 2010; Tan et al., 2010; Luo et al., 2011; Ma et al., 2012) are designed to detect the missing of tagged items, rather than to seek a missing tag. A simple method to detect tags' missing is to identify all tags' IDs periodically by using RFID authentication protocols. However, this method is rather inefficient. Because, the authentication must be performed frequently enough among all tags which may have a huge number. Therefore, the foremost objective of existing RFID monitoring researches is to improve time-efficiency. Even so, RFID monitoring are only able to detect a tag's missing, rather than to guide a seeker to find the lost tag.

RFID location/navigation applications (Bu et al., 2012; Kim and Chong, 2009; Ni et al., 2011; Cheng et al., 2012; Yang et al., 2013; Digiampaolo and Martinelli, 2014) are to pinpoint/navigate tagged items, commonly, in indoor environments. A series of tags and/or readers are deployed as landmarks in a coordinate space. A reader/tag can be located/navigated/pinpointed by comparing the phases/strengths of signals received from different landmarks. The application scenarios of RFID location/navigation are similar with RFID seeking. However, these applications are more suitable for industrial utilizations than personal uses, because they rely upon many

[*] Corresponding author. Tel./fax: +86 731 84574481.
E-mail address: xiewei@nudt.edu.cn (W. Xie).

1084-8045/$ - see front matter © 2014 Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.jnca.2014.01.006

pre-deployed nodes. Obviously, it is unnecessary for a person to deploy a lot of RFID devices inside his/her house, just for seeking some lost items occasionally. Besides, the person may lose his/her items outside the house.

RFID searching (Tan et al., 2007, 2008b; Won et al., 2008; Lin et al., 2009; Hoque et al., 2010; Kim et al., 2011; Lee et al., 2012; Chun et al., 2011) is a special type of RFID authentication. In an RFID searching protocol, a reader only wants to authenticate a specified tag among all tags. Then, the reader can know whether the specified tag is among the searched group of tags. RFID searching protocols can guide a seeker to find a wanted tag among a lot of similar tags. However, the process is rather inefficient. The seeker has to divide all tagged items into many small groups, and to search in each group to check if the wanted one is there. Besides, for a seeker who tries to find a lost tag in a blind spot, an RFID searching application can only warn the seeker that the tag is nearby, rather than pinpoint the lost tag's position.

Moreover, most RFID searching protocols are unsecure for RFID seeking. (1) Some protocols (Tan et al., 2007, 2008b; Lin et al., 2009; Lee et al., 2012) reveal the privacy of mobile reader holders. A reader's identifier is broadcasted as a constant and plaintext value in these protocols, enabling an attacker to trace the reader holder by tracing the reader's identifier. (2) Some protocols (Won et al., 2008; Hoque et al., 2010; Chun et al., 2011) are vulnerable to DoS (Denial of Service) attacks. The research (Yoon, 2012) pointed out that the protocol (Chun et al., 2011) is vulnerable to DoS attacks due to requiring symmetric encryption on a tag. We notice that the protocol (Won et al., 2008) has the same vulnerability with the protocol (Chun et al., 2011). (3) Some protocols (Tan et al., 2007, 2008b; Won et al., 2008; Lin et al., 2009; Kim et al., 2011; Chun et al., 2011) are unsecure to RFID seeking due to lack of mutual authentication. If a tag did not authenticate a reader while being authenticated by the reader, the tag would be maliciously sought by anyone using an unauthorized reader.

An efficient and secure approach to find a wanted tag might be as follows: the seeker uses his RFID reader to broadcast an encrypted and untraceable message like “I am looking for the item with the tag ID=X”. Then, only the wanted tag ID=X can understand the request. After mutual authentication between the tag and the reader, the tag activates its attached indicator. As a result, the tag-controlled indicator starts a light/sound alarm by flashing/buzzing, guiding the seeker to find the tag directly.

1.1. Contribution

There are two main contributions in this paper: (1) A new type of RFID application, i.e., RFID seeking is defined and formulated with detailed requirements. RFID seeking can guide a seeker to find a lost tagged item in a blind spot, or to find a wanted tagged item among a mass of similar ones. (2) A secure RFID seeking protocol is proposed, meeting all the given requirements simultaneously for the first time. The proposed protocol is server-less, lightweight, privacy-friendly, and is secure against common attacks such as eavesdropping, manipulating, replaying, tracing, Denial of Service (DoS), etc.

The rest of this paper is organized as follows. In Section 2, RFID seeking are defined and formulated with detailed requirements after the presentation of two typical application scenarios. In Section 3, The first secure RFID seeking protocol is proposed in two phases. Its design concepts are discussed step by step. In Section 4, the proposed protocol is evaluated, meeting all the requirements listed in Section 2. Its security is formal verified by using AVISPA tool. Its superiority is shown in comparisons with related works. In Section 5, we give our conclusions and future works.

2. Problem overview

In this section, RFID seeking is introduced with two exampled application scenarios, and then presented in a formal way. Detailed requirements for RFID seeking protocols are also suggested.

2.1. Application scenarios

RFID seeking is helpful in two kinds of application scenarios.

One application scenario is to find a lost item in a blind sport like a secluded corner. Imagine that, a lady lost an expensive necklace in her way home. The necklace had been tagged with a tag-controlled indicator, which would generate sound/light alarms once the tag was activated. The lady had a PDA embedded with an RFID reader. She walked back along her track, holding the PDA to seek the necklace. When she was near the necklace, the tag was activated by the reader. And then, the tag-controlled indicator started an alarm via buzzing/flashing, guided the lady to find the lost necklace in bushes Fig. 1.

The other application scenario is to find a wanted tagged item among a mass of similar ones. Imagine that, a postman was delivering lots of postal packages within a city. For each receiver, the postman needed to pick a specified package among similar others. This work could be very oppressive without automation. Fortunately, all packages had been tagged with tag-controlled indicators. The postman was enabled to seek a wanted package by using his PDA embedded with an RFID reader i.e. after inputting a receiver's ID, the corresponding tag is activated, and the tag-controlled indicator starts buzzing/flashing, leading the postman to find the right package quickly.

