



Contents lists available at ScienceDirect

Computer Networks

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

REACT: An RFID-based privacy-preserving children tracking scheme for large amusement parks

Xiaodong Lin^a, Rongxing Lu^b, Davis Kwan^a, Xuemin (Sherman) Shen^{b,*}

^a Faculty of Business and Information Technology, University of Ontario Institute of Technology, Oshawa, Ontario, Canada L1H 7K4

^b Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, Ontario, Canada N2L 3G1

ARTICLE INFO

Article history:

Received 15 December 2009

Received in revised form 22 April 2010

Accepted 9 May 2010

Available online xxxx

Responsible Editor: J. Misić

Keywords:

RFID

Children tracking

Privacy preserving

Pocket switched network

ABSTRACT

In this paper, we propose an RFID-based privacy-preserving children tracking (REACT) scheme for helping locate missing children in large amusement parks and other public venues. The scheme is characterized by the cooperation among RFID readers, storage nodes and control center, which are strategically deployed across the amusement park, as well as employees and visitors in the park. When a passive RFID tag, physically attached on a child, approaches an RFID reader, the reader will process the tag information. The reader then forwards the information to a storage node through a pocket switched network formed by employees and visitors in the park. When locating a lost child is requested, the system is able to track the missing child by querying the tag information stored in the storage nodes. Detailed security analysis shows that the proposed REACT scheme achieves child's identity privacy, unlinkable location privacy and forward security. In addition, extensive simulations demonstrate that as more visitors participate in the pocket switched network, the performance of our proposed REACT scheme increases which directly improves the efficiency for the locating lost children.

© 2010 Elsevier B.V. All rights reserved.

1. Introduction

One of the greatest fears of parents is, without a doubt, losing sight of their children. Each year approximately 65,000 children are reported missing in Canada [1], leading to people suffering in different ways such as anguish and franticness of parents and the potential loss of children lives. A fraction of these cases occur when the children are in public venues such as shopping malls, playgrounds and amusement parks. In the worst case scenario, these missing children are never reunited with their parents. Locating a child in an amusement park can be a very difficult task. For example, large amusement parks usually cov-

er an area greater than one squared kilometer, e.g., the Canada's wonderland [2].

On a typical day during the high season, there may be tens of thousands of visitors in the park. Finding one single child from this crowd is sometimes next to impossible, like finding a needle in a hay stack. It is not unusual that guest services at amusement parks constantly have long line ups and are busy trying to help anxious parents locate their lost children. It takes at least a couple of hours on average to locate a child in the park and in the worst case, they may never be found as they have already left the park. This is a major safety issue that is important to both the park operators and visitors. Unfortunately, there are currently no systems in place to aid in the tracking of missing children in public venues. Most searches for missing children cases are performed by reviewing recorded security surveillance tapes and requesting the help of bystanders and witnesses. Although there have been some success with this approach, any further methods to increase the success rate

* Corresponding author.

E-mail addresses: xiaodong.lin@uoit.ca (X. Lin), rxlu@bbcr.uwaterloo.ca (R. Lu), dkwan@georgina.ca (D. Kwan), xshen@bbcr.uwaterloo.ca (Xuemin (Sherman) Shen).

should be welcomed by the general public. Nowadays there are many existing location technologies (e.g., GPS, Satellite), which can be used to keep track of the location of a child. However, with these technologies, the children being tracked must carry a GPS receiver or cellular phone. GPS receivers and cellular phones are moderately sized electronic devices that require extra care and protection to prevent damage to the components. As a result, these devices become very inconvenient to the children when playing in an amusement park, especially during water-related activities. Another approach to personnel tracking is to implant a special chip into a person, so that the person can be tracked through communication between the chip and a satellite. However, it is extremely expensive to implement for the purpose of tracking in an amusement park setting and requires a chip to be permanently implanted into the children. Thus, it is highly desired to have cost effective and efficient personnel tracking systems in place to protect children in public venues.

Recently, RFID technology [3–5] has been emerging as a promising method for the purpose of identification and tracking using radio waves due to its low cost and broad applicability. In this paper, we present a new RFID-based privacy-preserving children tracking (REACT) scheme, which utilizes RFID tags placed on children, for example, integrated to a wristband which is worn by a child, and will track their movements throughout the park as they pass through the various checkpoints equipped with RFID readers. The data (also called tag information) collected from these checkpoints will be relayed back to storage nodes wirelessly where queries can be performed by the park operators to locate a child in the park at the request of the parent. Although the proposed REACT scheme will be based on an amusement park setting, the system should be portable to fit any public venue.

However, there are several challenges facing RFID-based personnel tracking system for amusement parks. Firstly, with the large physical area that must be covered, there will be a large number of RFID readers scattered around the park in order to effectively monitor the entire park due to the limited coverage of RFID radio. It will be infeasible and inefficient to provide consistent network connections to all RFID readers with the backbone network, where storage nodes are located, over a wireless or wired link. While some readers may have consistent communication links with the backbone network, the majority of the readers have to relay information between themselves and the storage nodes through the help of other communication devices carried by park employees and visitors (or patrons). Secondly, security and privacy preservation is of importance to the success of such a tracking system. It is crucial to prevent any adversary from being able to track and/or control children, which could pose security threats to the general public and lead to child abduction. Finally, it is well known that RFID devices, in particular, RFID tags, lack computation, storage, energy, and communication capacities necessary for most cryptographic schemes adopted by most of security and privacy preservation protocols. As a result, it is critical to design an efficient and effective secure and privacy-preserving protocol between a tag and a reader suitable for an RFID

environment. In summary, the main contributions of this paper are threefold.

- Firstly, we study a hierarchical network framework composing of RFID readers, storage nodes and central control center to efficiently monitor a large-scale amusement park, and propose an RFID-based children tracking (REACT) scheme, where the tag information can be forwarded from RFID readers to the storage nodes with a *pocket switched network* [6] formed by park employees and visitors who carry the wireless communication devices in the amusement park. With the REACT scheme, the location of a lost child with an attached passive RFID tag can be effectively identified in a large amusement park. To the best of our knowledge, the proposed REACT scheme is the first RFID-based solution to effectively track children in a large-scale amusement park.
- Secondly, to prevent a *privacy-curious* attacker from being able to track and/or control children in a large amusement park, the child's privacy (in particular, identity privacy and unlinkable location privacy [7–11]) in the proposed REACT scheme are concealed. Even though an attacker obtains the current position of a child, it still cannot infer the past locations of the child, also known as forward security.
- Thirdly, we develop a custom simulator to demonstrate the effectiveness of the proposed REACT scheme. The more visitors participating in the *pocket switched network*, the more quickly the proposed REACT scheme can identify the locations of lost children in a large amusement park.

The remainder of this paper is organized as follows. In Section 2, we introduce the system model, communication model and design goal. Then, we present the REACT scheme in Section 3, followed by the security analysis and performance evaluation in Sections 4 and 5, respectively. We also review some related work in Section 6. Finally, we draw our conclusions in Section 7.

2. System model, communication model and design goal

In this section, we formulate the system model, the communication model, as well as identify the design goal.

2.1. System model

We consider a heterogeneous RFID-based children tracking system, which consists of a control center (CC), a small number of resource-rich storage nodes $\mathcal{S} = \{s_1, s_2, \dots\}$ and a large number of RFID readers $\mathcal{R} = \{r_1, r_2, \dots\}$, in a large amusement park, i.e., Canada's Wonderland [2], as shown in Fig. 1.

