Fast Identification of Blocked RFID Tags

Xiulong Liu, Xin Xie, Xibin Zhao, Kun Wang, Keqiu Li, Alex X. Liu, Song Guo, Jie Wu

Abstract—The widely used RFID systems are vulnerable to the denial-of-service (DoS) attacks launched by malicious blocker tags. This paper studies how to quickly and completely identify the valid RFID tags that are blocked. The existing work that can seemingly address this problem suffers from either low time-efficiency or serious false positives. This paper proposes a hybrid approach that consists of two complementary component protocols, namely *Aloha Filtering (AF)* and *Poll&Listen (PL)*. *AF* is fast but inaccurate, while *PL* is accurate but slow. Taking the merit of each protocol, our hybrid approach is to first repeat the fast *AF* for multiple rounds to quickly filter out the target tags that are definitely not blocked. Then, on the size-reduced remaining set that just contains a small number of suspicious tags, we invoke the accurate *PL* to verify the intactness of each suspicious tag with 100% confidence. We optimize the round count of *AF* that trades off between the time costs of *AF* and *PL* to minimize the total time of *AF+PL*. As required in the optimization process, we need to know the size of the blocked tag set and that of the unknown tag set, which, however, are not known in advance. To estimate these two set sizes, we propose a supplementary protocol called *Simultaneous Estimation of the Blocked tag size and the Unknown tag size (SEBU)*. The key advantages of our approach over the prior art are four-fold. First, unlike the detection protocol that just discovers the existence of blocking attacks, our approach exactly identifies all the blocked target tags. Second, our approach is compliant with the C1G2 standard, and does not require any modifications to be made to the commercial RFID tags. It only needs to be installed on readers as a software module. Third, our approach does not involve any false positives. Finally, our approach significantly reduces the execution time when compared with the state-of-the-art schemes that can completely identify the blocked tags.

Index Terms—RFID, Blocked tags, Complete Identification, Trade-off, Estimation.

1 Introduction

1.1 Motivation & Problem Formulation

The next generation internet will be the internet of things (IoT) [1]–[10], which is presumed to be enabled by integrating simple computing plus communications capabilities into common objects of everyday use. Radio Frequency Identification (RFID) is a compelling technology for creation of such pervasive sensor networks owning to its potential for ubiquitous, low-cost/lowmaintenance use. RFID has been widely used in various applications such as supply chain management [6], [11]–[14], anti-counterfeit [15], indoor localization [16], object tracking [17], *etc.* IDTechEx forecasted that the total RFID market can rise to $27.3 billion in 2024 [18].

A great deal of effort has been made to address the practical problems, *e.g.*, tag identification [19]–[21] for item inventory, tag cardinality estimation [22]–[24] for stock monitoring, missing tag detection [25], [26] for theft surveillance, *etc.* Different from these papers, this paper focuses on the diagnosis issue, specifically, pinpointing the blocking attack that could make the RFID system crash. Specifically, the most popular MAC layer communication mechanism adopted by the RFID devices are framed slotted aloha protocol [20], in which each RFID tag chooses a slot to respond to the reader with its ID or other stored information. The reader is able to identify a tag in a slot when only one tag responds. While RFID technology has promising prospects, it is vulnerable to the denial-of-service (DoS) attacks launched by malicious blocker tags. Generally, we classify the possible DoS attacks into two types. The first type is called *randomly blocking*, *i.e.*, the blocker tag randomly chooses some slots to inject noise to make the communication channel between the reader and valid tags more crowded, and thus reducing the throughput of the RFID systems. The second type is called *specified blocking*, *i.e.*, the blocker tag specifies some tag IDs to block. Such a blocker tag is preconfigured with a set of blocking tag IDs, and simulates a set of fake tags each with a blocking ID. Different from valid RFID tags, the blocker tag only responds with noise instead of any useful information. However, if the noise replied by blocker is coincidentally the same as what the real tag replied, the reader will see it as a singleton reply. Fortunately, the probability of this case is as small as $\frac{1}{2^{16}} \approx 0.000015$ (we use 16-bit `RN16` in this paper). Similar with [27], we also ignore this issue due to the small probability. As most RFID literature [25], [28]–[33] stated, an RFID tag uses its ID to calculate a hash function, thereby pseudo-randomly choosing a slot from a slotted time frame to respond to the reader's query. As a result, the responses from the valid tags whose IDs are in the blocking ID set will be always corrupted by the noise from blocker tag. Such valid tags are called blocked tags, because their IDs or the stored information can never be correctly received by the valid reader.