2.2. Formulation of RFID seeking

Consider an RFID system that consist of a set of readers $R=\{R_1,\dots,R_i,\dots,R_m\}$ and a set of tags $T=\{T_1,\dots,T_j,\dots,T_n\}$. Only

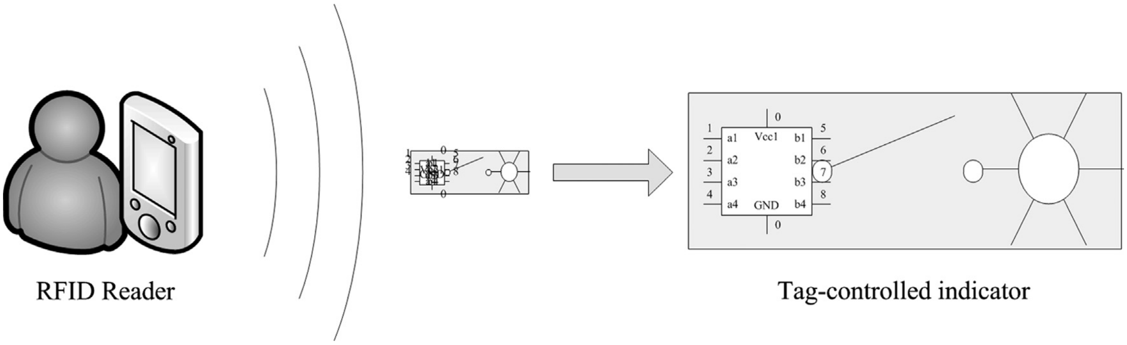


Fig. 1. RFID seeking by using tag-controlled indicators.

the reader R_i is authorized to identify the tags. Each tag has a state value $S=\{S_0, S_1\}$ which controls an corresponding attached indicator. In an RFID seeking protocol, a user U who holds R_i, is going to find a special tag T_j which is lost in a blind sport or among a lot of similar tags. Firstly, R_i broadcasts a request to activate T_j. After mutual authentication, T_j alters its state from S_0 to S_1, activating its indicator to generate sound/light alarms via buzzing/flashing. As a result, U is navigated to find T_j according to the alarming indicator. Meanwhile, an attacker A may try to compromise the RFID seeking protocol, and to identify/locate U by tracing R_i or activating T_j in unauthorized ways.

2.3. Requirements

According to the above formulation and application scenarios, an RFID seeking protocol should meets some basic requirements as follows.

1. *The protocol should be server-less, i.e. without any intervention from a backend server to complete the seeking process*. That is because U may use R_i to seek T_j in an offline location. For instance, the lady may lose her necklace when she travels to a remote scenic region; the postman may need to deliver a package to a suburb or a closed warehouse where there is no public networks.
2. *The protocol should notify a wanted tag that it is sought by a reader while other tags/readers do not know which tag is sought*. On one hand, if T_j is not informed, the corresponding tag-controlled indicator cannot be activated to guide U. On the other hand, if $R_s(s \neq i), T_k(k \neq j)$ are also enabled to know the identifier of T_j, A can also know what U is looking for, revealing individual privacy.
3. *A reader should broadcast encrypted and inconstant messages to seek a tag*. Otherwise, the identifiable/traceable messages of R_i will reveal U's individual privacy of identity/location. i.e. A can identify, locate, and trace U according to the broadcasted messages of R_i.
4. *A tag should respond with encrypted and inconstant messages to a reader*. Otherwise, the identifiable/traceable messages of T_j will reveal U's individual privacy of identity/location. i.e. A can identify, locate, and trace U according to the responded messages of T_j.
5. *The protocol should provide mutual authentication between a reader and a wanted tag*. On one hand, if R_i does not authenticate T_j, U can be misguided by a malicious tag $T_k(k \neq j)$. On the other hand, if T_j does not authenticate R_i, T_j can be maliciously sought by A using an unauthorized reader $R_s(s \neq i)$.
6. *The protocol should be lightweight, i.e. the computation capability required on a tag should be no more than that supporting hashing*. Neither symmetric nor public encryption should be required on T_j. Otherwise, A are enabled to launch DoS attacks by continuously requesting T_j which is busy with encrypting and decrypting (Yoon, 2012).

It is worth noting that, the time-efficiency is not listed as a main design objective in this paper, because it is not as important as that in an RFID monitoring protocol which identifies a huge number of tags frequently and periodically. On one hand, in the first application scenario for RFID seeking (i.e. to find a lost tagged item in a blind spot), there are not a huge number of tags to be authenticated. On the other hand, in the second application scenario (i.e. to find a wanted tagged item among similar ones), although there may be a huge number of tags, the seeking process is performed only once when needed, rather than frequently and periodically performed.

Table 1
Requirements of similar protocol types.

Types	Monitoring	Searching	Navigating (locating)	Seeking
Requirement#1	Needless	Essential	Sometimes	Essential
Requirement#2	Needless	Sometimes	Sometimes	Essential
Requirement#3	Needless	Essential	Sometimes	Essential
Requirement#4	Needless	Essential	Sometimes	Essential
Requirement#5	Essential	Sometimes	Sometimes	Essential
Requirement#6	Essential	Essential	Essential	Essential
The main concern	Efficiency	Security	Accuracy	Security/ privacy

To the best of our knowledge, none of the current works meet all above requirements for RFID seeking. Actually, in monitoring/searching/navigating/locating protocols, which are similar with RFID seeking, only some of the requirements are met (see Table 1).

3. The proposed protocol

In this section, a secure RFID seeking protocol is proposed. It is composed of an initialization phase and a seeking phase. Its design concepts are discussed step by step. The notations used in this paper are described in Table 2.

3.1. Initialization phase

An RFID reader R_i first downloads an Access List (AL) from a certificate authority (CA). It is worth noting that, the mobile reader is usually a portable device such as a PDA or a smart phone, rather than a well protected backend server. If it is stolen, then all tag's secrets in it would be revealed. To tackle this concern, a reader-specific key like $H(R_i||K_j)$, instead of K_j, is required to be stored in the AL. In this case, the reader AL is

$$L_i \equiv \{(T_1, H(R_i||K_1)), \dots, (T_j, H(R_i||K_j)), \dots, (T_n, H(R_i||K_n))\}.$$

That is, the reader with identifier R_i is given a reader-specific key $H(R_i||K_j)$ for each tag. As a result, the reader's identifier R_i is required to be sent to a tag, enabling the tag to generate the reader-specific secret $H(R_i||K_j)$ to be verified by the reader. However, we use

$$L_i \equiv \{(T_1, K_1), \dots, (T_j, K_j), \dots, (T_n, K_n)\}$$

to simplify the description in this paper. The reader-stolen issue can be solved easily by replacing K_j with $H(R_i||K_j)$.

