This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2017.2752239, IEEE Internet of Things Journal

Efficiently and Completely Identifying Missing Key Tags for Anonymous RFID Systems

Honglong Chen, *Member, IEEE*, Zhibo Wang, *Member, IEEE*,
Feng Xia, *Senior Member, IEEE*, Yanjun Li, and Leyi Shi

***Abstract*—RFID systems can be applied to efficiently identify the missing items by attaching them with tags. Prior missing tag identification protocols concentrated on identifying all of the tags. However, there may be some scenarios in which we just care about the *key tags* instead of all tags, making it inefficient to merely identify the missing key tags due to the interference of replies from the *ordinary tags* (i.e., non-key tags). In this paper, we propose to investigate the problem of efficiently and completely identifying the missing key tags for anonymous RFID systems in which the tag privacy is required to be well protected. Firstly we propose a VEctor-based missing Key tag Identification protocol called VEKI. Then we propose an improved protocol called iVEKI, which consists of two phases: ordinary tag deactivation and missing key tag identification. The parameters of the proposed VEKI and iVEKI protocols are theoretically optimized to maximize the time efficiency. Finally we conduct extensive simulations to evaluate the proposed VEKI and iVEKI protocols and the simulation results illustrate that they outperform other existing protocols in terms of execution time.**

***Index Terms*—Anonymous RFID systems, efficiently and completely, missing key tag identification, parameter optimization**

I. Introduction

With the recent rapid development of wireless sensor networks [3], [27]–[29] and Internet of things [35], [36], radio frequency identification (RFID) has been an emerging technology with wide industrial applications such as localization [5], object tracking [8], warehouse management [26] and supply chain management [7], etc. A large-scale RFID system always consists of a back-end server, multiple readers and thousands of low-cost tags [20]. According to whether they are within the readers' interrogating regions or not, the tags can be classified into *present tags* and *missing tags* [6]. RFID systems can be applied to identify the missing items by using readers to identify the tags attached on the items. A recent report [25] illustrated that the U.S. retail industry lost about 42 billion dollars in 2013 due to shrink, including shoplifting, employee or supplier fraud and administrative errors. Therefore, missing tag identification becomes severely significant and has attracted much attention from the research community.

Most of prior missing tag identification protocols concentrated on identifying all the tags of the system. However, there may be some scenarios in which we only care about the *key tags* [16] instead of all tags. For instance, in a large shopping mall, there are some expensive items such as jewelries and watches and the tags attached on them are considered as the key tags, while the tags attached to the other relatively cheap items are considered as the ordinary tags. In some situations, the clerk may just want to monitor the expensive items (or a particular set of items), which can be actualized by identifying the missing key tags. However, it is inefficient to adopt the prior protocols in identifying the missing key tags for the RFID system since the *ordinary tags*, i.e., non-key tags, (with a larger population) will also reply to the reader's query and interfere with the missing key tag identification.

A potential solution for the missing key tag identification in RFID systems is to query the ID of each key tag and the one with no reply can be identified as missing. However, in this paper, we consider an anonymous RFID system, in which the tag ID should not be directly transmitted in the air to preserve the privacy [30]. Take the shopping mall for an example again, the key tag ID should be well protected since it would be risky to make the tag ID corresponding to some expensive item publicly known. The potential attackers may make use of this information to intrude into the system, such as launching a cloning attack [2]. Another example of the anonymous RFID system is a package of medicine purchased by someone from Amazon, since the package information may be closely related to the customer's privacy [14], the tag ID affixed on it should be well protected to keep private. Therefore, the ID-query protocol is inapplicable for the anonymous RFID system.

In this paper, we concentrate on efficiently and completely identifying the missing key tags for anonymous RFID systems. There are two major challenges: 1) Identification efficiency: how to improve the time efficiency of the missing key tag identification procedure with much more ordinary tags? 2) Anonymity guarantee: the tag privacy should be well protected during the identification procedure. A prior work called ETOP [19] was proposed to collect real-time information from a subset of tags in a large RFID system. However, ETOP intended to solve a different problem but not missing tag identification. Furthermore, ETOP cannot protect the tag privacy since in the poll phase the IDs of some tags will be broadcast by the reader. To the best of our knowledge, our work is the first to investigate the problem of missing key tag identification

Honglong Chen is with the College of Information and Control Engineering, China University of Petroleum, Qingdao, P. R. China. Email: chenhl@upc.edu.cn. Zhibo Wang is with the School of Computer, Wuhan University, Wuhan, P.R. China. Email: zbwang@whu.edu.cn. Feng Xia is with the School of Software, Dalian University of Technology, Dalian, P. R. China. Email: f.xia@ieee.org. Yanjun Li is with the College of Computer Science and Technology, Zhejiang University of Technology, Hangzhou, P. R. China. Email: yjli@zjut.edu.cn. Leyi Shi is with the College of Computer and Communication Engineering, China University of Petroleum, Qingdao, P. R. China. Email: shileyi@upc.edu.cn.

Corresponding author: Zhibo Wang.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2017.2752239, IEEE Internet of Things Journal

for anonymous RFID systems. We adopt the framed slotted Aloha [9] due to its high efficiency as the fundamental in the missing key tag identification. We firstly propose a vector-based missing key tag identification protocol called VEKI. In VEKI protocol, the reader constructs and broadcasts a vector indicating the status of each slot to simultaneously identify the missing key tags and deactivate the ordinary tags without revealing the tag privacy. To further improve the time efficiency, we propose the iVEKI protocol, consisting of the ordinary tag deactivation phase and the missing key tag identification phase. The parameters of the proposed VEKI and iVEKI protocols are theoretically optimized to maximize the time efficiency, i.e, to minimize the execution time.

The main contributions of this paper are summarized as follows:

- We make the first effort to investigate the problem of efficiently and completely identifying the missing key tags for anonymous RFID systems;
- We firstly propose a vector-based missing key tag identification protocol called VEKI, which simultaneously identifies the missing key tags and deactivates the ordinary tags without revealing the tag privacy;
- We then propose the iVEKI protocol to further improve the time efficiency, which consists of the ordinary tag deactivation phase and the missing key tag identification phase;
- We conduct extensive simulations to validate the effectiveness of our proposed VEKI and iVEKI protocols.

The rest of this paper is organized as follows. Section II discusses the prior missing tag identification protocols and anonymous RFID systems. Section III defines the system model. Section IV proposes the vector-based missing key tag identification protocol (VEKI). Section V proposes the iVEKI protocol. Section VI conducts the performance evaluation. Section VII concludes this paper and puts forward the future work.

II. Related Work

RFID technology has been widely adopted in many industrial applications [4], [11], [18], [31], one of which is missing tag identification, i.e., to identify whether a tag is present or not. Furthermore, in those applications, protection of the tag privacy has been paid more and more attention, making the anonymous characteristic severely important for the RFID systems. There have been lots of research works [1], [10], [14], [16], [21], [32] on missing tag identification and anonymous RFID systems in recent years. In this section, we will conduct the literature review on these two research directions.

Missing tag identification: In terms of missing tag problems, there are two categories of detection protocols, i.e., probabilistic and deterministic [17], [22]. Probabilistic missing tag detection protocols [17], [22], [26] concentrate on detecting the missing-tag event without identifying the missing tag's ID. While the deterministic missing tag detection protocols need to identify the IDs of missing tags. The deterministic protocols are also called missing tag identification, which can be used as a supplement once the missing-tag event is detected by the probabilistic protocols. Sheng *et al.* proposed DM in [24] to identify the missing tags using continuous scanning, which was done based on the previously gathered information. ProTaR [23] was proposed to efficiently identify the missing tags, which exploited a novel mask to promote the mitigation of the typical tag collision problem and leveraged a bit vector to achieve compact tag transmissions. Li *et al.* proposed the IIP [12], which tried to reduce the ratio of collision slots during the missing tag identification to achieve a high efficiency. MTI [33] was a missing tag identification protocol instructed by a back-end server to conduct multiple synchronized scans within the readers' respective coverage zone. To improve the efficiency, SFMTI was proposed in [13] to reconcile some of the expected collision slots, which is useless for missing tag identification, into singleton slots.

Anonymous RFID systems: The sampling-based key tag tracking protocol (S-KT) [16] considered an anonymous RFID system, in which the RFID reader only knows the IDs of the key tags. S-KT focused on estimating the cardinality of the key tags using a singleton slot-based estimator. Note that S-KT intended to solve the problem of estimating the number of key tags in the RFID system, which is different with that of this paper. REB [14] proposed to estimate the tag cardinality when there existed commercially available blocker tags in the system, which are RFID devices pre-configured with a set of genuine tag IDs to protect their ID privacy. GREAT [1] investigated the cloning attack detection problem in an anonymous RFID system by reframing the collision slots into singleton and empty ones. DeClone [2] proposed a deterministic detection of cloning attacks for anonymous RFID systems by using a tree traversal method. Note that GREAT and DeClone considered the scenario that the reader did not know the tags' IDs in advance. However, in the anonymous RFID system considered in this paper, we assume the reader knows the tag IDs but should protect the tags' ID privacy.