Although the random blocking attack can reduce the throughput of the RFID systems, each tag still has a chance to report its ID (or other information) to the reader. However, the specified blocking attack can make some of the tags unable to report its ID

- *Xiulong Liu and Song Guo are with the Department of Computing, The Hong Kong Polytechnic University, Hong Kong, China.*
- *Xin Xie is with the School of Computer Science and Technology, Dalian University of Technology, China.*
- *Xibin Zhao is with Key Laboratory for Information System Security, Ministry of Education (KLISS), Tsinghua National Laboratory for Information Science and Technology (TNList), School of Software, Tsinghua University. (Xibin Zhao is the corresponding author).*
- *Kun Wang is with the School of Internet of Things, Nanjing University of Posts and Telecommunications, China. (e-mail: kwang@njupt.edu.cn)*
- *Keqiu Li is with the School of Computer Science and Technology, Tianjin University, China.*
- *Alex X. Liu is with the Department of Computer Science and Engineering, Michigan State University, East Lansing, MI 48824-1226 USA.*
- *Jie Wu is with the Department of Computer and Information Sciences, Temple University, USA.*

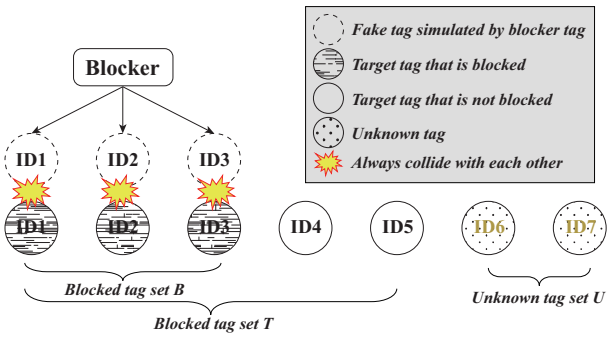


Fig. 1. Exemplifying the system model of the studied problem.

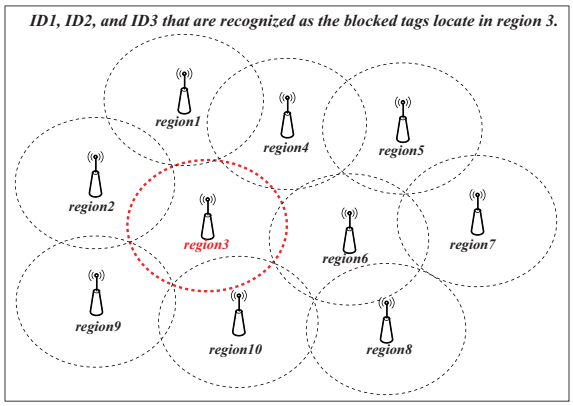


Fig. 2. Exactly identification of blocked tags can help find out which regions the blocker tags locate in.

any more. Hence, we think the specified blocking attack poses a more serious threat to the RFID systems. Moreover, the random blocking attack has been studied in the literature [34]. However, no dedicated effort has been paid to addressing the specified blocking attack. Hence, this paper focuses on the specified blocking attack, and studies how to quickly and completely identify the blocked tags. For example, consider a warehouse where each frozen food is affixed with a sensor-augmented RFID tag for monitoring the temperature. The tags that are blocked by the malicious blocker tag can never correctly report the temperature information to the valid readers. If we cannot identify the food whose temperature is above an allowable threshold in a timely manner, it may rapidly decay. Clearly, blocking attack can cause serious economic losses or even security issues. We desire to know the exact tags on which items or at which locations are blocked, so as to accurately measure the adverse affect of the blocking attacks on current RFID system, and further take effective countermeasures.