Each tag T_j has a controlling binary state S_j initialized to be passive, i.e. $S_j=0$. S_j is activated only after a mutual authentication between the tag T_j and a reader R_i. if S_j is activated, i.e. $S_j=1$, the tag-controlled indicator stars an alarm via buzzing and/or flashing, guiding the seeker, who holds the authenticated reader R_i, to find the wanted tag T_j. The seeking phase of the proposed protocol is illustrated in Fig. 2.

3.2. Seeking phase

1. The reader R_i broadcasts α, β, N_R to seek a specified tag T_s, where $\alpha = H(T_s||N_R) \oplus R_i$ and $\beta = H(R_i||N_R) \oplus T_s$.
2. Each nearby tag T_j generates $R' = H(T_j||N_R) \oplus \alpha$ and $T' = H(R'||N_R) \oplus \beta$ to check if itself is right the wanted tag sought by the reader. If $T' = T_j$, it means $s = j$, i.e. the reader is seeking T_j. Then T_j generates $\varepsilon = H(K_j||N_R||N_T)$. Otherwise $T' \neq T_j$, it means $s \neq j$, the reader is not seeking T_j but another tag. Then

Table 2
Notations and descriptions.

Notation	Description
R_i, R'	Identifiers of readers, with bit length L
T_j, T_s, T'	Identifiers of tags, with bit length L
N_R	A random number generated by a reader
N_T	A random number generated by a tag
$rand_L$	A random number with bit length L
K_j	The secret of the tag T_j.
S_j	The controlling state of T_j. It is either passive or active. i.e. $S_j \in \{0,1\}$
L_i	An access list downloaded by the reader R_i from a certificate agency
$H(\cdot)$	An one-way hash function with output length L. i.e. $H(\cdot): \{0,1\}* \rightarrow \{0,1\}^L$
$\oplus$	XOR operation
$\|\|$	Concatenation operation
n	The number of tags in an Access List

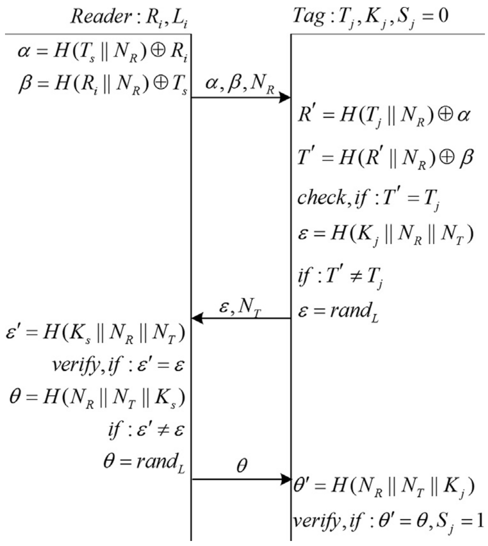

$Reader: R_i, L_i$
$Tag: T_j, K_j, S_j = 0$
$\alpha = H(T_s \| N_R) \oplus R_i$
$\beta = H(R_i \| N_R) \oplus T_s$
α, β, N_R
$R' = H(T_j \| N_R) \oplus \alpha$
$T' = H(R' \| N_R) \oplus \beta$
$check, if: T' = T_j$
$\varepsilon = H(K_j \| N_R \| N_T)$
$if: T' \neq T_j$
ε, N_T
$\varepsilon = rand_L$
$\varepsilon' = H(K_s \| N_R \| N_T)$
$verify, if: \varepsilon' = \varepsilon$
$\theta = H(N_R \| N_T \| K_s)$
$if: \varepsilon' \neq \varepsilon$
$\theta = rand_L$
θ
$\theta' = H(N_R \| N_T \| K_j)$
$verify, if: \theta' = \theta, S_j = 1$

Fig. 2. The proposed seeking phase.

T_j generates $\varepsilon = rand_L$. Each nearby tag T_j responds to the reader with different ε, N_T.

3. The reader generates $\varepsilon' = H(K_s||N_R||N_T)$ compared with each received ε. If there is a matched $\varepsilon' = \varepsilon$, it means the sought tag is found. Then R_i generates $\theta = H(N_R||N_T||K_s)$. Otherwise all $\varepsilon' \neq \varepsilon$, it means the sought tag is not nearby. Then R_i generates $\theta = rand_L$. The reader R_i responds each tag with a corresponding θ.
4. The sought tag T_j generates $\theta' = H(N_R||N_T||K_j)$ compared with the received θ. If they are matched, it means that the reader has the real secret of the tag, i.e. the reader has been authorized to seek the tag. The tag's controlling state is activated, i.e. $S_j = 1$, then, the tag-controlled indicator stars an alarm via buzzing and/or flashing, guiding the seeker, who holds the authenticated reader R_i, to find the wanted tag T_j.

3.3. Discussion

The design concepts in the seeking phase is discussed step by step as follows:

1st step: The reader generates and broadcasts $\alpha = H(T_s||N_R) \oplus R_i$. It can be viewed as an encrypted form of R_i while $H(T_s||N_R)$ is the one-time pad key. The reader also generates and broadcasts $\beta = H(R_i||N_R) \oplus T_s$. It can be viewed as an encrypted form of T_s while $H(R_i||N_R)$ is the one-time pad key. The random number N_R is used as a fresh seed to make the key inconstant in each session. Due to both the reader's identifier R_i and the wanted tag's identifier T_s are transmitted in forms with confidentiality and freshness, the first step is resistant against common attacks such as eavesdropping, manipulating, replaying, tracing, DoS, etc.

2nd step: Only the sought tag $T_j = T_s$ is able to generate the matched key $H(T_j||N_R) = H(T_s||N_R)$and obtain the real $R' = R_i$ by calculating

$$R' = \alpha \oplus H(T_j||N_R) = (H(T_s||N_R) \oplus R_i) \oplus H(T_j||N_R).$$

Having the real $R' = R_i$ enables the sought tag $T_j = T_s$ to generate the matched key $H(R'||N_R) = H(R_i||N_R)$ and check if itself is the wanted tag by verifying $T' = T_j$ where

$$T' = \beta \oplus H(R'||N_R) = (H(R_i||N_R) \oplus T_s) \oplus H(R'||N_R).$$

And then, the wanted tag generates and responds with $\varepsilon = H(K_j||N_R||N_T)$ where N_T as well as N_R are random numbers to provide freshness. Each unwanted tag responds a $\varepsilon = rand_L$. All these responses are with the same bit length L and are always changed as or like random numbers. To our knowledge, it is infeasible to launch any valid attacks on them.