- Control center (CC): The CC is a trustable and powerful entity and is usually located at the amusement park entrance, for example, guest services room. The CC is responsible for the management of the storage nodes and RFID readers as well as the registration of chil-

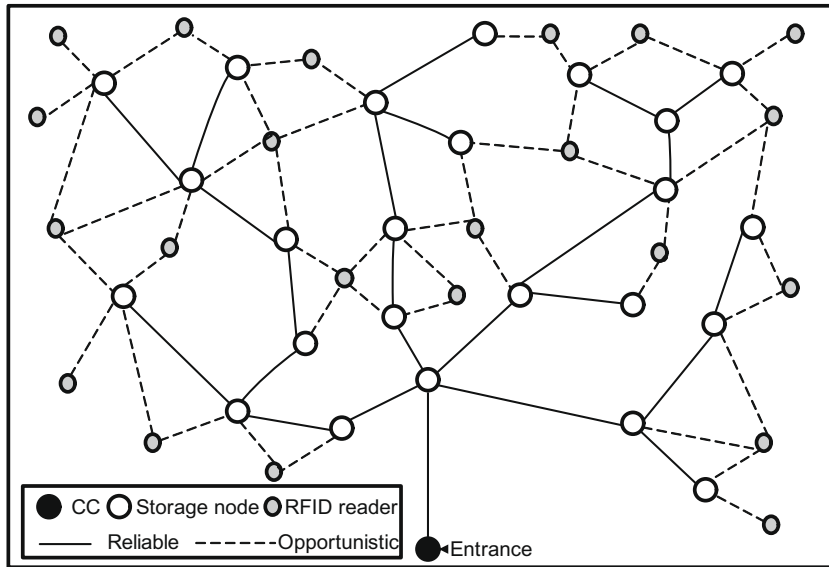


Fig. 1. Network model under consideration in a large amusement park.

dren-carrying RFID tags. Later, when parents lose their children in the amusement park, the CC can help them query and locate the previous and current positions of the specific children via the deployed storage nodes and RFID readers.

- Storage nodes $\mathcal{S}$: Storage nodes with their high-storage-capacity play a vital role for the RFID-based children tracking system. Storage nodes are usually deployed at the intersections in the amusement park. The main task of these storage nodes is to (i) store the data reported by the RFID readers and (ii) answer queries from the parents at the control center.
- RFID readers $\mathcal{R}$: A large number of RFID readers are deployed at different locations in the amusement park. Each RFID reader consists of a radio frequency transmitter and receiver. Once a passive RFID tag attached on a child is within range of an RFID reader, the RFID reader can read the tag information. Because the RFID reader is not rich in storage, it will periodically report the collected tag information to the storage nodes.

2.2. Communication model

2.2.1. Communication between CC and storage nodes

We assume both the CC, denoted as s_0 , and storage nodes $\mathcal{S} = \{s_1, s_2, \dots\}$ are equipped with wireless communication devices, e.g., WiFi or cellular system. At the same time, the communications among $\{s_0, s_1, s_2, \dots\}$ are bidirectional, i.e., two nodes within their wireless transmission range R may communicate with each other. Therefore, if a storage node s_i is close to the CC s_0 , it can directly contact with the CC. However, if a storage node is far from the transmission range of the CC, it should resort to other nodes to establish a route and then communicate with the CC. Formally, the communication between the CC and storage nodes can be represented as an undirected graph $G = (\mathcal{S}, E)$, where $\mathcal{S} = \{s_0, s_1, s_2, \dots\}$ and $E = \{e_{ij} | s_i, s_j \in \mathcal{S}\}$ is the

set of edges. If the distance $|s_i - s_j|$ is less than or equal to the transmission range R , $e_{ij} = 1$. Otherwise, $e_{ij} = 0$. Because the storage nodes $\mathcal{S} = \{s_1, s_2, \dots\}$ are well deployed in the amusement park, it is reasonable to assume that $G = (\mathcal{S}, E)$ is a connected graph. Then, based on the Dijkstra shortest path algorithm [12], each storage node $s_i \in \mathcal{S}$ can find its shortest reliable path to the CC.

2.2.2. Communication between storage node and RFID readers

The RFID readers are usually deployed at on-demand spots. When an RFID reader is very close to the intersection in the amusement park, it could directly communicate with the nearby storage node. However, if the RFID reader is far away from the storage node, the communication becomes *opportunistic*. In specific, the RFID reader reports the tag information by a *pocket switched network* [6], as shown in Fig. 2, where the pocket nodes (including the park's employees and visitors) carrying wireless devices in their pockets pull the collected tag information from RFID readers and push them to the storage nodes in their travel path.

2.2.3. Communication between RFID reader and tags

Assume that the RFID tags attached to the children in the amusement park are inexpensive passive tags, which are powered by the signal of an interrogating reader. Therefore, the communication between the RFID readers and tags only work within short ranges. i.e., a few meters.

2.3. Design goal

Before describing the design goal for the RFID-based children tracking system, we make the following assumptions in our system. First, all devices in the amusement park, including the control center, storage nodes and RFID readers, are in fixed positions. Once they are deployed in the amusement park, their positions cannot be easily displaced. In our system, we assume that the control center

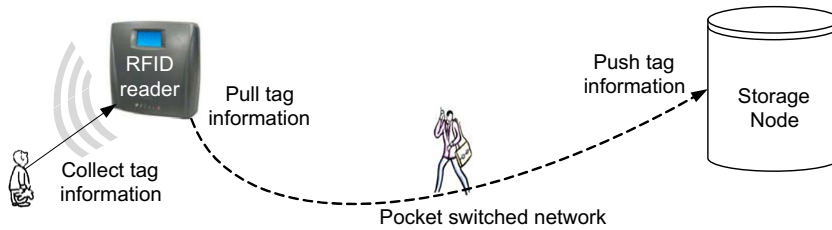


Fig. 2. Pocket switched network in large amusement parks.

is fully trustable, storage nodes are not compromised, while the RFID readers could be faked by some attackers used for collecting tag information. Concretely, we consider a *privacy-curious* attacker in the threat model as follows: A *privacy-curious* attacker is a party that doesn't kidnap children at the amusement park, yet attempts to learn and trace the position information of a specific child. Specifically, to reveal the location privacy of a child, the attacker could use fake RFID readers to link the positions of the child. Note that an attacker can also perform a denial of service (DoS) attack such that a legitimate RFID reader fails to read the normal RFID tags in a large amusement park. However, the DoS attack cannot compromise the location privacy of child. Thus, how to defend against DoS attacks are beyond the scope of this paper.

To resist the *privacy-curious* attacker, our design goal in this paper is to develop an RFID-based privacy-preserving children tracking system which can achieve the following requirements:

- R-1: Once a child is lost in a large amusement park, the proposed tracking system should be able to help the parent effectively locate the position of the child.
- R-2: The proposed tracking system should also have ability to conceal the child's privacy from a *privacy-curious* attacker, even after the attacker has eavesdropped and collected many tag information using bogus RFID readers.
- R-3: The RFID tags attached on the children should be very low cost such that parents are willing to accept the children tracking service in a large amusement park.

3. Proposed RFID-based privacy-preserving children tracking scheme

In this section, we present our RFID-based privacy-preserving children tracking (REACT) scheme, which mainly consists of the following parts: system initialization, child registration, privacy-preserving location information collection, opportunistic location information aggregation, and child location query. Before introducing our scheme, we first review the architecture of the low cost passive RFID tag, which guides what security techniques can be chosen and implemented in the children tracking system.