The studied problem of *complete identification of blocked tags* is formulated as follows. As illustrated in Fig. 1, let T be the set of the *target tags* that we want to verify. B represents the set of *blocked target tags*. We use U to denote the set of the *unknown tags* whose IDs are not known in prior. An example is given below to explain why we have unknown tags in a practical system. In a multi-tenant warehouse, for a tenant, the tags belonging to other tenants but in the vicinity of its RFID reader are unknown because this tenant normally has no right to know those tags' information [31]. The target tag set T is known in advance. On the contrary, we know neither the detailed tag IDs in B or U, nor their sizes $|B|$ or $|U|$. What we know is their relationship: $B \subseteq T$, and $T \cap U = \emptyset$. This paper studies how to quickly identify the blocked tags in B with no false positives. Here, *false positive* occurs when the target tags that are not blocked are misrecognized as the blocked ones.

1.2 Limitations of Prior Art

The key limitations of previous work are summarized as four aspects: just boolean detection result, non-C1G2 compliant, involving false positives, and low time-efficiency. The probabilistic blocked tag detection protocol [34] aims at diagnosing whether there is a blocking attack in the RFID system. We think such a boolean answer (just yes or no) returned by the detection protocol is not sufficient. In what follows, we will give two examples to explain what we can benefit from exactly identifying the blocked tags. First, in large-scale scenarios as illustrated in Fig. 2, multiple readers need to be deployed to cover the whole monitoring area due to the limited communication range of a single reader. In reality, we usually know where each RFID tag is deployed. Thus, if we exactly know which tags are blocked, it is more easy for us to find the regions where the malicious blocker tags locate. For example, if we know the tags ID1, ID2, and ID3 are blocked, and they locate in the *region 3*. Then, we can directly go to *region 3* to find out the blocker tag, instead of searching all regions one by one. Second, the tagged objects in an RFID system are usually of different values. The blocker tag will cause different degrees of damage to the system, when it blocks different tags. Thus, if we exactly know which tags are blocked, we can measure the degree of the adverse effect caused by the blocking attack, and then take the proper countermeasures. Here, exact identification of each blocked tag is more desirable. Wang *et al.* focused on identifying the blocking range for tree-based RFID systems [35]. However, the prevalent C1G2 RFID standard does not support the tree-based mechanism, which drastically limits the use of their scheme. The cloned tag identification protocol, *S-BID* [27], was proposed with an unrealistic assumption that all the tag IDs in a system should be known in advance. *S-BID* is based on the framed slotted Aloha protocol. It assumes that each tag has a pseudo-random hash function and uses it to select a slot from the time frame to respond. The back-end server is able to predict which slots in the time frame should be singleton (only one tag response in it), collision (two or more tag responses in it), and empty (no tag response). If the reader finds that an expected singleton slot turns out to be a collision one, we can assert that the tag selected in this slot is definitely cloned. Extensive simulation results demonstrate that *S-BID* suffers from serious false positives in the practical scenarios with unknown tags. The Aloha-based identification protocols can identify the intact tags in the singleton slots. The tags that are not identified seem to be blocked. But do not forget that hash collisions inherent in Aloha-based protocols can also cause an intact target tag to be not identified. Hence, the Aloha-based identification protocols also suffer from false positives. The tree-based identification protocols [19] do identify the blocked target tags with 100% accuracy. However, extensive simulation results show that *Tree Hopping* [19], the state-of-the-art tree-based identification protocol, is of low time-efficiency.

1.3 Proposed Approaches

The rules of designing our approaches are to overcome the limitations of prior art that are summarized in Section 1.2. In this paper, we first propose a simple but false positive-free protocol

called *Poll&Listen (PL)*. Specifically, the reader polls the target tag IDs in T one by one, and then listens to the channel to check the received tag response. A tag will respond to the reader, upon finding that its ID is queried. If a target tag is blocked, the reader will receive a collision response; otherwise, it will receive a singleton response. Clearly, *PL* can identify all blocked tags in T with no false positives. However, *PL* is time-consuming because it incurs heavy transmission of tag IDs in the low-rate wireless channel. Therefore, it is not time-efficient to perform *PL* on a large target tag set T.