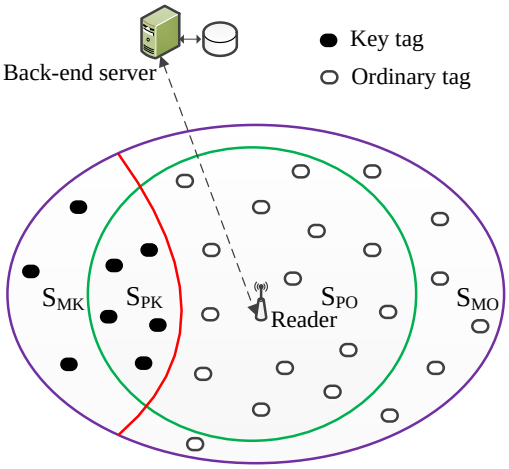
Although either the missing tag identification or the anonymous RFID systems have been well studied recently, there is no prior research work on solving the missing key tag identification problem for anonymous RFID systems. In this paper, we concentrate on investigating this problem and propose the VEKI and iVEKI protocols, the performance evaluation of which illustrates the importance of our study.

III. System Model

A. Network Model

In this paper, we consider an RFID system, which consists of a back-end server, an RFID reader and N tags. The RFID reader and the back-end server can communicate with each other via a high data rate link. Therefore, hereinafter we will use "reader" to represent them as an integral part. Each tag has a unique 96-bit ID according to the EPC C1G2 standard [9], which is known by the reader. Also, each tag has been equipped with the same uniform hash function $\mathcal{H}(\cdot)$. The N tags consist of $|S_K|$ key tags and $|S_O|$ ordinary tags, where S_K and S_O represent the set of key tags and the set of ordinary tags in the system, respectively. The key tags may be attached on some expensive items such as jewelries or watches, while the

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2017.2752239, IEEE Internet of Things Journal



S_{MK}: Set of missing key tags S_{PO}: Set of present ordinary tags

S_{PK}: Set of present key tags S_{MO}: Set of missing ordinary tags

Fig. 1. Illustration of the missing key tag identification scenario.

ordinary tags can be attached on relatively cheap items. Note that some of the key tags may be transformed into ordinary tags, and vice versa. In the RFID system, the key tags can be distinguished from the ordinary tags using different ways. For example, the reader can maintain this information and consequently it knows whether a tag is a key tag or ordinary tag. Another way is to assign different category IDs to the key tags and ordinary tags respectively, i.e., all the key tags share a category ID and the ordinary tags share the other category ID. As shown in Fig. 1, some of the key tags may be out of the reader's interrogating range, which are called missing key tags and denoted as S_{MK}. The set of key tags that are within the reader's interrogating range are called present key tags and denoted as S_{PK}. Similarly, we denote S_{MO} and S_{PO} as the set of missing ordinary tags and the set of present ordinary tags, respectively. Hence, $|S_K| = |S_{MK}| + |S_{PK}|$, $|S_O| = |S_{MO}| + |S_{PO}|$, and $N = |S_K| + |S_O|$. Hereinafter, for ease of presentation, we also use K and O to denote $|S_K|$ and $|S_O|$, respectively. In this paper we only consider the single-reader scenario and our proposed protocols can be easily extended to work in multi-reader scenario with logical OR operations.

The *framed slotted Aloha* protocol [9] can be used in the communications between the reader and tags for collision avoidance as follows. When the reader intends to collect information of a set of tags, it conducts a series of frames, each of which consists of multiple time slots. For each frame, the reader queries the tags by broadcasting parameters $\langle f, R \rangle$, where f is the frame size and R is a random seed. Then each tag picks a slot with an index of $\mathcal{H}(ID, R)$ mod f to reply, where $\mathcal{H}(\cdot)$ is a hash function deployed by the reader and tags in advance, ID is the tag's identity.

The reader can classify each slot into one of three types: *empty slot* with no tag reply, *singleton slot* with exact one tag reply and *collision slot* with multiple tag replies. Furthermore, we use *non-empty slots* to represent the union of the singleton slots and the collision slots, and use *non-singleton slots* to represent the union of empty slots and the collision slots. If we just need to distinguish a non-empty slot from empty ones, the tag can just reply a one-bit response [12], [21], [22], after which the reader can determine whether the slot is empty or not by detecting whether there is an idle carrier or a busy carrier within this slot. While to verify a singleton slot, a multi-bit response is necessary. To this end, the slots can also be classified based on their lengths into the following three types: *tag slot* (the slot to transmit a 96-bit ID), *long-response slot* (the slot to transmit a long-response with multi-bit information) and *short-response slot* (the slot to transmit a short-response with one-bit information), respectively. We denote t_{tag}, t_l and t_s as the length of a tag slot, a long-response slot and a short-response slot, respectively. For simplicity, in this paper we set $t_{tag} = 2.4\ ms$, $t_l = 0.8\ ms$ and $t_s = 0.4\ ms$, respectively [**?**], [17], [33]. In this paper, we adopt the segmentation technique [5], [6], [15] to improve the efficiency. In the segmentation technique, the slot-status information of a frame can be divided into multiple segments, each of which consists of 96 bits and can be transmitted within t_{tag}.

B. Attack Model

An anonymous RFID system [16] is considered in this paper, in which there is an attacker attempting to reveal the tag privacy. Here the tag privacy includes both the following two elements [4]:

- *Tag ID privacy:* it refers to the 96-bit ID of each tag. To protect the tag ID privacy effectively, the ID of each tag can not be transmitted directly in the air.
- *Category ID privacy:* it refers to the first s binary bits of each tag's ID, which can be regarded as its category ID ($1 < s < 96$). To protect the category ID privacy effectively, the reader can not select a specific category of tags by directly sending a *Select* command with the corresponding category ID.

The tag privacy protection is very important. For example, after eavesdropping the tag ID, the attacker can launch a cloning attack [2], which can behave the same with the tag. Consequently, even if a cloned tag is missing, it will not be successfully identified due to the cloning attack's reply to the reader. Therefore, in the considered anonymous RFID system, the reader can neither query each key tag directly nor select only the key tags for further identification. Hence, it motivates us to propose the efficient and complete missing key tag identification protocols without revealing the tag privacy in this paper.

C. Problem Statement

Since the key tags may be attached on some expensive items, sometimes the identification of missing key tags should be paid much more attention to avoid capital loss. In this paper, we concentrate on efficiently and completely identifying the missing key tags for anonymous RFID systems. As the missing key tag identification will be performed periodically, it is necessary to achieve a high identification efficiency, i.e.,

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2017.2752239, IEEE Internet of Things Journal

to identify the missing key tags as soon as possible, especially for the large-scale RFID systems [17]. As shown in Fig. 1, the problem can be summarized as: *to minimize the execution time of completely identifying the tags in S_{MK} for an RFID system without revealing the tag privacy given that S_K and S_O are known by the reader.*

IV. Vector-Based Missing Key Tag Identification Protocol

In this section, we propose the vector-based missing key tag identification protocol called VEKI to efficiently and completely identify the missing key tags without revealing the tag privacy. We firstly present the protocol description of the VEKI. After that we discuss the parameter settings to minimize the execution time.

A. Protocol Description of VEKI

When the reader conducts missing key tag identification, the present ordinary tags will also respond to the reader, which will interfere with the missing key tag identification procedure and make it inefficient. Therefore, a potential solution is to deactivate the present ordinary tags during the missing key tag identification. The idea behind the VEKI protocol is to construct a vector indicating the status of each slot and broadcast this vector for each tag to determine how to respond.

The VEKI protocol consists of multiple rounds. Here we denote r as the number of rounds and the determination of r will be discussed in next subsection. At the beginning of an arbitrary round i, the reader broadcasts parameters $\langle f_i, R\rangle$, where f_i is the frame size and R is a random seed which is fresh in each round. After receiving the parameters, each tag determines which slot to reply by calculating $\mathcal{H}(ID, R)$ mod f_i. Meanwhile, the reader can estimate the status of each slot in the current frame since it knows the IDs of all the tags, including both the key and ordinary ones. Then the reader constructs a $2f_i$-bit vector, denoted as V_i, which consists of f_i slot indicators. Each slot indicator consists of two bits and its value depends on the expected status of the associated slot. Specifically, the relationship between the value of each slot indicator in V_i and the status of its associated slot is described follows:

- '00': if the associated slot is expected to be empty;
- '01': if the associated slot is expected to be singleton and is only selected by one key tag;
- '10': if the associated slot is expected to be non-empty and is only selected by ordinary tag(s);
- '11': if the associated slot is expected to be collision and is selected by at least one key tag.