3rd step: The reader verifies each received ε and responds with a corresponding θ. It can be a meaningful hashed value $\theta = H(N_R||N_T||K_s)$ or a meaningless random number $\theta = rand_L$, according to whether the wanted tag is nearby. However, in both cases, θ is with freshness and confidentiality, i.e. it is inconstant, hashed/random with the same bit length L, thus, invulnerable to known attacks.

4th step: The wanted tag verifies the reader's θ to authenticate the reader. With the help of mutual authentication, attackers with unauthorized readers are infeasible to maliciously seek a tag via activating the tag's controlling state to trigger the tag-controlled indicator.

4. Analysis, verification, evaluation and comparison

This section shows that the proposed protocol is eligible for RFID seeking and better than existing works in many aspects.

4.1. Analysis of complexity and resistance

4.1.1. Tags' computation capability requirement

The proposed scheme does not meet the Class 1 Generation 2 (C1G2) standard (Chien and Chen, 2007), because it requires a tag to support a hash function. Therefore, it is not a standard lightweight scheme. However, most RFID authentication schemes require a hash function implemented by a tag (see e.g. Tan et al., 2007, 2008b; Won et al., 2008; Lin et al., 2009; Hoque et al., 2010; Kim et al., 2011; Lee et al., 2012). It can greatly enhances a scheme's security, while increasing the cost of a tag only in a reasonable range. Moreover, using a hash function does not necessarily require a lot more logic gates in the tag. For instance, the research (Guo et al., 2011) presented a lightweight hash-function family, suitable for extremely constrained devices such as passive RFID tags.

4.1.2. The number of communication steps

The proposed scheme provides mutual authentication in only three communication steps. This is the least number of steps essential for mutual authentication theoretically and practically. i.e. in the 1st step, the reader challenges the tag; in the 2nd step, the tag responds to and challenges the reader; in the 3rd step, the reader responds to the tag.

4.1.3. *Collision of tags*

In the proposed protocol, there may be a lot of responding tags nearby the reader. To avoid collision of tags, on one hand, an optional approach is that: not all but only a part of unwanted tags responds to the reader. On the other hand, an anti-collision scheme can be used. However, RFID anti-collision is an independent research field with many mature works (Zhen et al., 2005; Myung et al., 2006; Shih et al., 2006; Klair et al., 2010; Gandino et al., 2011; Namboodiri et al., 2012; Djeddou et al., 2013). This paper is not aimed at designing an RFID anti-collision protocol.

The proposed protocol is resistant against common attacks such as

4.1.4. *Resistance against eavesdropping and manipulating*

Besides random numbers, only hashed values are transmitted in the proposed protocol. Therefore, important values such as reader-identifier, tag-identifier, tag-key cannot be extracted from eavesdropped messages which are hashed. Similarly, an attacker cannot manipulate the hashed messages validly without corresponding secret values.

4.1.5. *Resistance against replaying and tracing*

All the hashed messages transmitted in the proposed protocol contain random numbers which are generated by readers and/or tags. Protocol messages are unique for each session, defending against replaying and tracing attacks.

4.1.6. *Resistance against DoS attacks*

The proposed protocol does not rely upon any synchronized state between tags and readers. Therefore, attackers cannot stop tags from being authenticated again by desynchronization attacks. Moreover, high-level algorithms are not required to executed by tags. Thus, attackers cannot launch DoS attacks by requesting a tag continuously.

It is worth noting that, the wanted tag's alarm via buzzing/flashing may be exploited by an attacker. For example, the attacker may approach the wanted tag before the seeker. This attack can be prevented by using specialized headphone/glasses, making the buzzing/flashing only audible/visible to the seeker. Actually, this paper focus more on attacks in protocol layer than in practice.

4.2. *Formal verification*

In this subsection, the security of the proposed protocol is proofed by using an automatic formal verification tool.

Among currently available automated protocol verification tools, Automated Validation of Internet Security Protocols and Applications (AVISPA) (Armando et al., 2005) has gained the considerable attention of the industry to practice fast verifications. AVISPA is a tool for building and analyzing security protocols. This tool provides a role-based, expressive formal language for protocol specification and integrates four different back-ends, which perform the actual analysis of the protocol.

The formal specification language used in AVISPA is called High Level Protocol Specification Language (HLPSL). To verify a protocol in AVISPA tool, it is necessary to model the candidate protocol and the intruder in HLPSL (von Oheimb, 2005), and to execute the actual analysis.

AVISPA tools employ four back-ends to tackle validation of security protocols: On-the-fly Model-Checker (OFMC), Constraint-Logic-based Attack Searcher (CL-ATSE), SAT-based Model-Checker (SATMC) and Tree Automata based on Automatic Approximations for the Analysis of Security Protocols (TA4SP). The architecture of AVISPA is shown in Fig. 3.

The proposed password update phase is formalized in HLPSL as in Fig. 4, and the result of AVISPA is shown in Fig. 5. OFMC and CL-ATSE output SAFE while SATMC and TA4SP output INCONCLUSIVE, because only OFMC and CL-ATSE can verify the protocols that use algebraic properties of exclusive-or (XOR) and modular exponentiation.

4.3. *Evaluation*

The proposed protocol meets all the requirements listed in Section 2.3 for RFID seeking.