Second, we propose a lightweight protocol called *Aloha Filtering (AF)* to drastically shrink the large target tag set T by quickly filtering out most of the target tags that are definitely not blocked. Specifically, the reader queries all the tags (*i.e.*, $T \cup U$) by broadcasting the parameters R and f, where R is a random seed and f is the number of slots in the forthcoming frame. Each tag pseudo-randomly chooses a slot sc in the frame to respond to the reader with `RN16` (a 16-bit random string), by calculating the hash function $sc = \mathcal{H}(ID, R) \mod f$. Hash-enabled solution (such as missing tag identification [25], [26], [36], and tag searching [37], *etc.*) is one of the most promising topics in the past decade. These protocols assume that each tag contains a hash function, such that a tag can select a random but predicable time slot to reply with a one-bit presence signal that shows its existence. However, the hash function has not been implemented in COTS tags in reality, which make the reviewer think the proposed protocol is a more academic/less industry-based approach. We did a comprehensive research of existing hash functions and found an existing news that Yang *et al.* [38] has designed and implemented a group of analog on-tag hash primitives (called Tash) for COTS Gen2-compatible RFID systems, which moves the hash-based protocols forward from theory to practice. There are three types of slots in the frame: *empty slot*, in which no tag responds; *singleton slot*, in which only one tag responds; *collision slot*, in which two or more tags respond. Accordingly, we can obtain an array $\mathbb{TU}[0..f-1]$, each entry with value 0, 1, or c, representing empty, singleton, or collision slot, respectively. On the other hand, we can virtually execute the Aloha protocol with the same parameters R and f on the target tag set T. Thus, we can get another array $\mathbb{T}[0..f-1]$. Due to the existence of blocked tags and unknown tags, these two arrays may be different. If $\mathbb{T}[i] = 1$ and $\mathbb{TU}[i] = 1$, we can assert that the target tag choosing slot i is definitely not blocked. If $\mathbb{T}[j] = 0$ and $\mathbb{TU}[j] \neq 0$, the tags choosing slot j are definitely the unknown tags. In the slots, like i and j, the reader sends command to deactivate the intact target tags or unknown tags. Unlike *PL*, *AF* is time-efficient because it only needs a tag to transmit 16-bit `RN16` instead of 96-bit tag ID.

Generally, *PL* is accurate, but time-consuming due to the heavy transmission of tag IDs. On the contrary, *AF* is time-efficient, but inaccurate because its probabilistic nature inherent from Aloha mechanism may cause the false positives. Hence, *AF* and *PL* are complementary to each other and should be jointly used. A hybrid approach is to first repeat *AF* for several rounds to quickly filter out most of the intact target tags, and then perform *PL* on the size-reduced target tag set T.

1.4 Technical Challenges and Solutions

The first technical challenge is to optimize the frame count n of *AF*, thereby minimizing the total execution time $\mathcal{T}_{AF}^n + \mathcal{T}_{PL}^n$, where $\mathcal{T}_{AF}^n$ and $\mathcal{T}_{PL}^n$ are the time cost of *AF* and *PL*, respectively, when executing *AF* for n frames. If the frame count n of *AF* is too small, the size of the target tag set T will not be sufficiently reduced; as a result, performing *PL* on T is still time-consuming. On the contrary, if the frame count n of *AF* is too large, the target tag set T does quickly shrink at the first several frames; however, the size of T will no longer significantly reduce for the last several frames, because most of the intact target tags have already been filtered out by previous frames. Hence, repeating excessive frames of *AF* may deteriorate the time-efficiency instead. Essentially, the frame count n trades off between the time costs of *AF* and *PL*. To optimize the value of frame count n of *AF*, we first calculate the expressions of the time cost $\mathcal{T}_{AF}^n$ and $\mathcal{T}_{PL}^n$, respectively. Then, we formulate and solve a constraint optimization problem with the goal of minimizing $\mathcal{T}_{AF}^n + \mathcal{T}_{PL}^n$.