The reader needs to broadcast the vector V_i to the tags. If $2f_i > 96$, the reader divides V_i into $\lceil \frac{2f_i}{96} \rceil$ segments as done in [12], [13], [34], each of which is denoted as VS_i^j ($0 \le j \le \lceil \frac{2f_i}{96} \rceil - 1$). Therefore, each segment can be transmitted within a tag slot, i.e., t_{tag}. Then the reader sequentially broadcasts each of the segments. Each tag can map its ID to the associated slot indicator and segment. Since each tag knows its replying slot index, assumed as c ($0 \le c \le f_i - 1$), it can determine that the associated slot indicator lies in segment VS_i^k with bit index $c - 96k$ and $c + 1 - 96k$, where $k = \lfloor \frac{2c}{96} \rfloor$. Each tag just needs to receive one segment, which it is mapping to. After receiving its mapping segment, each tag can get its associated slot indicator. There are three different cases for each tag with the received slot indicator:

- Case 1: the received slot indicator is '01', indicating that the tag is a key tag and it is the only one selecting the associated slot;
- Case 2: the received slot indicator is '10', indicating that the tag is an ordinary tag;
- Case 3: the received slot indicator is '11', indicating that the tag may be either a key tag or an ordinary one.

Note that no tag will receive its slot indicator as '00', which indicates an empty slot, since the associated slot is selected by at least one receiving tag and cannot be empty. After broadcasting each segment VS_i^j, the reader will execute a sub-frame j with the number of slots equal to the number of slot indicators with value of '01'. Therefore, in each sub-frame, only the tags in Case 1 mapping to this sub-frame, i.e., the key tags, each of which selects a singleton slot in this sub-frame, will reply. Furthermore, each of the replying tags determines its replying slot by calculating the number of slot indicators with value of '01' preceding its associated slot indicator in the corresponding segment. And in each replying slot, the associated tag will reply a one-bit message for the reader to identify its presence. Therefore, if the slot is non-empty, the associated tag is present; otherwise, the associated tag is missing because there is no reply in this slot. By detecting the status of each slot in each sub-frame, the reader can determine whether the associated key tag is missing or not. As soon as each present key tag replies in its associated slot, it will deactivate itself in the following rounds since its presence has already been identified.

For the tags in Case 2, they can determine that they are ordinary tags and deactivate themselves immediately after receiving the associated slot indicators. Note that although some of the tags in Case 2 may be missing ordinary ones, the reader does not need to differentiate them from the present ordinary tags. And during the following rounds, all the tags in Case 2 (including both the present and missing ones) will be excluded when calculating the value of each slot indicator.

For the tags in Case 3, it is difficult for the reader to verify the presence of the key tags, since there are also some ordinary tags selecting this slot. Therefore, all the tags in Case 3 just keep silent in the current round and continue to participate in the identification of next round.

We denote K_i and O_i as the expected number of key tags and ordinary tags, which have not been verified by the reader before round i. Thus, $K_1 = K$ and $O_1 = O$. Also, we denote K_i^* as the expected number of newly verified key tags (either present or missing) in round i and denote O_i^* as the expected number of deactivated ordinary tags in round i. Therefore, $K_i = K_{i-1} - K_{i-1}^*$ and $O_i = O_{i-1} - O_{i-1}^*$. Accordingly, in round i, only $K_i + O_i$ tags participate in the missing key tag identification procedure. The missing key tag identification procedure will be conducted round by round until all the r rounds have been finished.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2017.2752239, IEEE Internet of Things Journal

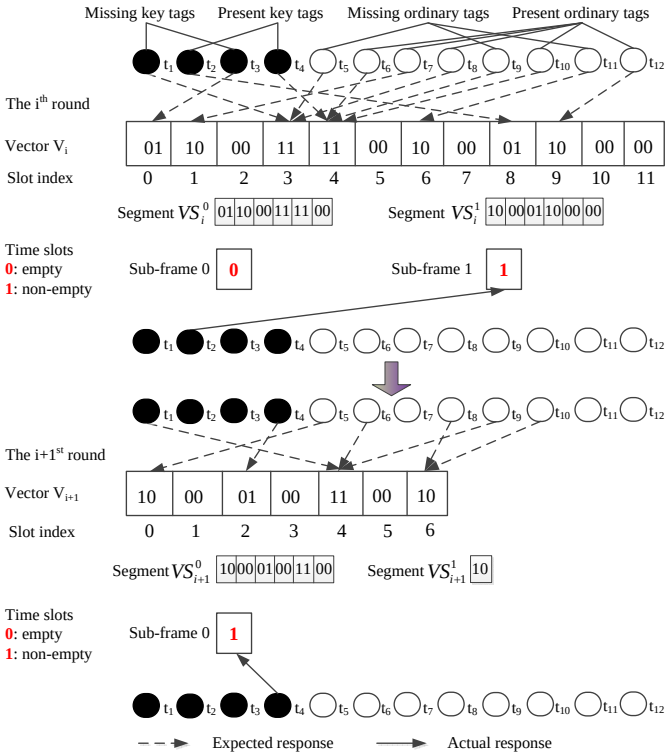


Fig. 2. Illustration of the missing key tag identification procedure of the VEKI protocol.

Example: As shown in Fig. 2, before round i, $S_{MK} = \{t_1, t_3\}$, $S_{PK} = \{t_2, t_4\}$, $S_{MO} = \{t_5, t_9, t_{11}\}$ and $S_{PO} = \{t_6, t_7, t_8, t_{10}, t_{12}\}$. After the reader broadcasting the parameters, it can construct the vector V_i, which can be divided into segment VS_i^0 and VS_i^1. As there is only one slot indicator with value of '01' in VS_i^0, the associated slot of which is selected by t_3, the sub-frame 0 only consists of one slot. t_3 can be identified as a missing key tag when the reader detects no response in the slot. Similarly, t_2 can be identified as a present key tag, which will deactivate itself in the following rounds. Since t_7, t_{11} and t_{12} select the slots with slot indicator value of '10', they also deactivate themselves in the following rounds. Consequently, there are only 7 tags participating in round $i+1$. Similarly, in round $i+1$, t_4 can be identified as a present key tag, which will deactivate itself in the following rounds. And t_5, t_8 and t_{10} can be deactivated and excluded in the following rounds.

In this paper, we define that the tag privacy is well protected if the tag privacy cannot be directly obtained or be inferred. Then we can get the following Theorem.

Theorem 1. *The proposed VEKI protocol can well protect the tag privacy.*

Proof: In the VEKI protocol, the tag ID and category ID have not been directly transmitted during the missing key tag identification procedure. Also, since each tag uses the hash function to calculate its reply slot index, its tag ID and category ID cannot be inferred even if its reply is overheard. Thus the tag privacy cannot be directly obtained or be inferred and we can claim that the tag privacy is well protected. ■

B. Parameter Determination

After presenting the VEKI protocol, we need to determine the parameters, including the frame size f_i and number of rounds r, to maximize the missing key tag identification efficiency.

We denote T_i as the execution time of round i in the VEKI protocol. Obviously, T_i consists of three parts: the time to broadcast the parameters, to broadcast the segments and to execute the sub-frames. The parameters can be broadcasted within one tag slot, i.e., t_{tag}. Since in round i, the reader constructs a $2f_i$-bit vector V_i, which can be divided into $\lceil \frac{2f_i}{96} \rceil$ segments, it needs $\lceil \frac{2f_i}{96} \rceil \cdot t_{tag}$ to broadcast them. As shown in Fig. 2, the number of slots in all of the sub-frames in round i equals the number of key tags mapping to the singleton slots, i.e., K_i^*. Here K_i^* represents the expected number of newly verified key tags in round i. Therefore, the time to execute the sub-frames in round i is $K_i^* \cdot t_s$. Consequently, we can obtain:

$$T_i = (\lceil \frac{2f_i}{96} \rceil + 1) \times t_{tag} + K_i^* \times t_s. \tag{1}$$

Recall that there are $K_i + O_i$ tags participating in round i. The probability that a key tag selects a singleton slot equals the probability that the selected slot is not selected by any other $K_i + O_i - 1$ tags. Thus, we can get:

$$K_i^* = \binom{K_i}{1} \times \frac{1}{f_i} \times (1 - \frac{1}{f_i})^{K_i + O_i - 1} \times f_i \approx K_i \times e^{-\frac{K_i + O_i - 1}{f_i}} \approx K_i \times e^{-\frac{K_i + O_i}{f_i}}. \tag{2}$$

Theorem 2. *The average time to verify per key tag in round i of the VEKI protocol can be minimized when $f_i = K_i + O_i$.*