3.1. Passive RFID tag's architecture

The architecture of a passive RFID tag is shown in Fig. 3, which includes a coiled antenna and a less complex chip.

Because a passive tag is typically inexpensive, it doesn't contain a battery itself [3]. Instead, the power is supplied by the RFID reader. For example, when radio waves from an RFID reader are encountered by a passive tag, the coiled antenna within the tag forms a magnetic field, where the tag can draw the power and energize the circuits in the chip, and then use the energy to send the information stored on the tag to the RFID reader.

The chip embedded in the tag is less complex, which cannot support neither a timer, a random number generator (RNG) [13] nor high-cost cryptographic algorithms [14]. The only cryptographic algorithm that a passive tag can support is the Linear Feedback Shift Register (LFSR) based hash function [15], where the generation of hash is only based on multiplications with random binary matrixes. Let $H: \{0,1\}^m \rightarrow \{0,1\}^n$, where $n < m$, be an efficient keyed LFSR based hash function, which can map any input $M = (M_1, M_2, \dots, M_m)$ into a shorter hash value $H(K; M) = (h_1, h_2, \dots, h_n)$ with a key $K = \{k_1, k_2, \dots, k_n\}$. LFSR based hash function is simple but keeps most of the strength of the Carter–Wegman hash family [16]. See the Appendix for the detailed LFSR based hash construction. Formally, a secure hash function is called ϵ -balanced if $\forall \tilde{M} \neq 0, h$, the probability $\Pr[H(\tilde{M}) = h] \leq \epsilon$. As proved in [15], we know the LFSR based hash function $H: \{0,1\}^m \rightarrow \{0,1\}^n$ is ϵ -balanced for $\epsilon \leq \frac{m}{2^{n-1}}$. When $n = 64$, $m = 128$, $\epsilon \leq \frac{1}{2^{56}}$, which shows that LFSR based hash function achieves good security/cost ratio and can be securely applied in RFID-based children tracking system.

3.2. Detailed procedure of the REACT scheme

3.2.1. System initialization

Based on the system requirements, the following steps are performed by the control center to bootstrap the system:

Step 1 (Initialize system parameters): Let $\mathbb{G}$ and $\mathbb{G}_T$ be two cyclic groups of large prime order q . Suppose $\mathbb{G}$ and $\mathbb{G}_T$ are

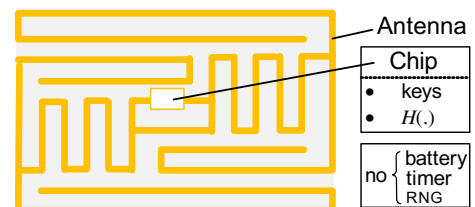


Fig. 3. Architecture of a passive RFID tag under consideration.

equipped with a pairing, i.e., a non-degenerated and efficiently computable bilinear map $e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$ such that $e(g_1^a, g_2^b) = e(g_1, g_2)^{ab} \in \mathbb{G}_T$ for all $a, b \in \mathbb{Z}_q^*$ and any $(g_1, g_2) \in \mathbb{G} \times \mathbb{G}$ [17]. Let g be the generator of $\mathbb{G}$, the control center chooses a random $s \in \mathbb{Z}_q^*$ as the master key, and computes the public key $P_{cc} = g^s$. In addition, three secure cryptographic hash functions H_0, H_1, H are chosen, where $H_0 : \{0, 1\}^* \rightarrow \mathbb{G}$, $H_1 : \{0, 1\}^* \rightarrow \mathbb{Z}_q^*$ and $H : \{0, 1\}^{128} \rightarrow \{0, 1\}^{64}$ be a LSRF based hash function constructed from an irreducible LFSR hash polynomial with degree 64 over $GF(2)$, i.e., $f(x) = x^{64} + \sum_{i=0}^{63} c_i \cdot x^i$, for $c_i \in \{0, 1\}$. In the end, the control center sets the system parameters as $params = \{\mathbb{G}, \mathbb{G}_T, q, g, e, P_{cc}, H_0, H_1, H, f(x)\}$.

Step 2 (Deploy storage nodes): The control center preloads each storage node $s_i \in \mathcal{S} = \{s_1, s_2, \dots\}$ with $params = \{\mathbb{G}, \mathbb{G}_T, q, g, e, P_{cc}, H_0, H_1, H, f(x)\}$ and a private key $sk_i = H_0(s_i)^s$, where s_i is the identity of the i th storage node, and deploys s_i at a critical point in the large amusement park, for example, an intersection. Because any two neighboring storage nodes s_i and s_j can derive their static shared key $k_{ij} = H_1(e(sk_i, H_0(s_j))) = H_1(e(sk_j, H_0(s_i)))$, the node-to-node authentication is achieved [17]. Sequentially, the authenticated transmission from any storage node to the control center is guaranteed as well.

Step 3 (Deploy RFID readers): The control center also deploys each RFID reader $r_i \in \mathcal{R} = \{r_1, r_2, \dots\}$ at critical locations L_i in the large amusement park, then preloads the reader r_i with $params = \{\mathbb{G}, \mathbb{G}_T, q, g, e, P_{cc}, H_0, H_1, H, f(x)\}$ and a location-aware private key $lk_j = H_0(L_i)^s$. Later, when the RFID reader is ready to report the collected tag information, it can use the location-aware key lk_j to sign location-based signature for authentication.

3.2.2. Child registration

Assume that the amusement park opens at time t_s and closes at time t_e every day, and the control center divides the period $t_e - t_s$ into l time slots $T_1, T_2, \dots, T_l$, where each $T_i \in \{0, 1\}^{128}$. When parents decide to choose the children tracking service for their child c_i in the large amusement park at slot T_α during their visit to the park, they first make a registration at the control center. Then, the control center executes the following steps:

- Step 1:** The control center assigns a 64-bit key $K_i = (k_1^i, k_2^i, \dots, k_{64}^i)$ for each time slot T_i , where $T_\alpha \leq T_i \leq T_l$. Because the passive RFID tag is low-storage and in order to achieve forward security, the key $K_{i+1} = (k_1^{i+1}, k_2^{i+1}, \dots, k_{64}^{i+1})$ in slot T_{i+1} is derived from $K_i = (k_1^i, k_2^i, \dots, k_{64}^i)$ in slot T_i by applying the LSRF based hash function H , i.e., $K_{i+1} = H(K_i; T_i)$.
- Step 2:** The control center initializes a new passive RFID tag and preloads the tag with the key K_α in slot T_α , the LSRF based hash function H , and the current timestamp t_c .
- Step 3:** The control center attaches the tag on the child c_i in a reliable way. In such a way, the tag won't easily drop when the child is playing.

Note that, for the reason of security, the control center doesn't deal with the scenario when multiple children reg-

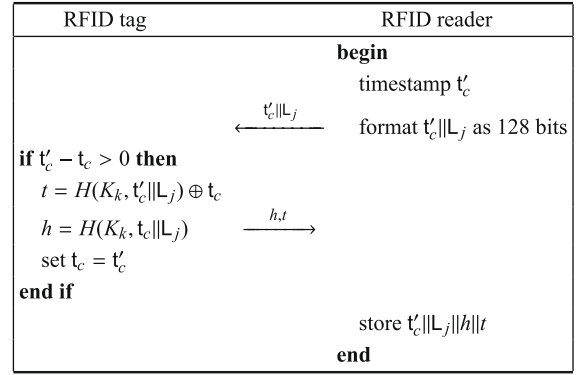


Fig. 4. Privacy preserving location information collection.

ister simultaneously, instead, only one child can register at one time.