The second technical challenge is to estimate the set sizes $|B|$ and $|U|$ in a simultaneous manner. The optimization of *AF+PL* closely depends on the set sizes of $|T|$, $|B|$, and $|U|$. However, except for $|T|$, the other two variables are not known in advance. This paper proposes an estimation protocol called *Simultaneous Estimation of the Blocked tag size and the Unknown tag size (SEBU)*. We first present two functional estimators for estimating the set sizes $|B|$ and $|U|$, respectively, where the numbers of $\langle *, 0\rangle$ and $\langle 1, 1\rangle$ slot pairs observed from $\mathbb{TU}[0..f-1]$ and $\mathbb{T}[0..f-1]$ are used as the inputs of our estimators. Second, we calculate the variance of each estimator to measure the estimation deviation. Third, we calculate the minimum rounds of estimation to ensure that the estimates can satisfy the required accuracy. Finally, rigorous analysis is given to optimize the parameters to minimize $\max\{\mathcal{T}_B, \mathcal{T}_U\}$, where $\mathcal{T}_B$ and $\mathcal{T}_U$ are the time required to ensure the accuracy of these two estimates, respectively.

1.5 Novelty and Advantage over Prior Art

This paper formalizes the practically important problem of blocked tag identification, where we abandon the unrealistic assumption that all tag IDs are known in advance. The technical novelty of this paper is in proposing the hybrid approach called *AF+PL* and the simultaneous estimation approach called *SEBU*. In addition, we have addressed the two technical challenges summarized above. The key advantages of the proposed approach over the prior art are four-fold: (1) Our approach exactly identifies all the target tags that are blocked, instead of just reporting a boolean result. Hence, we can provide more information to evaluate the adverse affect of the blocking attacks. (2) Our approach is compliant with the C1G2 standard, and does not require any modifications to be made to the commercial RFID tags. It only needs to be installed on readers as a software module. (3) Our approach can correctly identify the blocked tags without any false positives. (4) Extensive simulation results reveal that our approach significantly reduces the execution time when compared with the state-of-the-art schemes that can completely identify the blocked tags.

The remainder of this paper is organized as follows. In Section 2, we present *AF+PL*. In Section 3, we present methods to estimate the set sizes $|B|$ and $|U|$. Section 4 presents the extensive simulation results to evaluate the performance of the proposed protocol. Section 5 reviews the related work. Finally, we conclude the paper in Section 6.

2 Design of Hybrid Approach: *AF+PL*

For clarity, we first describe a straightforward protocol called *Poll&Listen (PL)*, which is quite simple and 100% accurate, but

inefficient because it needs to queries each 96-bit ID in a large target tag set. To overcome the deficiency of *PL* meanwhile maintaining the 100% accuracy, we propose a hybrid approach *AF+PL*, which invokes the lightweight *Aloha Filtering (AF)* scheme before running *PL* to quickly shrink the target tag set T by filtering out most unblocked (intact) target tags. Then, performing the *PL* protocol on such a size-reduced target tag set may require much less time than directly invoking *PL*. While *AF* could fast reduce the number of target tags that need to be verified by *PL*, it is not cost-free and excessive execution of *AF* may deteriorate the overall time-efficiency instead. Hence, after the detailed protocol description, we theoretically optimize the round count of *AF* that trades off between the time cost of *AF* and *PL*.

2.1 The Straightforward Protocol: PL

A simple but false-free solution to identification of blocked tags is to poll and verify the intactness of the target tags in T one by one. In what follows, we will explain how to use the commands available in the C1G2 standard to implement the *PL* protocol. The reader uses the `Select` command containing a target tag ID to let the tag with this ID be active. Then, the reader issues a single-slot frame by broadcasting the `Query` command; if the target tag is blocked, it and the blocker tag will simultaneously respond with `RN16` to the reader. If the reader receives a signal collision, we can assert that the queried target tag is blocked; otherwise, this target tag is intact. After polling all the target tag IDs, we can identify all the blocked target tags in B with no false positives. However, if a real tag and the blocker tag occasionally reply the same *RN16* in the same slot, the reader will see it as a singleton slot indeed. Thus, we mistakenly assert that this tag is not blocked. Although such false negative exists, fortunately, it is as small as $\frac{1}{2^{16}} \approx 0.000015$. In practice, the blocked tag identification protocol is usually periodically executed. Hence, even if a few blocked tags are not identified in this round of identification process due to the above rare false negative, they still have a chance to be identified in the next round of identification. Next, we will analyze the time cost of the *PL* protocol. Let t_{id} represent the time taken by the reader to send the `Select` command; t_{qry} represents the time taken by the reader to broadcast the `Query` command to initialize a single-slot frame; t_{rn} represents the time taken by the tag to respond with `RN16` to the reader. We need to poll each of the $|T|$ target tags, hence, the time cost of *PL* is $|T| \times (t_{id} + t_{qry} + t_{rn})$. Note that, the blocker tag may also simulate some fake tags whose IDs are not within the target tag set. But the blocker tag will never reply such an ID, because it will not be queried by the reader.