Proof: Combining Eqs. (1) and (2), we can get the average time to verify per key tag in round i as:

$$\frac{T_i}{K_i^*} = \frac{(\lceil \frac{2f_i}{96} \rceil + 1) \times t_{tag} + K_i^* \times t_s}{K_i \times e^{-\frac{K_i + O_i}{f_i}}} \approx \frac{\frac{f_i}{48} \times t_{tag}}{K_i \times e^{-\frac{K_i + O_i}{f_i}}} + t_s.$$

Therefore, our objective is to minimize $\frac{T_i}{K_i^*}$. The partial derivative of $\frac{T_i}{K_i^*}$ with respect to f_i is:

$$\frac{\partial \frac{T_i}{K_i^*}}{\partial f_i} = \frac{\frac{t_{tag}}{48} \times (1 - \frac{K_i + O_i}{f_i})}{K_i \times e^{-\frac{K_i + O_i}{f_i}}}.$$

Let $\frac{\partial \frac{T_i}{K_i^*}}{\partial f_i} = 0$, we can get $f_i = K_i + O_i$. When $f_i < K_i + O_i$, $\frac{\partial \frac{T_i}{K_i^*}}{\partial f_i} < 0$, and when $f_i > K_i + O_i$, $\frac{\partial \frac{T_i}{K_i^*}}{\partial f_i} > 0$. Thus, we can minimize the average time to verify per key tag by setting $f_i = K_i + O_i$. ■

Then we need to calculate K_i and O_i respectively to determine f_i. As we mentioned, $K_i = K_{i-1} - K_{i-1}^*$. Based on Eq. (2), we can obtain:

$$\begin{aligned} K_i &= K_{i-1} - K_{i-1}^* = K_{i-1} - K_{i-1} \times e^{-\frac{K_{i-1} + O_{i-1}}{f_{i-1}}} = K_{i-1} \times (1 - e^{-1}) \\ &= K_1 \times (1 - e^{-1})^{i-1} = K \times (1 - e^{-1})^{i-1}. \end{aligned} \tag{3}$$

On the other hand, the probability that an ordinary tag is deactivated equals the probability that it selects a slot, which

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2017.2752239, IEEE Internet of Things Journal

is not selected by any key tag (but may be selected by other ordinary tags). Thus, we can get:

$$O_i^* = \binom{O_i}{1} \times \frac{1}{f_i} \times (1 - \frac{1}{f_i})^{K_i} \times f_i \approx O_i \times e^{-\frac{K_i}{K_i + O_i}}.$$

Similarly, as we mentioned that $O_i = O_{i-1} - O_{i-1}^*$, we can obtain:

$$O_i = O_{i-1} \times (1 - e^{-\frac{K_{i-1}}{K_{i-1}+O_{i-1}}}). \quad (4)$$

By combining Eqs. (3) and (4), we can iteratively calculate the frame size f_i based on $K_1 = K$, $O_1 = O$ and $f_i = K_i + O_i$.

To estimate the number of rounds r, we need to determine when can the reader verify all the key tags. We denote ϵ as a positive real number. Let $K_r = \epsilon$, indicating that before round r, the expected number of key tags which have not been verified is ϵ. Therefore, after r rounds, the reader tends to verify all the key tags if ϵ is small enough. We can get:

$$K \times (1 - e^{-1})^{r-1} = \epsilon \Rightarrow r \geq \frac{\ln \frac{\epsilon}{K}}{\ln(1 - e^{-1})} + 1. \quad (5)$$

Note that the reader knows the IDs of all the tags, it can acquire the information that how many key tags are verified in each round. Therefore, the reader can terminate the missing key tag identification procedure as soon as all the key tags have been verified. Here we provide Eq. (5) to estimate the number of rounds.

V. Improved Vector-Based Missing Key Tag Identification Protocol

In the proposed VEKI protocol, some of the ordinary tags are deactivated simultaneously when verifying the presence of the key tags. According to the parameter optimization, the frame size $f_i = K_i + O_i$, indicating that the participation of ordinary tags greatly decreases the efficiency, especially when O is much larger than K. Therefore, one of the directions to improve the efficiency is separating the ordinary tag deactivation and missing key tag identification into two independent phases, which motivates us to propose the iVEKI protocol.

In this section, we propose the improved vector-based missing key tag identification protocol for the anonymous RFID systems called iVEKI to enhance the efficiency, which consists of the ordinary tag deactivation phase and the missing key tag identification phase. In the first phase, the reader deactivates all the ordinary tags in the system to prohibit their interference on the missing key tag identification. And in the second phase, the reader verifies the presence of each key tag. We firstly present the protocol description of iVEKI. After that we propose to maximize the efficiency via parameter optimization.

A. Protocol Description of iVEKI

1) Ordinary Tag Deactivation Phase: To deactivate the ordinary tags, the reader can broadcast a specific message for each tag to decide whether or not to deactivate itself. The ordinary tag deactivation phase consists of r_1 rounds. At the beginning of each round i, the reader broadcasts parameter $\langle f_i', R \rangle$, where f_i' is the frame size and R is the random seed. Each tag selects a slot to reply after receiving the parameters. The reader can also estimate the status of each slot in the current frame since it knows the IDs of the known tags, including both the key and ordinary tags. Then the reader constructs an f_i'-bit ordinary tag deactivation vector, denoted as OV_i. Each bit in OV_i is set as '0' if its associated slot is selected by only ordinary tag(s), and is set as '1' otherwise. When $f_i' > 96$, the reader divides OV_i into $\lceil \frac{f_i'}{96} \rceil$ segments and sequentially broadcasts them, each of which can be conducted within a tag slot. After receiving its associated segment, each tag can interprets it and check the value of its corresponding bit. If it is '0', the tag deactivates itself. Since the tag corresponding to a bit '0' is an ordinary tag, only some of the ordinary tags will deactivate in each round.

Note that the reader can easily calculate the number of deactivated ordinary tags and get the number of undeactivated ordinary tags after this round. The ordinary tag deactivation phase will be conducted until all the ordinary tags are deactivated. We will discuss the determination of f_i' and r_1 later.

2) Missing Key Tag Identification Phase: After the ordinary tag deactivation phase, there will be no ordinary tag participating in the missing key tag identification phase. Thus, the missing key tag identification problem becomes much simpler, in which there is no interference from ordinary tags.

The missing key tag identification phase consists of r_2 rounds. At the beginning of an arbitrary round i, the reader broadcasts parameters $\langle f_i, R \rangle$, where f_i is the frame size and R is the random seed. Here we also denote K_i as the expected number of unverified key tags before round i. Thus, only the K_i key tags participate in the current round. Each key tag selects a slot to reply after receiving the parameters. Furthermore, since the reader knows the set of key tags to participate in the current round, it can also estimate the status of each slot in the current frame. Then the reader constructs an f_i-bit key tag identification vector, denoted as KV_i. Each bit in KV_i is set as '1' if there its associated slot is expected to be singleton, i.e., only one key tag selects its associated slot, and '0' otherwise. If $f_i > 96$, the reader divides KV_i into $\lceil \frac{f_i}{96} \rceil$ segments, each of which is denoted as KVS_i^j $(0 \leq j \leq \lceil \frac{f_i}{96} \rceil - 1)$ as shown in Fig. 3 and can be transmitted within t_{tag}. The reader then sequentially broadcasts the segments, each of which is followed by a sub-frame. Each tag can map itself to one of the segments and determine whether or not to reply in the associated sub-frame. Only the tag whose corresponding bit is '1' will reply in its associated sub-frame. Therefore, the number of slots in each sub-frame equals the number of '1' in the corresponding segment. In each sub-frame, the reader detects whether there is a response in each slot to verify the corresponding key tag's presence. Each present key tag, which replies in its associated slot, can be identified as present and will deactivate itself in the following rounds. At the end of round i, the reader can identify some missing key tags together with some present key ones, which will be excluded in the following rounds. The missing key tag identification will be conducted until all the r_2 rounds have been finished.