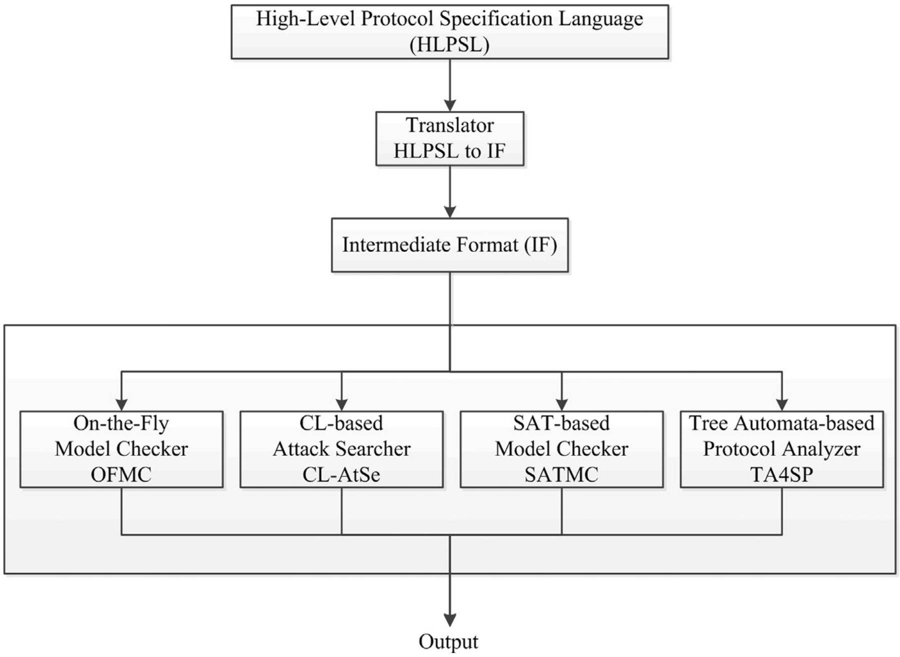
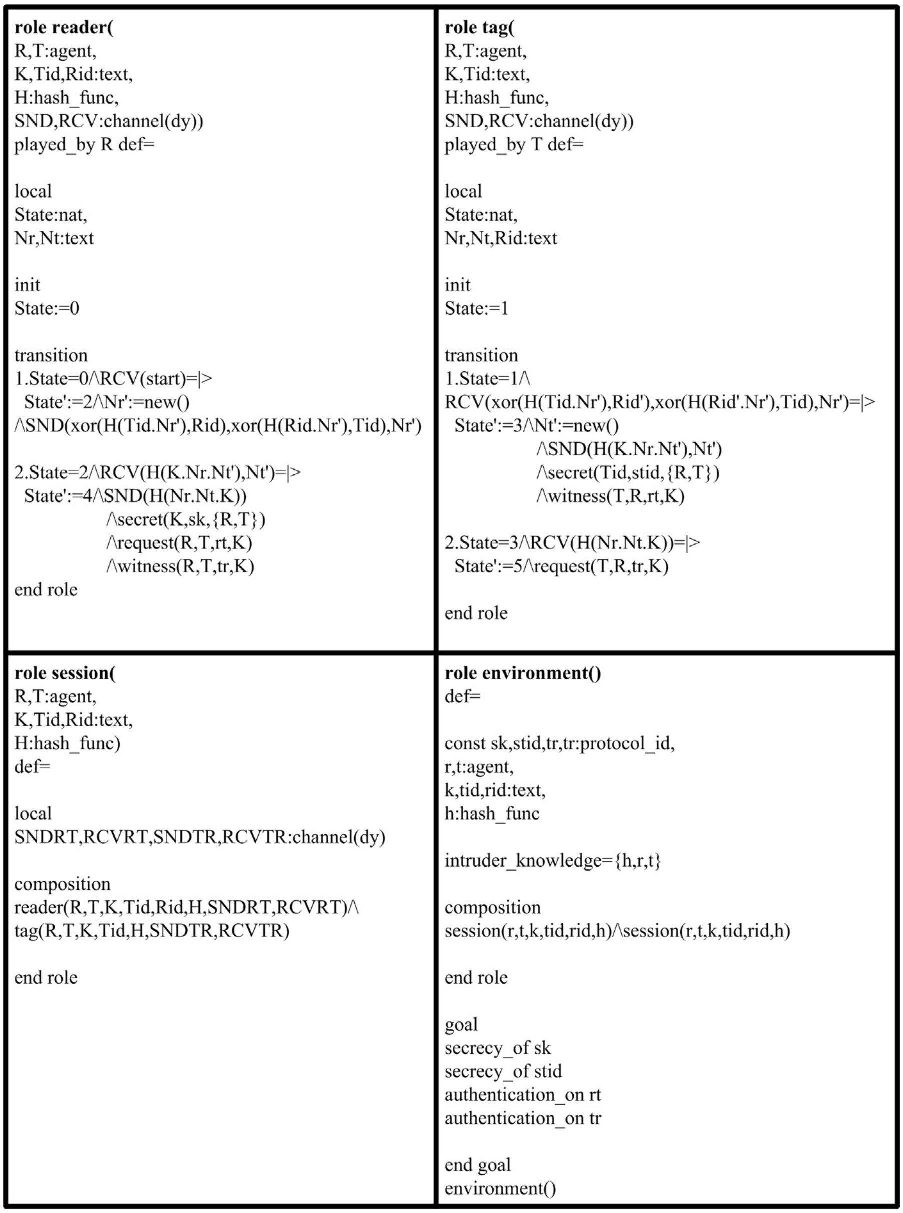

High-Level Protocol Specification Language (HLPSL)
Translator HLPSL to IF
Intermediate Format (IF)
On-the-Fly Model Checker OFMC
CL-based Attack Searcher CL-AtSe
SAT-based Model Checker SATMC
Tree Automata-based Protocol Analyzer TA4SP
Output