2.2 The Hybrid Protocol: AF+PL

Directly performing the *PL* protocol on a large target tag set T is time-consuming due to the heavy transmission of tag IDs. It is desirable to propose an lightweight protocol that can quickly shrink the target tag set T by filtering out most unblocked (intact) target tags. Then, performing the *PL* protocol on such a size-reduced target tag set may require much less time than directly invoking *PL*. We propose using the framed slotted Aloha protocol specified in the C1G2 standard to filter out the intact target tags and the unknown tags. Note that, both *intact target tag* and *unblocked target tag* indicate the tags in $T - B$, we may use them interchangeably in the rest of this paper.

The reader queries the tags by broadcasting the parameters R and f, where R is a random seed and f indicates the number

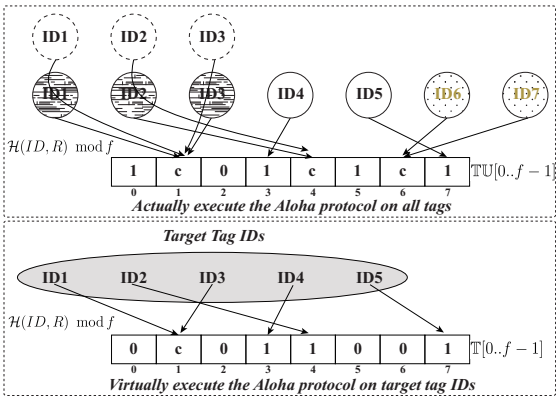


Fig. 3. Exemplifying the basic idea of *AF*.

of slots in the forthcoming time frame. Each tag initializes its slot counter sc by calculating the hash function $sc = \mathcal{H}(ID, R) \mod f \in [0, f-1]$. At the end of each slot, the reader sends the `QueryRep` command to synchronize the slots. Upon receiving the `QueryRep` command, a tag will decrement its slot counter sc by one. In any slot, the tags whose slot counters sc become 0 will respond to the reader with a 16-bit random string called `RN16`. Note that, for practical reasons [15], [19], the actual frame size should be no more than 512. A solution is that we let the reader announce a large frame size f called *broadcasted frame size*, but terminates the frame after the first $f' \leq 512$ slots, where f' is called the *executed frame size*.

The frame contains three types of slots: the *empty slot* in which no tag responds; the *singleton slot* in which only one tag responds; the *collision slot* in which two or more tags respond. By executing the Aloha protocol on the tag set $T \cup U$, we can obtain an array $\mathbb{TU}[0..f'-1]$, in which a bit is 0 if the slot with the same index is empty; a bit is 1 if the slot is singleton; a bit is c if the slot is collision. Since the target tag set T is known in prior, we can use the same parameters R and f to *virtually* execute the Aloha protocol on the tag IDs in T. Thus, we can get another array $\mathbb{T}[0..f'-1]$, in which a bit is 0 if no tag ID in T is hashed to this position; a bit is 1 if only one tag ID in T is hashed to this position; a bit is c if two or more tag IDs in T are hashed to this position. It is easy to know that, if there are neither blocked tags nor unknown tags, the arrays $\mathbb{TU}[0..f-1]$ and $\mathbb{T}[0..f-1]$ should always be the same, because the same hashing parameters R and f are used. However, due to the existence of blocked tags and unknown tags, the array $\mathbb{TU}[0..f'-1]$ may be different from $\mathbb{T}[0..f-1]$. We can conclude that, if $\mathbb{T}[i] = 1$ and $\mathbb{TU}[i] = 1$, the target tag that responded in the slot with index of i is definitely non-blocked. In this example, we know ID4 is mapped to the slot with index of 3, because we know $H(ID4, R) \mod f = 3$. Moreover, we find that $\mathbb{T}[3] = 1$ and $\mathbb{TU}[3] = 1$. Then, we can assert that the target tag ID4 is definitely not blocked. Similarly, we can also assert that the target tag ID5 is definitely not blocked. Then, ID4 and ID5 will be removed from the target tag set T, and we only need to query the other 3 target tag IDs in the *P&L* protocol, instead of querying all 5 target tag IDs. Since each tag only needs to respond with the 16-bit `RN16` in our *AF* protocol, which is much shorter than the 96-bit tag ID. Therefore, *AF* can filter out some of the unblocked target tags in a time-efficient way. On the other hand, if $\mathbb{T}[i] = 0$ while $\mathbb{TU}[i] = 1$ or c, the tags responded in this slot are definitely unknown tags. In the above two types of slots, the reader sends