Example: As shown in Fig. 3, assume all the ordinary tags have been deactivated in the ordinary tag deactivation phase and there is no ordinary tag participating in the missing key tag identification phase. Before round i in phase II of the iVEKI protocol, $S_{MK} = \{t_1, t_2, t_3, t_4\}$ and $S_{PK} = \{t_5, t_6, t_7, t_8, t_9, 5_{10}\}$.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2017.2752239, IEEE Internet of Things Journal

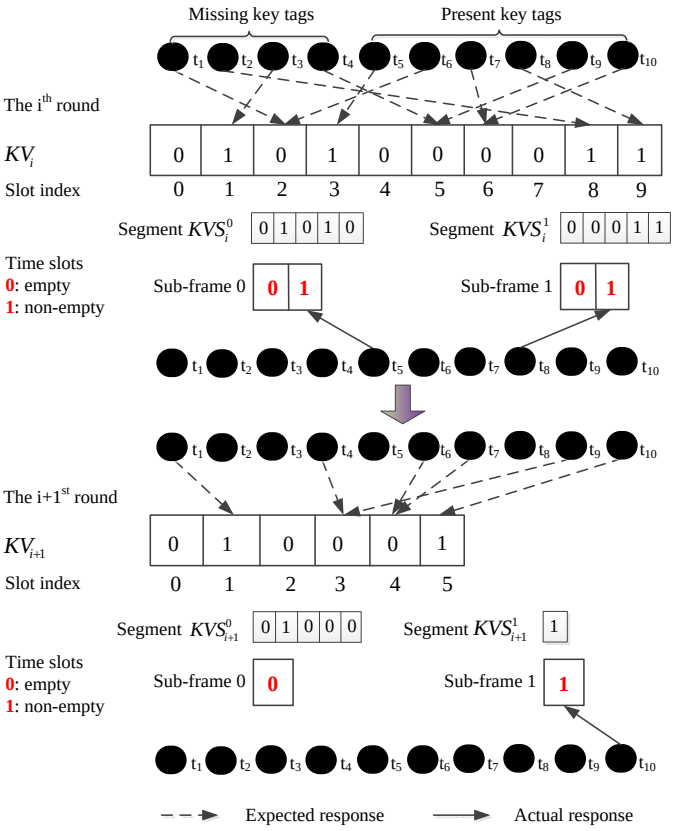


Fig. 3. Illustration of the missing key tag identification phase in the iVEKI protocol.

In round i, each of tags t_2, t_3, t_5 and t_8 selects an expected singleton slot. Therefore, t_2 and t_3 are identified as missing, and t_5 and t_8 are identified as present, which deactivate themselves. The above four tags are excluded in round $i+1$. At the end of round $i+1$, t_1 can be identified as missing and t_{10} can be identified as present. Both of the t_5 and t_8 will be deactivated and excluded in the following rounds.

Theorem 3. *The proposed iVEKI protocol can well protect the tag privacy.*

Proof: It is similar to that of the VEKI protocol shown in Theorem 1, we omit the proof here to save space. ■

B. Parameter Determination

In this section, we discuss how to determine f_i', r_1, f_i and r_2 to maximize the efficiency.

We denote T_i' as the execution time for round i in the ordinary tag deactivation phase. Since in round i, the reader uses t_{tag} to broadcast the parameters and $\lceil \frac{f_i'}{96} \rceil \cdot t_{tag}$ to broadcast the segments, we can obtain:

$$T_i' = (\lceil \frac{f_i'}{96} \rceil + 1) \times t_{tag}.$$

We denote O_i' as the expected number of undeactivated ordinary tags before round i and $O_i^{*\prime}$ as the expected number of deactivated ordinary tags in round i. Thus, $O_1' = O$. For an ordinary tag, the probability that it will be deactivated in round i equals the probability that it selects a slot which is not selected by any key tag, i.e., $\frac{1}{f_i'} \cdot (1 - \frac{1}{f_i'})^K \cdot f_i'$. Thus, we can obtain:

$$O_i^{*\prime} = \binom{O_i'}{1} \times \frac{1}{f_i'} \times (1 - \frac{1}{f_i'})^K \times f_i' \approx O_i' \times e^{-\frac{K}{f_i'}}. \quad (6)$$

Therefore, the average time to deactivate per ordinary tag in round i of the ordinary tag deactivation phase can be calculated as:

$$\frac{T_i'}{O_i^{*\prime}} = \frac{(\lceil \frac{f_i'}{96} \rceil + 1) \times t_{tag}}{O_i' \times e^{-\frac{K}{f_i'}}} \approx \frac{\frac{f_i'}{96} \times t_{tag}}{O_i' \times e^{-\frac{K}{f_i'}}}.$$

The objective in the ordinary tag deactivation phase is to minimize $\frac{T_i'}{O_i^{*\prime}}$. We can get the partial derivative of $\frac{T_i'}{O_i^{*\prime}}$ with respect to f_i' as:

$$\frac{\partial \frac{T_i'}{O_i^{*\prime}}}{\partial f_i'} = \frac{t_{tag}}{96 \times O_i' \times e^{-\frac{K}{f_i'}}} \times (1 - \frac{K}{f_i'}). \quad (7)$$

Then, let Eq. (7) equal 0 and we can get $f_i' = K$. Moreover, when $f_i' < K$, $\frac{\partial \frac{T_i'}{O_i^{*\prime}}}{\partial f_i'} < 0$ and when $f_i' > K$, $\frac{\partial \frac{T_i'}{O_i^{*\prime}}}{\partial f_i'} > 0$. Thus, the efficiency can be maximized when $f_i' = K$. It is observed that f_i' does not depend on the number of ordinary tags. Therefore, the execution time can be reduced by separating the ordinary tag deactivation and missing key tag identification into two phases, especially when $K << O$.

To estimate the number of rounds r_1, we need to calculate O_i'. We can get $O_i' = O_{i-1}' - O_{i-1}^{*\prime}$. Therefore, based on Eq. (6), we can obtain:

$$\begin{aligned} O_i' &= O_{i-1}' - O_{i-1}^{*\prime} = O_{i-1}' - O_{i-1}' \times e^{-\frac{K}{f_i'}} = O_{i-1}' \times (1 - e^{-1}) \\ &= O_1' \times (1 - e^{-1})^{i-1} = O \times (1 - e^{-1})^{i-1}. \end{aligned}$$

Similarly, We denote η as a small enough positive real number. Let $O_{r_1}' = \eta$, indicating that before round r_1, the expected number of undeactivated ordinary tags is η. Thus, we can estimate r_1 as:

$$O \times (1 - e^{-1})^{r_1 - 1} = \eta \Rightarrow r_1 = \lceil \frac{\ln \frac{\eta}{O}}{\ln(1 - e^{-1})} \rceil + 1.$$

As we mentioned, the reader knows the IDs of the ordinary tags, it can calculate the exact number of undeactivated ordinary tags after each round. Therefore, the reader can guarantee that all the ordinary tags are deactivated in the ordinary tag deactivation phase.

We denote T_i as the execution time in round i of the missing key tag identification phase. We also denote K_i and K_i^* as the expected number of unverified key tags before round i and the expected number of newly verified key tags in round i, respectively. Thus, $K_1 = K$. The reader uses t_{tag} to broadcast the parameters and $\lceil \frac{f_i}{96} \rceil \cdot t_{tag}$ to broadcast the segments. Furthermore, there are K_i^* slots in all the sub-frames in round i, indicating that the reader will consume $K_i^* \cdot t_s$. We can get:

$$T_i = (\lceil \frac{f_i}{96} \rceil + 1) \times t_{tag} + K_i^* \times t_s.$$

For an unverified key tag, it can be verified to be present or not only when its associated slot is not selected by any other tag since only the singleton slots are executed. Thus, the

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2017.2752239, IEEE Internet of Things Journal

probability that an unverified key tag will be verified in round i equals the probability that it selects a singleton slot. Then we can get:

$$K_i^* = \binom{K_i}{1} \times \frac{1}{f_i} \times (1-\frac{1}{f_i})^{K_i-1} \times f_i \approx K_i \times e^{-\frac{K_i-1}{f_i}} \approx K_i \times e^{-\frac{K_i}{f_i}}. \quad (8)$$

Then we can get the average time to verify per key tag in round i of the missing key tag identification phase as:

$$\frac{T_i}{K_i^*} = \frac{(\lceil \frac{f_i}{96} \rceil + 1) \times t_{tag} + K_i^* \times t_s}{K_i \times e^{-\frac{K_i}{f_i}}} \approx \frac{\frac{f_i}{96} \times t_{tag}}{K_i \times e^{-\frac{K_i}{f_i}}} + t_s.$$

The objective in the missing key tag identification phase is to minimize $\frac{T_i}{K_i^*}$. Let the partial derivative of $\frac{T_i}{K_i^*}$ with respect to f_i equal 0, i.e., $\frac{\partial \frac{T_i}{K_i^*}}{\partial f_i} = 0$. After that we can get $f_i = K_i$ (when $f_i < K_i$, $\frac{\partial \frac{T_i}{K_i^*}}{\partial f_i} < 0$, and when $f_i > K_i$, $\frac{\partial \frac{T_i}{K_i^*}}{\partial f_i} > 0$).