Fig. 3. The architecture of AVISPA.



```
role reader(
R,T:agent,
K,Tid,Rid:text,
H:hash_func,
SND,RCV:channel(dy))
played_by R def=

local
State:nat,
Nr,Nt:text

init
State:=0

transition
1.State=0/\RCV(start)=|>
 State':=2/\Nr':=new()
/\SND(xor(H(Tid.Nr'),Rid),xor(H(Rid.Nr'),Tid),Nr')

2.State=2/\RCV(H(K.Nr.Nt'),Nt')=|>
 State':=4/\SND(H(Nr.Nt.K))
          /\secret(K,sk,{R,T})
          /\request(R,T,rt,K)
          /\witness(R,T,tr,K)
end role
```

```
role tag(
R,T:agent,
K,Tid:text,
H:hash_func,
SND,RCV:channel(dy))
played_by T def=

local
State:nat,
Nr,Nt,Rid:text

init
State:=1

transition
1.State=1/\
RCV(xor(H(Tid.Nr'),Rid'),xor(H(Rid'.Nr'),Tid),Nr')=|>
 State':=3/\Nt':=new()
          /\SND(H(K.Nr.Nt'),Nt')
          /\secret(Tid,stid,{R,T})
          /\witness(T,R,rt,K)

2.State=3/\RCV(H(Nr.Nt.K))=|>
 State':=5/\request(T,R,tr,K)

end role
```

```
role session(
R,T:agent,
K,Tid,Rid:text,
H:hash_func)
def=

local
SNDRT,RCVRT,SNDTR,RCVTR:channel(dy)

composition
reader(R,T,K,Tid,Rid,H,SNDRT,RCVRT)/\
tag(R,T,K,Tid,H,SNDTR,RCVTR)

end role
```

```
role environment()
def=

const sk,stid,tr,tr:protocol_id,
r,t:agent,
k,tid,rid:text,
h:hash_func

intruder_knowledge={h,r,t}

composition
session(r,t,k,tid,rid,h)/\session(r,t,k,tid,rid,h)

end role

goal
secrecy_of sk
secrecy_of stid
authentication_on rt
authentication_on tr

end goal
environment()
```

Fig. 4. The specification of the proposed protocol in HLPSL.

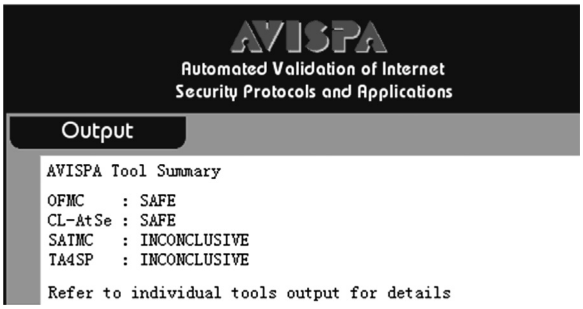
4.3.1. *Server-less*

It is without any intervention from a backend server to complete the seeking process. A reader downloads an AL from a CA in initialization phase. It is online. However, the reader seeks a special tag via the AL in seeking phase. It is offline and server-less. The protocol works well even in an environment where there are no networks.

It is worth noting that, the term “serverless” commonly means that a backend server is needless in authentication (seeking) phase, rather than in initialization phase. Actually, to our knowledge, current RFID protocols which are claimed as serverless, all need third parties in initialization phases. (see. e.g. Tan et al., 2007, 2008b; Won et al., 2008; Lin et al., 2009; Hoque et al., 2010; Kim et al., 2011; Lee et al., 2012; Chun et al., 2011).

4.3.2. *Providing seeking and monitoring*

The protocol informs a wanted tag that it is sought by a reader while other tags do not know which tag is sought. On one hand, the sought tag is notified by checking $T_s = T_j$ in the second step, and later triggers its tag-controlled indicator to guide the seeker. On the other hand, other tags are infeasible to obtain either the real R_i or the specified T_s, prevented from knowing which tag is sought by which reader. Moreover, the reader knows whether the sought tag is nearby checking if $\varepsilon' = \varepsilon$ in the third step. i.e. the proposed protocol also provides RFID monitoring in which a tag's absence can be detected.



AVISPA
Automated Validation of Internet
Security Protocols and Applications
Output

```
AVISPA Tool Summary

OFMC    : SAFE
CL-AtSe : SAFE
SATMC   : INCONCLUSIVE
TA4SP   : INCONCLUSIVE

Refer to individual tools output for details
```

Fig. 5. The verification results issued by the AVISPA tool.

Table 3
Comparisons.

Protocols	**Tan** (Tan et al., 2007, 2008b)	**Won** (Won et al., 2008)	**Lin** (Lin et al., 2009)	**Hoque** (Hoque et al., 2010)	**Kim** (Kim et al., 2011)	**Lee** (Lee et al., 2012)	**Chun** (Chun et al., 2011)	**Ours**
Server-less	√	√	√	√	√	√	√	√
Applicable to monitoring	√	√	√	√	√	√	√	√
Applicable to Seeking	√	√	√	√	×	√	×	√
Lightweight	√	×	√	√	√	√	×	√
Preserving readers' privacy	×	√	×	√	√	×	√	√
Preserving tags' privacy	√	√	√	√	√	√	√	√
Mutual authentication	×	×	×	√	×	√	×	√
DoS resistance	√	×	√	×	√	√	×	√

4.3.3. *Privacy-friendly to readers*

A reader broadcasts encrypted and inconstant messages to seek a tag. In the first step, the reader R_i broadcasts α, β, N_R, where N_R is a random number making the hash-based encryption $\alpha = H(T_s||N_R) \oplus R_i$ and $\beta = H(R_i||N_R) \oplus T_s$ fresh. Attackers are infeasible to crack R_i without T_s. It is infeasible to maliciously identify or trace the seeker by indentifying and tracing R_i.

4.3.4. *Privacy-friendly to tags*

A tag responds with hashed and inconstant messages to a reader. In the second step, if T_j is the sought reader, it will generate $\varepsilon = H(K_j||N_R||N_T)$, which is a keyed hashed value with random salt N_R, N_T. Otherwise, T_j will generate $\varepsilon = rand_L$, which is a random number with the same bit length of the valid $\varepsilon = H(K_j||N_R||N_T)$. Each nearby tag responds to the reader with unique and untraceable ε, N_T, preventing attackers from identifying or tracing a tag.

4.3.5. *Provide mutual authentication*

The protocol provides mutual authentication between a reader and a sought tag. On one hand, in the third step, the reader authenticates the wanted tag by verifying $\varepsilon' = \varepsilon$, disabling a forged tag to misguide the seeker. One the other hand, in the last step, the wanted tag authenticates the reader by verifying $\theta' = \theta$, disabling an unauthorized seeker to seek the tag.

4.3.6. *Lightweight*

Only hashing and PRNG (Pseudo Random Noise Generation) are required on a tag. Neither symmetric nor public encryption is required. Therefore, the protocol is resistant to the DoS attacks which continuously request a tag with limited resource.

4.4. *Comparison*

To the best of our knowledge, the proposed protocol is the first protocol meeting all the requirements listed in Section 2.3 for RFID seeking. According to the comparisons in Table 3, the proposed protocol is distinguished from current RFID searching protocols which are the most similar with RFID seeking.