3.2.3. Privacy preserving location information collection

When a child c_i attached with an RFID tag passes by an RFID reader at some location L_j , where the length of the identifier L_j is 64 bits, in the large amusement park at time slot T_k . As shown in Fig. 4, the RFID reader can detect it and read the tag information by performing the following interactive query protocol.

- Step 1:** The RFID reader first gains the current 64-bit timestamp t'_c , then formats the time & location $t'_c || L_j$ into 128 bits information, and finally sends $t'_c || L_j$ to the RFID tag.
- Step 2:** Upon receiving $t'_c || L_j$, the RFID tag first checks whether $t'_c - t_c > 0$. If it is true, the RFID tag uses the key K_k available at time slot T_k to compute $t = H(K_k, t'_c || L_j) \oplus t_c$, $h = H(K_k, t_c || L_j)$, and returns h, t to the RFID reader. Otherwise, the RFID tag doesn't respond the current RFID reader's query.
- Step 3:** After receiving the returned values h, t , the RFID reader formats the record $t'_c || L_j || h || t$ and temporarily stores it. Note that, each record here is only 256 bits.

3.2.4. Opportunistic tag information aggregation

Because the RFID reader is not rich in storage, each reader r_j at location L_j will periodically report the tag information to the storage nodes in a batch manner. The detailed steps are executed as follows.

- Step 1:** The RFID reader first aggregates several collected tag information into one record rec_j , and then uses the location-aware key $sk_j = H_0(L_j)^s$ to make a signature [18] on rec_j as $\sigma_j = (a_j, b_j)$, where $a_j = H_0(L_j)^r$, $b_j = sk_j^{r+H_1(rec_j, a_j)}$ with some random number $r \in \mathbb{Z}_q^*$.
- Step 2:** If the RFID reader is close to the intersection and within the transmission range of one nearby storage node, the RFID reader will directly send (rec_j, σ_j) to the storage node. If the RFID reader is far away from the some storage nodes, it will resort to the *pocket switched network* formed by selected visitors to carry the information (rec_j, σ_j)

to the storage nodes in an *opportunistic* manner, as shown in Fig. 5. In order to enhance the reliability in *opportunistic* transmission, Multi-Copy Multi-Destination (MCMD) policy is adopted, in which multi copies of (rec_j, σ_j) will be carried by different visitors to multi storage nodes.

It is worth noting that only a certain percentage of visitors are willing to register their own wireless devices to help carry and forward aggregated tag information. However, it is mandatory for each park employee to carry a wireless device to help with tag information forwarding.

Step 3: When a storage node receives a copy of (rec_j, σ_j) , it first uses the location L_j to verify the location-based signature σ_j by checking $e(g, b_j) \stackrel{?}{=} e(P_{cc}, a_j \cdot H_0(L_j)^{H_1(rec_j, a_j)})$. If it holds, the tag information in rec_j is authenticated and will be stored in the storage node; otherwise, rec_j will be rejected. The correctness is shown as follows:

$$\begin{aligned} e(g, b_j) &= e(g, sk_j^{r+H_1(rec_j, a_j)}) \\ &= e(g, H_0(L_j)^{s(r+H_1(rec_j, a_j))}) \\ &= e(g^s, H_0(L_j)^{r+H_1(rec_j, a_j)}) \\ &= e(P_{cc}, a_j \cdot H_0(L_j)^{H_1(rec_j, a_j)}). \end{aligned} \quad (1)$$

Batch verification. When several records $(rec_1, \sigma_1), \dots, (rec_n, \sigma_n)$ from different locations $(L_1, \dots, L_n)$ arrive at the storage node simultaneously, the following batch verification is adopted to improve the verification efficiency, i.e., $e(g, \prod_{i=1}^n b_i) = e(P_{cc}, \prod_{i=1}^n a_i \cdot H_0(L_i)^{H_1(rec_i, a_i)})$. The correctness of the batch signature verification can be derived from Eq. (1), and we refer readers to [19] for the efficiency and security analysis.

3.2.5. Child location query

When parents cannot find their child c_i from time slot T_s , they can report to the park authority and request the control center to help locate the child. Then, the child location query is executed in the following steps.

Step 1: Let K_s be the key of the passive RFID tag attached on the child c_i at time slot T_s . The control center first broadcasts the K_s to all storage nodes. Because

the secure channels have been established amongst the control center and all storage nodes, the query with (K_s, T_s) wouldn't be disclosed.

Step 2: After receiving (K_s, T_s) , each storage node $s_i \in S$ first computes the key set $\mathbb{K} = \{K_s, K_{s+1}, \dots, K_l\}$ with the LFSR based hash function H such that $K_{i+1} = H(K_i, T_i)$ where $T_s \leq T_i < T_l$. Then, the storage node s_i invokes the Algorithm 1 to get the privacy-preserving tracking records $\mathbb{D}'$.

Algorithm 1: Privacy Preserving Tracking Query

1: Procedure Privacy Preserving Tracking Query

Input: $\mathbb{K} = \{K_s, K_{s+1}, \dots, K_l\}$ and collected tag information $\mathbb{D} = \{t'_c \| L_j \| h \| t \mid t'_c \in [T_s, T_l]\}$

Output: $\mathbb{D}'$

```

2: set  $\mathbb{D}' = null$ 
3: for each record  $(t'_c \| L_j \| h \| t) \in \mathbb{D}$ 
4:   if  $t'_c \in$  time slot  $T_i$ , where  $T_s \leq T_i \leq T_l$ 
5:     compute  $t_c = H(K_i, t'_c \| L_j) \oplus t$ 
6:     if  $h = H(K_i, t_c \| L_j)$ 
7:       set  $\mathbb{D}' = \mathbb{D}' \cup \{(t'_c \| L_j \| h \| t)\}$ 
8:     end if
9:   end if
10: end for
11: return  $\mathbb{D}'$ 
12: end Procedure

```

Step 3: Each storage node returns its records $\mathbb{D}'$ to the control center via a predefined shortest path. Since the MCMD policy is adopted in the *opportunistic* tag information aggregation, the redundant records may produce in some downstream nodes when being forwarded to the control center. Therefore, before further forwarding the records, each downstream node should aggregate those records coming from its upstream nodes to eliminate the redundancy.

Step 4: After receiving all records related to the specific child c_i , the control center can construct the tracking information, as shown in Fig. 6. In addition, because a child usually stays at some amusement spot for some time, the current position of the child can be identified based on these track information.

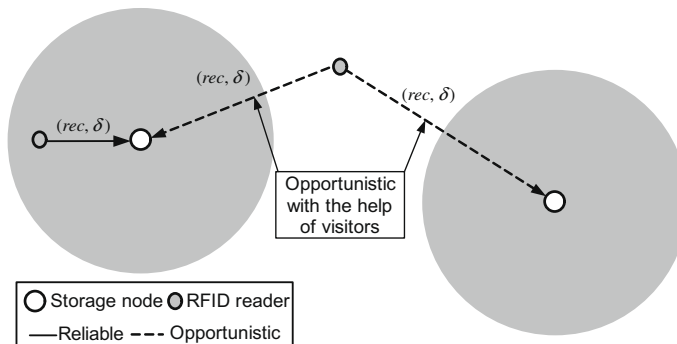


Fig. 5. Opportunistic tag information aggregation in MCMD policy.