TABLE 1
Main notations used in the paper.

Notation	Description
T	the set of target tags.
U/	the set of unknown tags.
B	the set of blocked tags.
$\|\cdot\|$	the set size.
$\widehat{\|\cdot\|}$	the estimated set size.
$\mathcal{H}(\cdot)$	hash function with uniform distribution.
f	broadcasted frame size.
f'	executed frame size.
t_{id}	time for sending `Select`.
t_{qry}	time for sending `Query`.
t_{rn}	time for sending `RN16`.
R	random seed.
$\mathcal{T}_{AF}^{n}$	time cost of *AF*, if n frames are executed by *AF*.
$\mathcal{T}_{PL}^{n}$	time cost of *PL*, if n frames are executed by *AF*.
$\Phi(\cdot)$	cumulative distribution function.
erf$(\cdot)$	standard error function.
erf$^{-1}(\cdot)$	inverse function of erf$(\cdot)$.
$\mathbb{T}[..]$	array by virtually running Aloha scheme on T.
$\mathbb{TU}[..]$	array by executing Aloha scheme on $T \cup U$.
$\mathcal{N}_{11}$	# of $\langle 1, 1\rangle$ in a frame.
$\mathcal{N}_{*0}$	# of $\langle *, 0\rangle$ in a frame.
$\mathcal{P}_{*0}$	probability that a slot is $\langle *, 0\rangle$.
$\mathcal{P}_{11}$	probability that a slot is $\langle 1, 1\rangle$.
$\mathcal{T}_U$	time for estimating $\|B\|$; time for estimating $\|U\|$.
α	required confidence interval.
β	required reliability.

the `ACK` command to deactivate the unblocked target tags and the unknown tags. These deactivated tags will not participate in the rest of process.

A *hybrid approach* proposed in this paper is to first repeat *AF* for n frames and then execute *PL* on the size-reduced target tag set. In large-scale RFID systems, a single reader may not be able to cover the whole area due to the limited communication range of the RFID devices, hence, multiple readers are required to be deployed. Since many effective reader-scheduling schemes have been proposed [39], the multiple readers can work as one big logical reader if the used parameters are consistent across the readers [15], [25], [40], [41]. Therefore, our protocol can work seamlessly in single-reader as well as multi-reader environments. Many excellent RFID literature [**?**], [25] has discussed the channel errors and the countermeasures, hence, this paper does not pay attention to this issue any more, and assumes we have an error-free communication channel between reader and tags. The main notations used in this paper are summarized in Table 1.

2.3 Parameter Optimization

Three key parameters, *i.e.*, f, f', and n, need to be optimized to minimize the total time cost of *AF+PL*. In this section, we first assume that we know the set sizes $|B|$ and $|U|$. Later, we will give a C1G-compliant protocol to estimate these two variables with guaranteed accuracy.

Let $\mathcal{P}_{ubf}$ be the probability that any unblocked target tag is filtered out in this frame. Here, the underlined letters compose the subscript of this notation. In the following, we also use the similar naming method. Recall that an unblocked target tag will be filtered out when it chooses a slot within the executed frame with size f', and this slot is not chosen by any other tags. We calculate $\mathcal{P}_{ubf}$ as follows:

$$\mathcal{P}_{ubf} = \frac{f'}{f}(1-\frac{1}{f})^{|T|+|U|-1} \approx \frac{f'}{f}e^{-\frac{|T|+|U|}{f}} \tag{1}$$