The proposed protocol and the protocols (Tan et al., 2007, 2008b; Won et al., 2008; Lin et al., 2009; Hoque et al., 2010; Lee et al., 2012) provide RFID monitoring and seeking while the protocols (Kim et al., 2011; Chun et al., 2011) only support RFID monitoring. In the proposed protocol and the protocols (Tan et al., 2007, 2008b; Won et al., 2008; Lin et al., 2009; Hoque et al., 2010; Lee et al., 2012), there is an approach for a tag to check if itself is the sought tag by the reader; and the reader knows whether the sought tag is nearby. Whereas in the protocols (Kim et al., 2011; Chun et al., 2011), only the reader knows whether the searched tag is nearby, there is no approach for a tag to check if itself is the searched tag by the reader. If there is a tag-controlled indicator, it cannot be activated by the tag to guide the seeker.

The proposed protocol and the protocols (Tan et al., 2007, 2008b; Lin et al., 2009; Hoque et al., 2010; Kim et al., 2011; Lee et al., 2012) are lightweight while the protocols (Won et al., 2008; Chun et al., 2011) employ high-level algorithms. In the proposed protocol and the protocols (Tan et al., 2007, 2008b; Lin et al., 2009; Hoque et al., 2010; Kim et al., 2011; Lee et al., 2012), a tag is only required to support hashing and PRNG which can be viewed as lightweight to a passive tag. Whereas in the protocols (Won et al., 2008; Chun et al., 2011) symmetric encryption is required on a tag, making these protocols away from lightweight. Moreover, as a result, the protocols (Won et al., 2008; Chun et al., 2011) are vulnerable to the DoS attacks in which attackers continuously request a tag to make it busy with encrypting and decrypting.

The proposed protocol and the protocols (Won et al., 2008; Hoque et al., 2010; Kim et al., 2011; Chun et al., 2011) preserve privacy of mobile reader holders while the protocols (Tan et al., 2007, 2008b; Lin et al., 2009; Lee et al., 2012) reveal users' privacy. In the proposed protocol and the protocols (Won et al., 2008; Chun et al., 2011), a reader's identifier is encrypted before broadcasted; in the protocol (Hoque et al., 2010), a reader is not labeled with an identifier; in the protocol (Kim et al., 2011), a reader's identifier is different when searching different tags. Thus, in these protocols, attackers are prevented from tracing a seeker via tracing a reader's identifier. Whereas, in the protocols (Tan et al., 2007, 2008b; Lin et al., 2009; Lee et al., 2012), a reader's identifier is constant and broadcasted without any encryption or hashing, revealing the identity and location privacy of the seeker who holds the reader to seek a tag.

The proposed protocol and the protocols (Hoque et al., 2010; Lee et al., 2012) provide mutual authentication between a tag and a reader, while the protocols (Tan et al., 2007, 2008b; Won et al., 2008; Lin et al., 2009; Kim et al., 2011; Chun et al., 2011) only provide unilateral authentication in which the tag is authenticated by the reader. Because the reader is not authenticated by the tag, the tag's owner can be maliciously traced by attackers using an unauthorized reader.

5. Conclusions and future works

Our main contributions in this paper include: (1) A novel type of RFID application protocol, i.e. RFID seeking has been formulated with detailed requirements. It can guide a user to find a lost tagged item in a blind spot or a wanted item among a mass of similar ones. (2). We have proposed the first RFID seeking protocol meeting all the given requirements. It is server-less, lightweight, privacy-friendly to both readers and tags, and is secure against common attacks such as eavesdropping, manipulating, replaying, tracing, DoS, etc.

The main limitations of this study include: (1) The proposed protocol still requires hashing on a tag, failing to meet C1G2 (Class 1 Generation 2) standard. (2) This academic paper does not provide a concrete hardware realization of the tag-controlled indicator because, actually, the realization of the tag-controlled indicator requires more adequate professional knowledge of hardware, which is beyond our research. However, our future work is to improve the protocol to be ultra-lightweight, and to implement a real RFID seeking application.

Acknowledgments

This work is partially supported by the National Natural Science Foundation of China under Grant nos. 61302091 and 61100196; the JiangSu Natural Science Foundation under Grant no. BK2011559.

References

Avoine G, Carpent X, Martin B. Privacy-friendly synchronized ultralightweight authentication protocols in the storm. J Network Comput Appl 2012;35:826–43.

Armando A, Basin D, Boichut Y, Chevalier Y, Compagna L, Cuellar J, et al. The Avispa Tool for the automated validation of internet security protocols and applications. In: Proceedings of CAV, Computer Aided Verification, LNCS 3576. Springer Verlag; 2005.

Bu K, Xiao B, Xiao Q, Chen S. Efficient misplaced-tag pinpointing in large RFID systems. IEEE Trans Parallel Distributed Syst 2012;23:2094–106.

Cheng W, Cheng X, Song M, Chen B, Zhao WW. On the design and deployment of RFID assisted navigation systems for VANETs. IEEE Trans Parallel Distributed Syst 2012;23:1267–74.

Chun JY, Hwang JY, Lee DH. RFID tag search protocol preserving privacy of mobile reader holders. IEICE Electron Express 2011;8:50–6.

Chien HY, Chen CH. Mutual authentication protocol for RFID conforming to EPC Class 1 Generation 2 standards. Comput Stand Interfaces 2007;29:254–9 (Feb).

Di Pietro R, Molva R. An optimal probabilistic solution for information confinement, privacy, and security in RFID systems. J Network Comput Appl 2011;34:853–63.

Digiampaolo E, Martinelli F. Mobile robot localization using the phase of passive UHF RFID signals. IEEE Trans Ind Electron 2014;61:365–76.

Djeddou M, Khelladi R, Benssalah M. Improved RFID anti-collision algorithm. AEU – Int J Electron Commun 2013;67:256–62.

Gandino F, Ferrero R, Montrucchio B, Rebaudengo M. Probabilistic DCS: an RFID reader-to-reader anti-collision protocol. J Network Comput Appl 2011;34:821–32.

Guo J, Peyrin T, Poschmann A. The PHOTON family of lightweight hash functions. In: Proceedings of the 31st annual international cryptology conference, CRYPTO, August 14, 2011–August 18, 2011. Santa Barbara, CA, United states; 2011. p. 222–39.