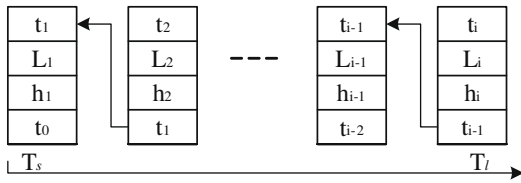


Fig. 6. Tracking information reconstructed at control center.

Correctness. Because of the one-wayness of the LSFR based hash function, only the authentic RFID tag attached on the child c_i can compute the real hash value. Thus, the storage nodes S can identify it once granted with the corresponding key. Since a previous timestamp t_c can be computed from each tag current information $t'_c \parallel L_j \parallel h \parallel t$, the child's tracking information can be plotted based on such linkability. Note that the tracking information is conditionally revealed. Without knowing the key K_k , t_c cannot be derived from $t = H(K_k, t'_c \parallel L_j) \oplus t_c$ and $h = H(K_k, t'_c \parallel L_j)$.

4. Security analysis

In this section, we analyze the security of the proposed RFID-based privacy-preserving children tracking scheme.

Following the system model discussed earlier, we know that the weakest part in the RFID-based tracking system is the passive RFID tag. According to the principle that security relies essentially on the strength of the weakest link [20], the privacy preservation in RFID-based system depends primarily on the security of passive RFID tag. Because the passive RFID tag is less expensive and, at the same time, supports less complexity cryptographic algorithms than other high-trustable devices, the perfect security in the passive RFID tag does not exist and would probably be ineffective and prohibitively expensive if it does exist. Therefore, a reasonable metric to measure the privacy preservation provided by the passive RFID tag is the privacy/cost ratio (PCR). Given some PCR, the privacy that needs to be protected is in direct proportion to the costs associated with privacy preservation. Thus, for low cost passive RFID tag, the provided privacy is obviously limited. Because the large amusement park is not as hostile as other scenarios, we only focus on the privacy preservation against a *privacy-curious* attacker in the amusement park. Specifically, the following security requirements can be achieved.

- **Identity privacy:** During the child registration phase, it is the control center that randomly chooses a key K_α for a specific child c_i , and no one else can link a key to the real child's identity, i.e., $K_\alpha \not\Rightarrow c_i$. Therefore, the identity privacy is ensured, even when a privacy-curious attacker obtains the key by compromising the passive RFID tag attached on the child.
- **Unlinkable location privacy:** Given two tag information $t_1 \parallel L_1 \parallel h_1 \parallel t$ and $t_2 \parallel L_2 \parallel h_2 \parallel t$. Because of the one-wayness of the LSFR based hash function $H()$, a privacy-curious attacker cannot extract the keys from h_1 and h_2 , and thus cannot judge whether or not they are produced by the same RFID tag. A privacy-curious attacker could

replay an RFID query with $t'_c \parallel L_j$ once it obtains a tag information $t'_c \parallel L_j \parallel h \parallel t$. However, even though no RNG and timer are implemented in the passive RFID tag (due to its cost limitation), the RFID tag can still resist this kind of attack. Because each tag stores the last-access timestamp t_c , once a timestamp $t'_c (< t_c)$ is replayed, the judge condition $t'_c - t_c > 0$ cannot pass in many RFID tags. Thus, the privacy-curious attacker has no idea to link a tag information with a specific child, and the location-link privacy is achieved.

- **Forward security.** Forward security means, even though an RFID tag is compromised at time slot T_s , the attacker, with the key K_s at T_s , cannot track the locations in the past time slots ($< T_s$). In the following, we formally prove that the passive RFID tag can achieve the forward security. Before proceeding with the proof, we first formalize the forward security model by the challenge-response game below.

Forward Security Game. In the game, the interaction between an attacker $\mathcal{A}$ and the passive RFID tags only occurs via oracle queries, which model the attacker capabilities in the real RFID attack scenarios. During the game, the attack may query different RFID tags at any given time slot T_s . Let T_i^s denote the instance i of a passive RFID tag at T_s and let b be a bit chosen uniformly at random. The query types available to the attacker are as follows:

- **Execute** ($T_1^s, T_2^s, \dots, T_n^s$): This query models the privacy-curious attacker $\mathcal{A}$ passively eavesdrops on honest executions among the RFID tags $T_1^s, \dots, T_n^s$ and RFID readers. It returns the tag information that were exchanged during an honest execution.
- **Send** ($T_i^s, t'_c \parallel L_j$): This query models an active attack, in which the privacy-curious attacker $\mathcal{A}$ actively uses an illegal RFID reader to obtain the tag information that an RFID tag T_i^s would generate upon receipt of the query $t'_c \parallel L_j$.
- **Corrupt** (T_i^s): This query models the privacy-curious attacker $\mathcal{A}$ obtains the key K_s by compromising T_i^s .
- **Test** ($T_i^{s-1}, I_0^{s-1}, I_1^{s-1}$): This query tries to capture the attacker's ability to link a tag information of the corrupted instance i in time slot T_{s-1} . The challenger runs the follows steps: (1) Flip a coin and get $b \in \{0, 1\}$; (2) Set I_b^{s-1} be the real tag information of instance i , and I_{1-b}^{s-1} be a tag information of other instance $\neq i$; (3) Send I_0^{s-1}, I_1^{s-1} to the privacy-curious attacker $\mathcal{A}$; (4) Obtain the guessing bit b' returned from $\mathcal{A}$.

We denote the advantage of the privacy-curious attacker $\mathcal{A}$ as the probability that $\mathcal{A}$ correctly guesses the value of b ; more precisely we define $\text{Adv}(\mathcal{A}) = 2\Pr[b = b'] - 1$, where the probability space is over all the random coins of the attacker and all the oracles. The RFID tag is said to be *forward security* if $\mathcal{A}$'s advantage is negligible in the security parameters.

Theorem 1 (Forward security). *The passive RFID tag can achieve the forward security provided that the LSFR hash function $H: \{0,1\}^{128} \rightarrow \{0,1\}^{64}$ is one-day secure in the RFID tag, where one-day secure means that the inverting of the hash H cannot be successful in one-day.¹*

Proof. The result comes from the fact that the attacker $\mathcal{A}$ cannot invert the LSFR based hash function. More precisely, suppose that, after a huge number of *Execute* and *Send* queries and obtaining the key K_s by *Corrupt*(T_i^s) in time slot T_s , the attacker $\mathcal{A}$ can win the above forward security game with a non-negligible advantage $\text{Adv}(\mathcal{A}) = \varepsilon$. That is, the attacker $\mathcal{A}$ can distinguish a valid tag information $t'_c \| L_j \| h \| t$ at time slot T_{s-1} , where $t'_c \in T_{s-1}$. By observing $t = H(K_{s-1}, t'_c \| L_j) \oplus t_c, h = H(K_{s-1}, t_c \| L_j)$, we know that the attacker $\mathcal{A}$ can correctly guess $b = b'$ by only two ways: (1) directly guessing b with $1/2$ probability, denoted as the event E_1 ; (2) obtaining the key K_{s-1} from K_s , where $K_s = H(K_{s-1}, T_{s-1})$, denoted as the event E_2 . Then, $\Pr[b = b'] = \Pr[E_1] + \Pr[E_2] = \frac{1}{2} + \Pr[E_2]$. By combining the definition $\text{Adv}(\mathcal{A}) = \varepsilon = 2\Pr[b = b'] - 1$ in the game, we have $\Pr[E_2] = \frac{\varepsilon}{2}$. Because ε is a non-negligible advantage, then $\Pr[E_2] = \frac{\varepsilon}{2}$ shows that the attacker $\mathcal{A}$ can invert the LSFR based hash with another non-negligible probability, but it contradicts with the LSFR hash function $H()$ is one-day secure in the RFID tag. Therefore, the passive RFID tag can achieve the forward security. $\square$

Note. Due to the low cost of the passive RFID tag, an attacker $\mathcal{A}$ could use the close time t_e to query the passive RFID tag. Then, any query with normal timestamp t'_c , where $t'_c < t_e$, will be rejected, as shown in Fig. 4. This is one kind of DoS attacks. As discussed in the earlier attack model, the DoS attacks are not considered in the current system. Nevertheless, if we increase the cost of the passive RFID tag by adding a timer, this kind of DoS attack can be easily resisted by checking the validity of the current timestamp t'_c .