Based on Eq. (8), we can also obtain:

$$\begin{aligned} K_i &= K_{i-1} - K_{i-1}^* = K_{i-1} \times (1 - e^{-\frac{K_i}{f_i}}) = K_{i-1} \times (1 - e^{-1}) \\ &= K_1 \times (1 - e^{-1})^{i-1} = K \times (1 - e^{-1})^{i-1}. \end{aligned}$$

Let $K_{r_2} = 1$, indicating that there is only one unverified key tag before round r_2, then this unverified key tag can be verified in round r_2 since it is the only tag participating in the current round. Therefore, we can guarantee that all the key tags can be verified after r_2 rounds, i.e., all the missing key tags can be identified. Consequently, we can estimate r_2 as:

$$K \times (1 - e^{-1})^{r_2 - 1} = 1 \Rightarrow r_2 \geq \frac{\ln \frac{1}{K}}{\ln(1 - e^{-1})} + 1. \quad (9)$$

VI. Performance Evaluation

In this section, we evaluate the performance of the proposed VEKI and iVEKI protocols. We implemented the VEKI and iVEKI protocols in Matlab. Although there is no existing work studying the problem of the missing key tag identification for anonymous RFID system, we still implemented two of the prior works namely IIP [12] and SFMTI [13] for performance comparison since they can be used to identify all the missing tags (including both the key and ordinary tags). In the IIP [12] protocol, the reader tries to identify the missing tags by observing the slots changing from expected non-empty to actual empty, in which each tag mapping to a collision slot will decide to participate in the current frame with probability of 50% to improve the slot utilization. In the SFMTI [13] protocol, the reader can reconcile some of the expected collision slots by reassign additional slots at the end of current frame for the associated tags to improve efficiency. When an expected non-empty slot is detected to be empty, the tags mapping to this slot can then be identified as missing. We illustrate the effectiveness of our proposed VEKI and iVEKI protocols by comparing their performance with the IIP and SFMTI protocols.

A. Simulation Settings

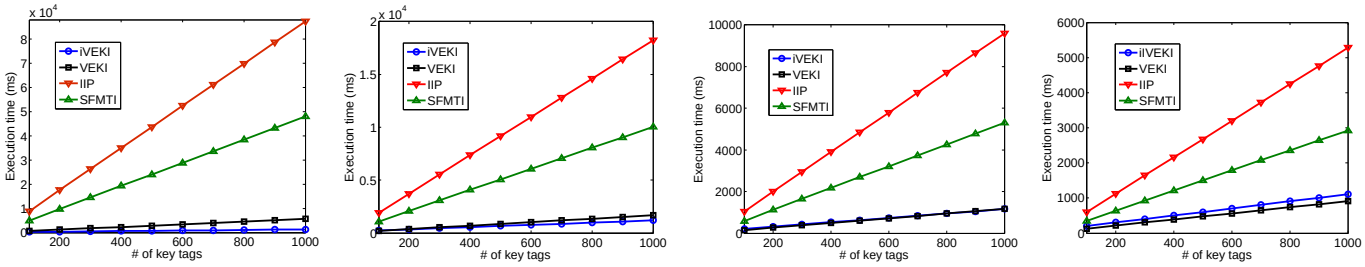
In the simulations, we consider an RFID system with a single reader. Note that our proposed VEKI and iVEKI protocols can also work in the multi-reader scenarios with simple logic OR operations. We assume that the communication link between the reader and tags is error-free and symmetric with the same transmission rate 62.5 Kbps [17], that is, $t_{tag} = 2.4\ ms$ and $t_s = 0.4\ ms$. We adopt $\eta = 0.01$ in the iVEKI protocol. For the scenario with non-error-free communication link, it can be solved by adding a cyclic-redundance check code in each transmitted segment as in [15], which, however, is out of consideration of this paper. Each simulation result is obtained by averaging 100 independent runs. Since all the missing key tags in the system can be successfully identified by the protocols, we adopt the execution time of the missing key tag identification procedure as the performance metric in the simulations in terms of milliseconds. Note that the execution time is calculated by counting the number of tag slots and the number of short-response slots required for the missing key tag identification procedure. Therefore, less execution time indicates higher missing key tag identification efficiency.

B. Performance Comparison

Fig. 4 shows the impacts of number of key tags on the performance of execution time of the proposed VEKI and iVEKI protocols and the existing ones with different value of K/O, i.e., when $K/O = 0.01$, $K/O = 0.05$, $K/O = 0.1$, and $K/O = 0.2$, respectively. Since the number of key tags is always smaller than that of ordinary tags in the practical applications, we only consider the scenarios that $K/O \leq 0.2$ in the simulations. The number of key tags is varied from 100 to 1000. And we set $|S_{MK}|/K = 0.1$ and $|S_{MO}|/O = 0.1$, i.e., 10% of the key tags and ordinary tags are missing, respectively. It illustrates that all the four protocols require more execution time with the increase of the number of key tags. The reason is that when the number of key tags increases, the number of ordinary tags will also increase, resulting in more known tags to verify. Obviously, the proposed VEKI and iVEKI protocols always outperform the other two protocols since the latter two protocols are designed to identify all the missing tags but not just the missing key tags. When $K/O = 0.01$ and $K/O = 0.05$, the iVEKI protocol consumes less execution time than that of the VEKI protocol. However, when $K/O = 0.1$, they consume similar execution time. And when $K/O = 0.2$, VEKI protocol performs better than iVEKI protocol, indicating that iVEKI protocol has advantage over VEKI protocol only when $K << O$, which validates our previous claim. The IIP protocol always consumes the most execution time.

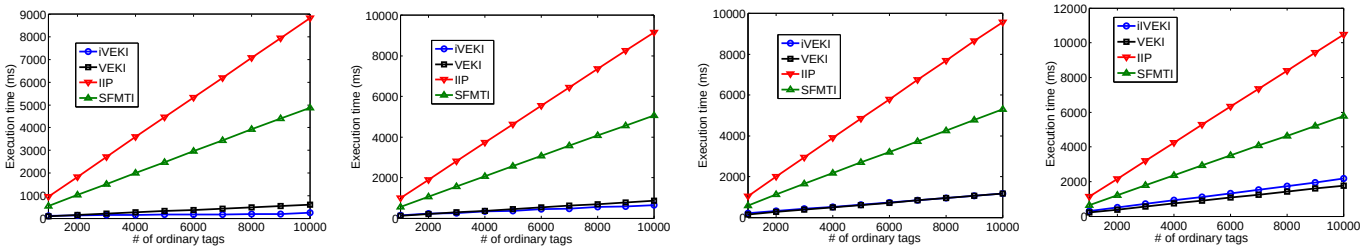
Fig. 5 shows the impacts of number of ordinary tags on the performance of execution time of the proposed VEKI and iVEKI protocols and the existing ones with different value of K/O, i.e., when $K/O = 0.01$, $K/O = 0.05$, $K/O = 0.1$, and $K/O = 0.2$ respectively. The number of ordinary tags is varied from 1000 to 10000. And we set $|S_{MK}|/K = 0.1$ and $|S_{MO}|/O = 0.1$. The results in Fig. 5 illustrate that when the number of ordinary tags increases, the execution time of all the four protocols will increase, since more ordinary tags

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2017.2752239, IEEE Internet of Things Journal



(a) $K/O = 0.01$ (b) $K/O = 0.05$ (c) $K/O = 0.1$ (d) $K/O = 0.2$

Fig. 4. Impacts of number of key tags on the performance of execution time with different value of K/O.



(a) $K/O = 0.01$ (b) $K/O = 0.05$ (c) $K/O = 0.1$ (d) $K/O = 0.2$

Fig. 5. Impacts of number of ordinary tags on the performance of execution time with different value of K/O.

indicates more known tags to verify. Also, the proposed VEKI and iVEKI protocols always outperform the other two existing ones. Similarly, the iVEKI protocol outperforms the VEKI protocol when $K/O = 0/01$ and $K/O = 0.05$. When $K/O = 0.1$, they consume similar execution time and when $K/O = 0.2$, VEKI protocol requires less execution time than that of iVEKI protocol. The IIP protocol always consumes the most execution time.

Fig. 6 illustrates the impacts of number of key tags on the performance of execution time of the proposed VEKI and iVEKI protocols and the existing ones when $O = 10000$ with different value of $|S_{MK}|/K$, i.e., when $|S_{MK}|/K = 0.1$, $|S_{MK}|/K = 0.5$ and $|S_{MK}|/K = 1$, respectively. The number of key tags is varied from 100 to 1000. And we set $|S_{MO}|/O = 0.1$. The results show that all the four protocols consume more execution time when the number of key tags increases. However, the growth rates of the execution time are much smaller than that in Fig. 4 since the number of ordinary tags here is fixed to be 10000. The proposed VEKI and iVEKI protocols outperform the other two existing protocols. And the iVEKI protocol consumes less execution time than the VEKI protocol. However, when the number of key tags increases to 1000, the iVEKI protocol perform almost the same with the VEKI protocol because $K/O = 0.1$ when $K = 1000$ ($O = 10000$). Furthermore, the value of $|S_{MK}|/K$ does not affect the execution time of all the four protocols since all the four protocols need to verify all the key tags no matter they are missing or not.