Hancke GP. Design of a secure distance-bounding channel for RFID. J Network Comput Appl 2011;34:877–87.

Hoque ME, Rahman F, Ahamed SI, Park JH. Enhancing privacy and security of RFID system with serverless authentication and search protocols in pervasive environments. Wireless Pers Commun 2010;55:65–79.

Kardas S, Celik S, Yildiz M, Levi A. PUF-enhanced offline RFID security and privacy. J Network Comput Appl 2012;35:2059–67.

Kim M, Chong NY. Direction sensing RFID reader for mobile robot navigation. IEEE Trans Autom Sci Eng 2009;6:44–54.

Kim Z, Kim J, Kim K, Choi I, Shon T. Untraceable and serverless RFID authentication and search protocols. In: Proceedings of the 9th IEEE international symposium on parallel and distributed processing with applications workshops, ISPAW, ICASE, SGH, GSDP. May 26, 2011–May 28, 2011. Busan, Republic of Korea; 2011. p. 278–83.

Klair DK, Chin K-W, Raad R. A survey and tutorial of RFID anti-collision protocols. IEEE Commun Surv Tutorials 2010;12:400–21.

Li T, Luo W, Mo Z, Chen S. Privacy-preserving RFID authentication based on cryptographical encoding. In: IEEE conference on computer communications. INFOCOM 2012. March 25, 2012–March 30, 2012. Orlando, FL, United states; 2012. p. 2174–82.

Li T, Chen S, Ling Y. Identifying the missing tags in a large RFID system. In: Proceedings of the 11th ACM international symposium on mobile ad hoc networking and computing. MobiHoc 2010. September 20, 2010–September 24, 2010. Chicago, IL, United States; 2010. p. 1–10.

Luo W, Chen S, Li T, Chen S. Efficient missing tag detection in RFID systems. In: IEEE INFOCOM 2011. April 10, 2011–April 15, 2011. Shanghai, China; 2011. p. 356–60.

Lin I-C, Tsaur S-C, Chang K-P. Lightweight and serverless RFID authentication and search protocol. In: Proceedings of the 2009 international conference on computer and electrical engineering. ICCEE 2009. December 28, 2009–December 30, 2009. Dubai, United Arab Emirates; 2009. p. 95–9.

Lee C-F, Chien H-Y, Laih C-S. Server-less RFID authentication and searching protocol with enhanced security. Int J Commun Syst 2012;25:376–85.

Ma C., Lin J., Wang Y. Efficient missing tag detection in a large RFID system. In: Proceedings of the 11th IEEE international conference on trust, security and privacy in computing and communications. TrustCom-2012. June 25, 2012–June 27, 2012. Liverpool, United kingdom; 2012. p. 185–92.

Myung J, Lee W, Srivastava J. Adaptive binary splitting for efficient RFID tag anti-collision. IEEE Commun Lett 2006;10:144–6.

Ni LM, Zhang D, Souryal MR. RFID-based localization and tracking technologies. IEEE Wireless Commun 2011;18:45–51.

Namboodiri V, Desilva M, Deegala K, Ramamoorthy S. An extensive study of slotted Aloha-based RFID anti-collision protocols. Comput Commun 2012;35:1955–66.

Rizzo F, Barboni M, Faggion L, Azzalin G, Sironi M. Improved security for commercial container transports using an innovative active RFID system. J Network Comput Appl 2011;34:846–52.

Sheng QZ, Zeadally S, Mitrokotsa A, Maamar Z. RFID technology, systems, and applications. J Network Comput Appl 2011;34:797–8.

Sakai K, Sun M-T, Ku W-S, Lai TH. Randomized Skip Lists-based private authentication for large-scale RFID systems. In: Proceedings of the 14th ACM international symposium on mobile ad hoc networking and computing. MobiHoc 2013. July 29, 2013–August 1, 2013. Bangalore, India; 2013. p. 277–80.

Shih D-H, Sun P-L, Yen DC, Huang S-M. Taxonomy and survey of RFID anti-collision protocols. Comput Commun 2006;29:2150–66.

Tan C.C., Sheng B., Li Q.How to monitor for missing RFID tags. In: Proceedings of 28th international conference on distributed computing systems. ICDCS 2008. July 17, 2008–July 20, Beijing, China; 2008a. p. 295–302.

Tan C, Sheng B, Li Q. Efficient techniques for monitoring missing RFID tags. IEEE Trans Wireless Commun 2010;9:1882–9.

Tan CC, Sheng B and Li Q., "Serverless search and authentication protocols for RFID. In: Proceedings of the 5th annual IEEE international conference on pervasive computing and communications. PerCom 2007. March 19, 2007–March 23, 2007. White Plains, NY, United States; 2007. p. 3–12.

Tan CC, Sheng B, Li Q. Secure and serverless RFID authentication and search protocols. IEEE Trans Wireless Commun 2008b;7:1400–7.

von Oheimb D. The high-level protocol specification language HLPSL developed in the EU project AVISPA. In: Proceedings of APPSEM 2005 Workshop; September 13, 2005.

Won TY, Chun JY, Lee DH. Strong authentication protocol for secure RFID tag search without help of central database. In: Proceedings of the 5th international conference on embedded and ubiquitous computing. EUC 2008. December 17, 2008–December 20, 2008. Shanghai, China; 2008. p. 153–8.

Yang P, Wu W, Moniri M, Chibelushi CC. Efficient object localization using sparsely distributed passive RFID tags. IEEE Trans Ind Electron 2013;60:5914–24.

Yoon E-J. Cryptanalysis of an RFID tag search protocol preserving privacy of mobile reader. In: Proceedings of the 9th IFIP international conference on network and parallel computing. NPC 2012.September 6, 2012–September 8, 2012. Gwangju, Republic of Korea; 2012. p. 575–80.

Zhang R, Liu Y, Zhang Y, Sun J. Fast identification of the missing tags in a large RFID system. In: Proceedings of the 2011 8th annual IEEE communications society conference on sensor, mesh and ad hoc communications and networks. SECON 2011. June 27, 2011–June 30, 2011. Salt Lake City, UT, United states; 2011. p. 277–86.

Zhen B, Kobayashi M, Shimizu M. Framed ALOHA for multiple RFID objects identification. IEICE Trans Commun 2005;E88-B:991–9.