5. Performance evaluation

In this section, we evaluate the performance of the proposed REACT scheme. Because the primary goal of the REACT scheme is to help parents identify the location of their lost children as quickly as possible, the high reliability and low latency are desirable. Recall that the tag information aggregation is based on pocket switched network, thus the opportunistic aggregation becomes the dominant factor affecting the reliability and the latency of the whole scheme. (Note that, the communications between the control center and storage nodes are reliable as discussed earlier, which thus do not incur high latency in the system.) In the following, taking the *delivery ratio* (defined as the fraction of tag information that are correctly delivered from the RFID readers to some storage nodes within a given time period) and *delivery latency* (defined as the time between when a tag information is collected at some RFID reader and when it is aggregated at some storage node) as the performance metrics, we use our custom simulator built

in Java to demonstrate the performance of the opportunistic tag information aggregation.

5.1. Simulation setup

By statistics, a larger amusement park could averagely attract 1000 children everyday. To model such a large amusement park, 24 storage nodes with proper transmission radius are first deployed in a restricted $1200 \times 1200 \text{ m}^2$ area to establish a connected network with the control center, as shown in Fig. 1. Assume that there are total $n = 150$ amusement spots (attractions) in the area, and 150 RFID readers are uniformly deployed in these spots. In addition, a number of pocket devices carried by the visitors, which form the pocket switched network, are also rambling in the large amusement park. Concretely, the detailed parameter settings used in the simulations are summarized in Table 1. In order to achieve more stable simulation results, we set a 60-min warm-up time during which results are not collected. We also vary the number of replicated tag information from 1 to 3 to check the reliability in MCMD policy.

Mobility model. In the pocket switched network, the performance of networking applications is highly contingent upon the mobility of pocket device holders. As pocket devices are mostly carried by the adult visitors in the large amusement park, modeling the mobility patterns of visitors (including children) can achieve a relatively accurate performance evaluation. Let state st_0 be when a visitor enters/exits the amusement park, and st_i denotes that the visitor has visited i amusement spots in the amusement park. If the visitor just enters the amusement park, he/she will go to an unvisited spot with the probability $p = 1$. If the visitor has visited i spots, he/she goes to an unvisited spot with the probability $p = \rho$, and rambles in visited spots with $1 - \rho$. After having visited all spots, the visitor leaves the amusement park with the probability $p = \rho$. On average, the visitor will stay at each amusement spot with T_{avg} . However, if some event is triggered, e.g., the amusement park closure time approaching or tourist's emergence call incoming with the probability 0.01, the visitor directly leaves the amusement park with the probability 1. Fig. 7 shows such visitor mobility model.

Table 1
Simulation Settings.

Parameter	Setting
Simulation area	1200 m $\times$ 1200 m
Simulation warm-up time	60 min
Simulation duration time	120 min
Storage nodes's number	24
Storage node's transmission range	200 m
RFID readers' number	150
RFID reader's transmission range	50 m
Children's number	1000
Child's velocity	1.8–2.0 m/s
Transmission range of RFID tags	5 m
Number of pocket devices N_p	[20, 40, ..., 200]
Pocket device's transmission range	80 m
Pocket device's velocity	1.0–2.0 m/s
Ave. staying time at each spot T_{avg}	[10, 20, 30] min
Number of replica of tag info. N_c	[1, 2, 3]

¹ If the 64-bit hash length is not enough to achieve the one-day secure, the hash length can be adaptively extended.

In the following, we set the parameter ρ as 0.85 ± 0.08 , and simulate the pocket switched network based tag information aggregation with different parameters N_p , T_{avg} and N_c . The duration for each simulation is 120 min, and all results are averaged over 10 runs.

5.2. Simulation results

Fig. 8 presents the *delivery ratio* versus the number of pocket devices carried by the visitors N_p , under different T_{avg} and N_c . In each subfigure, it is observed that the *delivery ratio* improves with the increase of the number of pocket devices N_p . The more the pocket devices, the better the *delivery ratio*. The reason is that the tag information can

be carried from RFID readers to storage nodes with more chances, when large numbers of pocket devices are involved in the opportunistic tag information aggregation. In addition, with the decrease of the average staying time T_{avg} , the *delivery ratio* can be improved as well. Comparing all subfigures (a)–(c), we can also validate the *delivery ratio* is improved when the N_c increases.

We further evaluate the effect of the number of pocket devices N_p on the *average delay*, with results illustrated in Fig. 9. From the figure, we can see that, with (1) the increase of N_p ; (2) the increase of N_c ; or (3) the decrease of T_{avg} , the *average delay* will be reduced. However, in real amusement park scenarios, the condition (3) is impractical to decrease T_{avg} . Therefore, by (1) encouraging more visi-

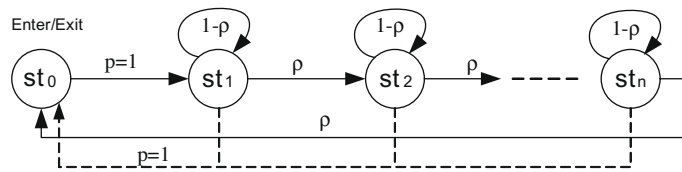


Fig. 7. Visitor mobility model considered in the large amusement park.

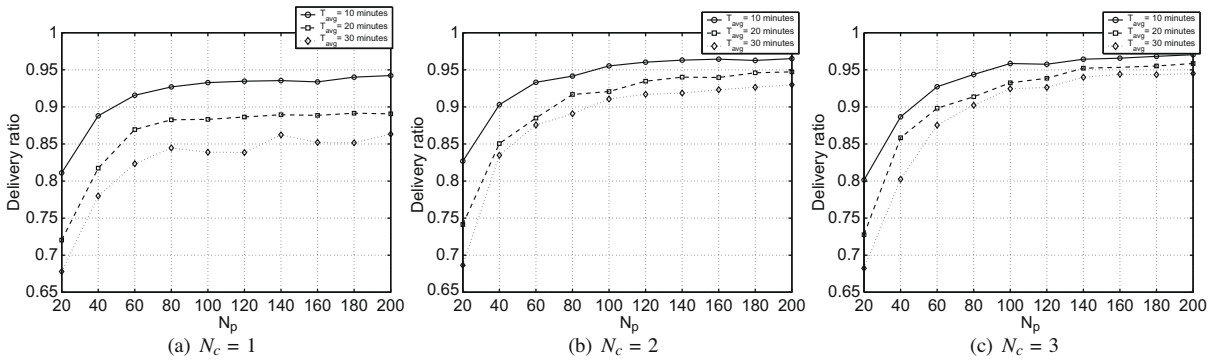


Fig. 8. Delivery ratio versus varying number of pocket devices.