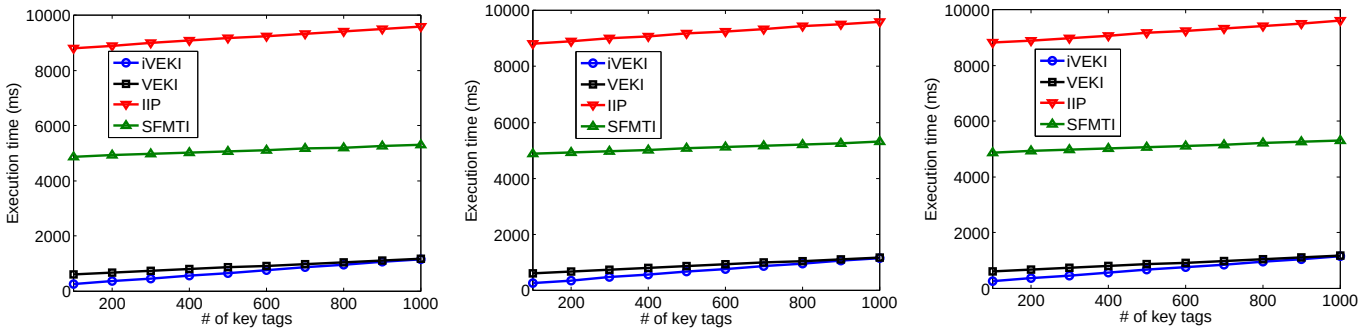
Fig. 7 shows the impacts of number of ordinary tags on the performance of execution time of the proposed VEKI and iVEKI protocols and the existing ones when $K = 100$ with different value of $|S_{MO}|/O$, i.e., when $|S_{MO}|/O = 0.1$, $|S_{MO}|/O = 0.5$ and $|S_{MO}|/O = 1$, respectively. The number of ordinary tags is varied from 1000 to 10000. And we set $|S_{MK}|/K = 0.1$. With the increase of number of ordinary tags, the execution time of all the four protocols will increase. The proposed VEKI and iVEKI protocols outperform the existing two protocols. And the iVEKI protocol performs the best. Also, the value of $|S_{MO}|/O$ does not affect the execution time of all the four protocols.

Summary: The proposed VEKI and iVEKI protocols perform much more efficiently than the IIP and SFMTI protocols, and the iVEKI protocol outperforms the VEKI protocol when $K/O \leq 0.1$. The execution time of the four protocols increases when the number of key tags or ordinary tags increases. However, $|S_{MK}|/K$ and $|S_{MO}|/O$ do not affect the execution time of the four protocols. Note that the IIP and SFMTI protocols are designed for missing tag identification, which is a different problem with ours in this paper. Nevertheless, via the performance evaluation, we can still claim that the simulation results illustrate the importance of our study since the proposed VEKI and iVEKI protocols can efficiently identify the missing key tags for the large-scale RFID systems.

VII. Conclusions and Future Work

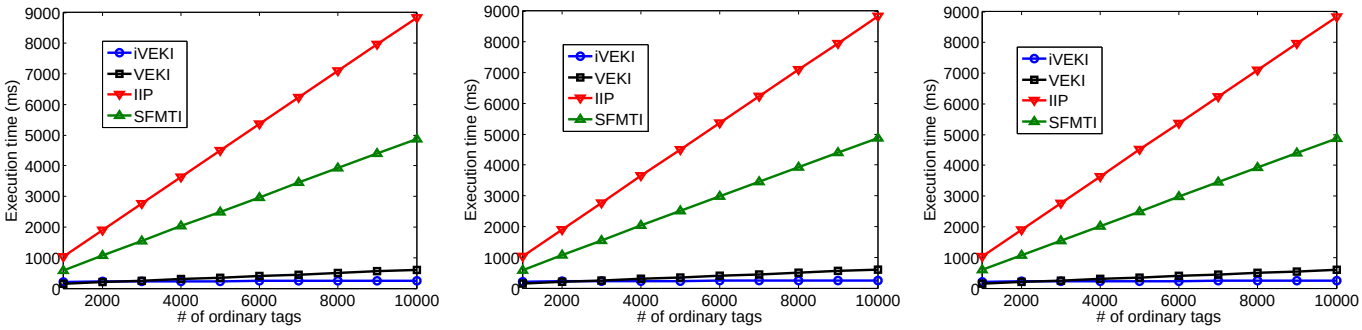
In this paper, we made the first effort to investigate the problem of efficient and complete missing key tag identification for the anonymous RFID systems. We firstly proposed a vector-based missing Key tag identification protocol called VEKI, in which the reader simultaneously identifies the missing key tags and deactivates the ordinary tags without revealing the tag privacy. We then proposed an improved protocol called iVEKI to further improve the efficiency, which consists of the ordinary tag deactivation phase and the missing key tag identification phase. We theoretically optimized the parameters of the proposed VEKI and iVEKI protocols to maximize the time efficiency. We finally conducted extensive simulations to

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2017.2752239, IEEE Internet of Things Journal



(a) $|S_{MK}|/K = 0.1$ (b) $|S_{MK}|/K = 0.5$ (c) $|S_{MK}|/K = 1$

Fig. 6. Impacts of number of key tags on the performance of execution time when $O = 10000$ with different value of $|S_{MK}|/K$.



(a) $|S_{MO}|/O = 0.1$ (b) $|S_{MO}|/O = 0.5$ (c) $|S_{MO}|/O = 1$

Fig. 7. Impacts of number of ordinary tags on the performance of execution time when $K = 100$ with different value of $|S_{MO}|/O$.

evaluate the VEKI and iVEKI protocols and the simulation results illustrate that they greatly outperform other existing protocols in terms of execution time.

This paper only considered the error-free communication link between the reader and tags, we intend to further investigate the non-error-free scenario for missing key tag identification as one of directions of the future work. Another direction in our future work is to consider the anonymous RFID system, in which the reader only knows the IDs of the key tags but not those of the ordinary tags.

Acknowledgement

This work was supported in part by NSFC grants (No.61772551, No.61502352, No.61572106, No.61772472), Qingdao Fundamental Research Project (No.15-9-1-79-jch), the Fundamental Research Funds for the Central Universities (No.16CX02059A, No.413000035), Natural Science Foundation of Hubei Province (No.2017CFB503), Natural Science Foundation of Jiangsu Province (No.BK20150383) and Natural Science Foundation of Zhejiang Province (No.LY17F020020).

References

[1] K. Bu, X. Liu, J. Luo, B. Xiao, and G. Wei, "Unreconciled Collisions Uncover Cloning Attacks in Anonymous RFID Systems," *IEEE Transactions on Information Forensics and Security*, vol. 8, pp. 429–439, 2013.

[2] K. Bu, M. Xu, X. Liu, J. Luo, S. Zhang, and M. Weng, "Deterministic Detection of Cloning Attacks for Anonymous RFID Systems," *IEEE Transactions on Industrial Informatics*, vol. 11, pp. 1255–1266, 2015.

[3] H. Chen and W. Lou, "On protecting end-to-end location privacy against local eavesdropper in Wireless Sensor Networks," *Elsevier Pervasive and Mobile Computing*, pp. 36–55, 2015.

[4] H. Chen, G. Ma, Z. Wang, F. Xia, and J. Yu, "Probabilistic Detection of Missing Tags for Anonymous Multi-Category RFID Systems," *IEEE Transactions on Vehicular Technology, DOI: 10.1109/TVT.2017.2726005*, 2017.

[5] H. Chen, G. Ma, Z. Wang, J. Yu, L. Shi, and X. Jiang, "Efficient 3-dimensional localization for RFID systems using jumping probe," *Pervasive and Mobile Computing, DOI: 10.1016/j.pmcj.2016.12.002*, 2016.

[6] H. Chen, G. Xue, and Z. Wang, "Efficient and Reliable Missing Tag Identification for Large-Scale RFID Systems with Unknown Tags," *IEEE Internet of Things Journal*, vol. 4, pp. 736–748, 2017.

[7] S. Chen, M. Zhang, and B. Xiao, "Efficient Information Collection Protocols for Sensor-Augmented RFID Networks," in *Proc. of IEEE INFOCOM*, 2011, pp. 3101–3109.

[8] W. Cheng, X. Cheng, M. Song, B. Chen, and W. W. Zhao, "On the Design and Deployment of RFID Assisted Navigation Systems for VANETs," *IEEE Transactions on Parallel and Distributed Systems*, vol. 23, pp. 1267–1274, 2012.

[9] EPCGlobal Inc., *Radio-Frequency Identity Protocols C1G2 UHF RFID Protocol for Communication at 860 MHz-960 MHz*, 2013.