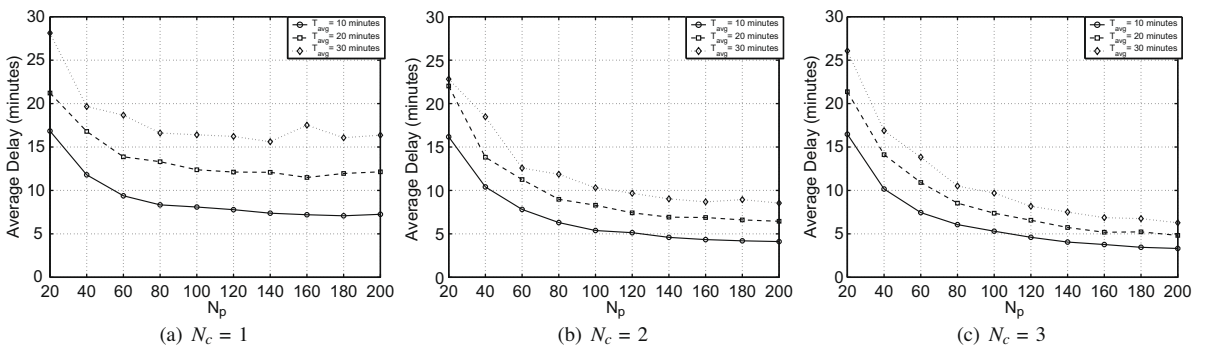


Fig. 9. Average delay versus varying number of pocket devices.

tors act as the pocket nodes plus (2) MCMD policy, the lost child can be quickly located by the proposed REACT scheme. Nowadays, missing children is a very serious issue facing our society. Various public campaigns can be launched to create awareness of missing children issues. As a result, we believe that more and more public are willing to serve as the pocket nodes during their visit to the park and thus make the proposed scheme very successful.

6. Related work

RFID-based personnel tracking is a major application and has attracted a lot of interest in recent years. Several efficient RFID-based personnel tracking schemes closely related to the proposed REACT scheme have been proposed [21–25]. However, the personnel's privacy-preserving during the tracking and positioning is not well addressed. In [21], Zhang et al. propose a general algorithm for RFID-based tracking and locating the persons in underground mine environments to help with management of mines and avoid enormous losses. However, due to the unique features of underground mine scenarios, the algorithm just investigates the optimal deployment of RFID readers, and leaves the person's privacy issues unconsidered. In [22], Huang et al. propose a psychiatric patient tracking system based on RFID technology. In the system, the collaboration among field generators, RFID readers and tags accomplishes the required functions in using RFID in psychiatric patient tracking. Specifically, the field generator constantly broadcast signals within its transmission range. When an RFID tag attached on the patient receives the trigger signal, it responds to a reader with the identifier of the field generator. Thus, the location of the patient associated with the tag can be approximately estimated. However, the system only aims to improve the tracking reliability, the patient's privacy is also not addressed. In [23], Satoh presents a framework for providing dynamically deployable settings. Using RFID-based tracking system, the framework can detect the people's location. Although the framework addresses the security and privacy issues, they are very sketchy. We have noticed that several detailed privacy-preserving RFID authentication schemes have been proposed, yet the privacy is only discussed at algorithm-level [26]. In [24,25], RFID-based children tracking has been studied, however the children privacy-preserving is not addressed.

Distinct from the above work, the proposed REACT scheme devises an RFID-based privacy-preserving children tracking in a large-scale area, and discusses the privacy-preserving in terms of both algorithm-level and system-level. In addition, since neither timer nor RNG is required, the architecture of the passive RFID tag employed in the REACT scheme is much simpler and less expensive, which attracts parents to accept the children tracking service in a large amusement park.

7. Conclusions

To help parents identify the locations of their lost children in large amusement parks, we have presented a pri-

vacy-preserving children tracking scheme based on RFID technology. The proposed scheme, named REACT, is characterized by the cooperation among RFID readers, storage nodes and control center as well as the employees and visitors of the parks in a large amusement park, and using the pocket switched network formed by the visitors to forward the children's tag information from RFID readers to some storage nodes for control center's query. By security analysis, the proposed REACT scheme achieves children's identity privacy, unlinkable location privacy and forward security. In addition, through extensive simulations we demonstrate the proposed REACT scheme can quickly locate the lost children's position, when more visitors are willing to participate in the pocket switched network in a large amusement park.

Acknowledgement

The research is financially supported by the Natural Sciences and Engineering Research Council of Canada (NSERC).

Appendix A

In the appendix, we will show how to construct LFSR based hash function $H: \{0,1\}^m \rightarrow \{0,1\}^n$, where n is the security parameter indicating the hash length, and m denotes the length of the input message $M = (M_1, M_2, \dots, M_m)$.

Let $f(x)$ be an irreducible LFSR hash polynomial with degree n over $GF(2)$, i.e., $f(x) = x^n + \sum_{i=0}^{n-1} c_i \cdot x^i$, where $c_i \in \{0,1\}$. Let $K = (k_1, k_2, \dots, k_n) \in \{0,1\}^n$ be a key, and set it as the initial state of LFSR hash. Then, LFSR outputs a sequence $(k_1, k_2, \dots, k_n, k_{n+1}, \dots, k_{n+m-1})$ with total $n + m - 1$ bits, and the sequence is used to construct a Toeplitz Matrix as

$$\mathbf{T}_M = \begin{pmatrix} k_n & k_{n+1} & \dots & k_{n+m-1} \\ \vdots & \vdots & \dots & \vdots \\ k_2 & k_3 & \dots & k_{m+1} \\ k_1 & k_2 & \dots & k_m \end{pmatrix}.$$

In the end, the hash value $H(K; M) = (h_1, h_2, \dots, h_n)$ on message $M = (M_1, M_2, \dots, M_m)$ can be calculated as

$$\begin{pmatrix} h_n \\ \vdots \\ h_2 \\ h_1 \end{pmatrix} = \mathbf{T}_M \cdot \begin{pmatrix} M_1 \\ M_2 \\ \vdots \\ M_m \end{pmatrix}.$$

Because of its simple construction, LFSR based hash function is suitable for the less complex hardware implementation in low cost passive RFID tag.

References

- [1] Missing Children Society of Canada, Website, <<http://www.mcsc.ca/>>.
- [2] Canada's Wonderland, Website, <<http://www.canadawonderland.com/>>.

- [3] Wikipedia, Radio-frequency identification, Website, <http://en.wikipedia.org/wiki/Radio-frequency_identification>.
- [4] J.-L. Chen, M.-C. Chen, C.-W. Chen, Y.-C. Chang, Architecture design and performance evaluation of RFID object tracking systems, *Computer Communications* 30 (9) (2007) 2070–2086.
- [5] M.A. Bonuccelli, F. Lonetti, F. Martelli, Instant collision resolution for tag identification in RFID networks, *Ad Hoc Networks* 5 (8) (2007) 1220–1232.
- [6] P. Hui, A. Chaintreau, J. Scott, R. Gass, J. Crowcroft, C. Diot, Pocket switched networks and human mobility in conference environments, in: *Proceedings of the 2005 ACM SIGCOMM workshop on Delay-tolerant networking*, Philadelphia, Pennsylvania, USA, 2005, pp. 244–251.
- [7] R. Lu, X. Lin, H. Zhu, P.-H. Ho, X. Shen, ECPP: Efficient conditional privacy preservation protocol for secure vehicular communications, in: *Proceedings of the 27th Conference on Computer Communications (INFOCOM 2008)*, Phoenix, Arizona, USA, April 2008, pp. 1229–1237.
- [8] X. Lin, X. Sun, P.-H. Ho, X. Shen, GSIS: a secure and privacy-preserving protocol for vehicular communication, *IEEE Transactions on Vehicular Technology* 56 (6) (2007) 3442–3456.
- [9] Y. Zhang, W. Liu, W. Lou, Y. Fang, Location-based compromise-tolerant security mechanisms for wireless sensor networks, *IEEE Journal on Selected Areas in Communications, Special Issue on Security in Wireless Ad Hoc Networks* 24 (2) (2006) 247–260.
- [10] R. Lu, X. Lin, H. Zhu, X. Shen, Spark: a new vanet-based smart parking scheme for large parking lots, in: *Proceedings of the 28th Conference on Computer Communications (INFOCOM 2009)*, Rio de Janeiro, Brazil, April 2009.
- [11] R. Lu, X. Lin, X. Shen, Spring: A social-based privacy-preserving packet forwarding protocol for vehicular delay tolerant networks, in: *Proceedings of the 29th IEEE International Conference on Computer Communications (INFOCOM 2010)*, San Diego, California, USA, March 2010.
- [12] E. Dijkstra, A note on two problems in connexion with graphs, *Numerische Mathematik* 1 (1959) 269–271.
- [13] H. Larrondo, M. Martin, C. Gonzalez, A. Plastino, O. Rosso, Random number generators and causality, *Physics Letters A* 352 (2006).
- [14] W. Mao, *Modern Cryptography: Theory and Practice*, Prentice Hall PTR, 2003.
- [15] H. Krawczyk, LFSR based hashing and authentication, in: *Proceedings of the 14th Annual International Cryptology Conference on Advances in Cryptology, Lecture Notes In Computer Science*, vol. 839, Springer-Verlag, 1994, pp. 129–139.
- [16] M.N. Wegman, J.L. Carter, New hash functions and their use in authentication and set equality, *Journal of Computer and System Sciences* 22 (3) (1981) 265–279.
- [17] D. Boneh, M.K. Franklin, Identity-based encryption from the weil pairing, in: *Proceedings of the 21st Annual International Cryptology Conference on Advances in Cryptology, Lecture Notes In Computer Science*, vol. 2139, Springer-Verlag, 2001, pp. 213–229.
- [18] J.C. Cha, J.H. Cheon, An identity-based signature from gap Diffie–Hellman groups, in: *Proceedings of the Sixth International Workshop on Theory and Practice in Public Key Cryptography, Lecture Notes In Computer Science*, vol. 2567, Springer-Verlag, 2003, pp. 18–30.
- [19] A.L. Ferrara, M. Green, S. Hohenberger, M. Pedersen, Practical short signature batch verification, in: *The Cryptographers' Track at the RSA Conference 2009 (CT-RSA 2009)*, Lecture Notes In Computer Science, 5473, Springer-Verlag, 2009, pp. 309–324.
- [20] B. Schneier, *Beyond Fear: Thinking Sensibly About Security in an Uncertain World*, Springer, 2006.
- [21] G. Zhang, L. Zhang, X. Liu, Time-shifting tracking and locating algorithm for rtltum system, in: *Proceedings of International Conference on Industrial and Information Systems*, 2009, IIS'09, April 2009, pp. 7–10.
- [22] C.-L. Huang, P.-C. Chung, M.-H. Tsai, Y.-K. Yang, Y.-C. Hsu, Reliability improvement for an RFID-based psychiatric patient localization system, *Computer Communications* 10 (3) (2008) 2039–2048.
- [23] I. Satoh, Location-based services in ubiquitous computing environments, *International Journal on Digital Libraries* 6 (3) (2006) 280–291.
- [24] A. Bednars, RFID everywhere: From amusement parks to blood supplies, *network world*, May 3, 2004.
- [25] L. Sullivan, Legoland uses wireless and RFID for child security, *InformationWeek.com*, April 28, 2004.
- [26] RFID Security & Privacy Lounge, Website, <<http://www.avoine.net/rfid/>>.



Xiaodong Lin received the Ph.D. degree in information engineering from Beijing University of Posts and Telecommunications, Beijing, China, in 1998 and the Ph.D. degree (with Outstanding Achievement in Graduate Studies Award) in electrical and computer engineering from the University of Waterloo, Waterloo, ON, Canada, in 2008. He is currently an Assistant Professor of information security with the Faculty of Business and Information Technology, University of Ontario Institute of Technology, Oshawa, ON, Canada. His research interests include wireless network security, applied cryptography, computer forensics, software security, and wireless networking and mobile computing. He was the recipient of a Natural Sciences and Engineering Research Council of Canada (NSERC) Canada Graduate Scholarships (CGS) Doctoral and the Best Paper Awards of the IEEE International Conference on Computer Communications and Networks (ICCCN 2009) and IEEE International Conference on Communications (ICC'07) - Computer and Communications Security Symposium.



Rongxing Lu is currently working toward the Ph.D. degree with the Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, Ontario, Canada. He is currently a Research Assistant with the Broadband Communications Research (BBCR) Group, University of Waterloo. His research interests include wireless network security, applied cryptography, and trusted computing.



environments.

Davis Kwan received the master degree in Information Technology Security from the University of Ontario Institute of Technology, Oshawa, ON, Canada, in 2009 and Bachelor degree in Administrative Studies, Information Technology from York University, Toronto, ON, Canada, in 2005. He is currently employed at the Town of Georgina, Ontario, Canada, in the role of IT Network Security Administrator. His research interests include wireless networking and security, mobile computing, ubiquitous computing and smart



Xuemin (Sherman) Shen received the B.Sc. (1982) degree from Dalian Maritime University (China) and the M.Sc. (1987) and Ph.D. degrees (1990) from Rutgers University, New Jersey (USA), all in electrical engineering. He is a University Research Chair Professor, Department of Electrical and Computer Engineering, University of Waterloo, Canada. His research focuses on mobility and resource management in interconnected wireless/wired networks, UWB wireless communications networks, wireless network security, wireless body area networks and vehicular ad hoc and sensor networks. He is a co-author of three books, and has published more than 400 papers and book chapters in wireless communications and networks, control and filtering. He serves as the Tutorial Chair for IEEE ICC'08, the Technical Program Committee Chair for IEEE Globecom'07, the General Co-Chair for Chinacom'07 and QShine'06, the Founding Chair for IEEE Communications Society Technical Committee on P2P Communications and Networking. He also serves as a Founding Area Editor for IEEE Transactions

on Wireless Communications; Editor-in-Chief for Peer-to-Peer Networking and Application; Associate Editor for IEEE Transactions on Vehicular Technology; KICS/IEEE Journal of Communications and Networks, Computer Networks; ACM/Wireless Networks; and Wireless Communications and Mobile Computing (Wiley), etc. He has also served as Guest Editor for IEEE JSAC, IEEE Wireless Communications, IEEE Communications Magazine, and ACM Mobile Networks and Applications, etc. He received the

Excellent Graduate Supervision Award in 2006, and the Outstanding Performance Award in 2004 and 2008 from the University of Waterloo, the Premier's Research Excellence Award (PREA) in 2003 from the Province of Ontario, Canada, and the Distinguished Performance Award in 2002 and 2007 from the Faculty of Engineering, University of Waterloo. He is a registered Professional Engineer of Ontario, Canada. He is the fellow of IEEE.