[10] W. Gong, H. Liu, X. Miao, K. Liu, W. He, L. Zhang, and Y. Liu, "Fast and Adaptive Continuous Scanning in Large-Scale RFID Systems," *IEEE/ACM Transactions on Networking*, pp. 1–12, 2016.

[11] F. Guidi, N. Decarli, and S. Bartoletti, "Detection of Multiple Tags Based on Impulsive Backscattered Signals," *IEEE Transactions on Communications*, vol. 62, pp. 3918–3930, 2014.

[12] T. Li, S. Chen, and Y. Ling, "Identifying The Missing Tags in A Large RFID System," in *Proc. of ACM MOBIHOC*, 2010, pp. 1–10.

[13] X. Liu, K. Li, G. Min, Y. Shen, A. Liu, and W. Qu, "Completely Pinpointing The Missing RFID Tags in A Time-Efficient Way," *IEEE Transactions on Computers*, vol. 64, pp. 87–96, 2015.

[14] X. Liu, B. Xiao, K. Li, A. X. Liu, J. Wu, X. Xie, and H. Qi, "RFID Estimation with Blocker Tags," *IEEE/ACM Transactions on Networking*, 2016.

[15] X. Liu, B. Xiao, S. Zhang, and K. Bu, "Unknown Tag Identification

in Large RFID Systems: An Efficient and Complete Solution," *IEEE Transactions on Parallel and Distributed Systems*, vol. 26, pp. 1775–1788, 2015.

[16] X. Liu, X. Xie, K. Li, B. Xiao, J. Wu, H. Qi, and D. Lu, "Fast Tracking the Population of Key Tags in Large-scale Anonymous RFID Systems," *IEEE/ACM Transactions on Networking*, vol. 25, pp. 278–291, 2017.

[17] W. Luo, S. Chen, Y. Qiao, and T. Li, "Missing-Tag Detection and Energy-Time Tradeoff in Large-Scale RFID Systems With Unreliable Channels," *IEEE/ACM Transactions on Networking*, pp. 1079–1091, 2014.

[18] W. Luo, Y. Qiao, S. Chen, and M. Chen, "An Efficient Protocol for RFID Multigroup Threshold-Based Classification Based on Sampling and Logical Bitmap," *IEEE/ACM Transactions on Networking*, vol. 24, pp. 397–407, 2016.

[19] Y. Qiao, S. C. T. Li, and S. Chen, "Energy-efficient Polling Protocols in RFID Systems," in *Proc. of ACM MOBIHOC*, 2011, pp. 1–9.

[20] M. Roberti, "A 5-cent Breakthrough," *RFID Journal*, vol. 5, 2006.

[21] M. Shahzad and A. X. Liu, "Every Bit Counts - Fast and Scalable RFID Estimation," in *Proc. of ACM MOBICOM*, 2012, pp. 365–376.

[22] ——, "Expecting the Unexpected: Fast and Reliable Detection of Missing RFID Tags in the Wild," in *Proc. of IEEE INFOCOM*, 2015, pp. 1939–1947.

[23] C. Shao, T. Kim, J. Yu, J. Choi, and W. Lee, "ProTaR: Probabilistic Tag Retardation for Missing Tag Identification in Large-Scale RFID Systems," *IEEE Transactions on Industrial Informatics*, vol. 11, pp. 513–522, 2015.

[24] B. Sheng, Q. Li, and W. Mao, "Efficient Continuous Scanning in RFID Systems," in *Proc. of IEEE INFOCOM*, 2010, pp. 1–9.

[25] Study: Shrink costs U.S. retailers $42 billion; employee theft tops shoplifting, *http://www.chainstoreage.com/article/study-shrink-costs-us-retailers-42-billion-employee-theft-tops-shoplifting*.

[26] C. C. Tan, B. Sheng, and Q. Li, "Efficient Techniques for Monitoring Missing RFID Tags," *IEEE Transactions on Wireless Communications*, vol. 9, pp. 1882–1889, 2010.

[27] Z. Wang, Q. Cao, H. Qi, H. Chen, and Q. Wang, "Cost-Effective Barrier Coverage Formation in Heterogeneous Wireless Sensor Networks," *Elsevier Ad Hoc Networks*, vol. 64, pp. 65–79, 2017.

[28] Z. Wang, H. Chen, Q. Cao, H. Qi, Z. Wang, and Q. Wang, "Achieving Location Error Tolerant Barrier Coverage for Wireless Sensor Networks," *Elsevier Computer Networks*, vol. 112, pp. 314–328, 2017.

[29] Z. Wang, J. Liao, Q. Cao, H. Qi, and Z. Wang, "Achieving k-barrier Coverage in Hybrid Directional Sensor Networks," *IEEE Transactions on Mobile Computing*, vol. 13, pp. 1443–1455, 2014.

[30] Z. Xia, X. Wang, L. Zhang, Z. Qin, X. Sun, and K. Ren, "A Privacy-preserving and Copy-deterrence Content-based Image Retrieval Scheme in Cloud Computing," *IEEE Transactions on Information Forensics and Security*, vol. 11, pp. 2594–2608, 2016.

[31] L. Xie, H. Han, Q. Li, J. Wu, and S. Lu, "Efficiently Collecting Histograms Over RFID Tags," in *Proc. of IEEE INFOCOM*, 2014, pp. 145–153.

[32] L. Yang, Y. Chen, X.-Y. Li, C. Xiao, M. Li, and Y. Liu, "Tagoram: Real-Time Tracking of Mobile RFID Tags to High Precision Using COTS Devices," in *Proc. of ACM MOBICOM*, 2014, pp. 237–248.

[33] R. Zhang, Y. Liu, Y. Zhang, and J. Sun, "Fast Identification of The Missing Tags in A Large RFID System," in *Proc. of IEEE SECON*, 2011, pp. 278–286.

[34] Y. Zheng and M. Li, "Fast Tag Searching Protocol for Large-Scale RFID Systems," *IEEE/ACM Transactions on Networking*, vol. 21, pp. 924–934, 2013.

[35] H. Zhou, V. C. M. Leung, C. Zhu, S. Xu, and J. Fan, "Predicting Temporal Social Contact Patterns for Data Forwarding in Opportunistic Mobile Networks," *IEEE Transactions on Vehicular Technology, DOI:10.1109/TVT.2017.274021*, 2017.

[36] H. Zhou, H. Zheng, J. Wu, and J. Chen, "Energy Efficiency and Contact Opportunities Trade-offs in Opportunistic Mobile Networks," *IEEE Transactions on Vehicular Technology*, vol. 65, pp. 3723–3734, 2016.

Honglong Chen received the M.E. degree in control theory and control engineering from Zhejiang University, China, in 2008, and the Ph.D degree in computer science from The Hong Kong Polytechnic University, Hong Kong, in 2012. He was a Postdoctoral Researcher in the School of CIDSE at Arizona State University from 2015 to 2016. He is currently an Associate Professor with the College of Information and Control Engineering, China University of Petroleum, China. His current research interests are in the areas of RFID and Internet of things. He has published more than 40 research papers in prestigious journals and conferences including IEEE TVT, IEEE TETC, IEEE IoT-J, IEEE INFOCOM, IEEE ICPP, IEEE ICCCN, etc. He is a member of IEEE and ACM.

Zhibo Wang received the B.E. degree in Automation from Zhejiang University, China, in 2007, and his Ph.D degree in Electrical Engineering and Computer Science from University of Tennessee, Knoxville, in 2014. He is currently an Associate Professor with the School of Computer, Wuhan University, China. His currently research interests include wireless sensor networks, cyber-physical systems, and mobile sensing. He is a member of IEEE and ACM.

Feng Xia is a Professor and PhD supervisor in the School of Software, Dalian University of Technology, China. He is the (guest) editor of several international journals. He serves as general chair, PC chair, workshop chair, publicity chair, or PC member of a number of conferences. He has authored/co-authored one book and more than 140 scientific papers in international journals and conferences. His research interests include social computing, mobile computing, and cyber-physical systems. He is a senior member of the IEEE, IEEE Computer Society, IEEE SMC Society, and a member of ACM and ACM SIGMobile.

Yanjun Li received the B.S. and Ph.D. degrees from Zhejiang University, Hangzhou, China, in 2004 and 2009, respectively, and another Ph.D. degree from Nancy University, Villers-les-Nancy, France, in 2010. She is currently an Associate Professor in School of Computer Science and Technology, Zhejiang University of Technology, Hangzhou, China. Her research area includes energy harvesting sensor networks and Internet of things.

Leyi Shi received the M.E. degree in computer science from China University of Petroleum, China, in 2002, and the Ph.D degree in computer science from Nankai University, China, in 2008. He has been a Visiting Scholar in University of North Carolina in 2011. He is currently a full Professor with the College of Computer and Communication Engineering, China Unviersity of Petroleum, China. His current research interests include computer networks, information security and game theory.