In the above equation, such an approximation is usually made in previous literature [29], [42], [43]. For an arbitrary unknown tag, the probability that it is filtered out in this frame is denoted as $\mathcal{P}_{ukf}$. Recall that an unknown tag is filtered out when it chooses a slot within the executed frame with size f', and this slot is not chosen by any target tags. Therefore, we can give the expression of $\mathcal{P}_{ukf}$ as follows:

$$\mathcal{P}_{ukf} = \frac{f'}{f}(1-\frac{1}{f})^{|T|} \approx \frac{f'}{f}e^{-\frac{|T|}{f}} \tag{2}$$

The time cost $\mathcal{T}$ of a frame is calculated by $\mathcal{T} = t_{qry} + f' \times t_{rn}$, where t_{qry} is the time for transmitting the `Query` command to initialize the frame, and t_{rn} is the time of each slot in the executed frame. Since each unblocked tag has the probability $\mathcal{P}_{ubf}$ to be filtered out in a frame, $(|T|-|B|)\times\mathcal{P}_{ubf}$ unblocked target tags will be filtered out on average. Our goal of executing the Aloha frame is to quickly shrink the target tag set by filtering out the unblocked target tags, and eventually accelerate the execution of the *PL* protocol. Therefore, we will optimize the values of f' and f to maximize the following efficiency function $\mathcal{F}$. The physical meaning of maximizing the value of $\mathcal{F}$ in Eq. (3) is that we want to use the least time to filter out the most unblocked target tags.

$$\mathcal{F} = \frac{(|T|-|B|)\times\mathcal{P}_{ubf}}{\mathcal{T}} \tag{3}$$

We propose Theorem 1 to optimize the values of f and f' to maximize the above efficiency function $\mathcal{F}$.

Theorem 1. *Given that a target tag set with size $|T|$, an unknown tag set with size $|U|$, and $|B|$ tags among T are blocked; the value of $\mathcal{F}$ in Eq. (3) is maximized when the broadcasted frame size f is set to $|T|+|U|$, and the executed frame size f' is set to* $\min\{f, 512\}$.

Proof. The first-order derivative $\frac{\partial\mathcal{F}}{\partial f}$ is calculated as follows:

$$\frac{\partial\mathcal{F}}{\partial f} = \frac{f'(|T|-|B|)\left\{(|T|+|U|)-f\right\}e^{-\frac{|T|+|U|}{f}}}{f^3(t_{qry}+f't_{rn})} \tag{4}$$

We observe from Eq. (4) that $\frac{\partial\mathcal{F}}{\partial f} = 0$ when $f = |T|+|U|$; $\frac{\partial\mathcal{F}}{\partial f} > 0$ when $f < |T|+|U|$; and $\frac{\partial\mathcal{F}}{\partial f} < 0$ when $f > |T|+|U|$. Therefore, the efficiency function $\mathcal{F}$ achieves the maximum values when the broadcasted frame size f is set to $|T|+|U|$. Similarly, the first-order derivative $\frac{\partial\mathcal{F}}{\partial f'}$ is calculated as follows:

$$\frac{\partial\mathcal{F}}{\partial f'} = \frac{(|T|-|B|)t_{qry}e^{-\frac{|T|+|U|}{f}}}{f(t_{qry}+f't_{rn})^2} \tag{5}$$

We observe from Eq. (5) that $\frac{\partial\mathcal{F}}{\partial f'}$ is always larger than 0. That is, the efficiency function $\mathcal{F}$ is a monotonously increasing function of the executed frame size f'. Hence, we should set f' to its maximum value. As a matter of fact, the executed frame size f' is less than or equal to the broadcasted frame size f. Moreover, f'

should be no more than 512 due to practical reasons. Therefore, we should set $f' = \min\{f, 512\}$. □

Assume that we repeat the *AF* protocol for $n \geq 0$ frames before executing the *PL* protocol. We represent the time cost of *AF* by $\mathcal{T}_{AF}^n$, and the time cost of *PL* by $\mathcal{T}_{PL}^n$. The numerical results shown in Fig. 4 reveal that the frame count n repeated by *AF* trades off between the time costs $\mathcal{T}_{AF}^n$ and $\mathcal{T}_{PL}^n$, and has a significant impact on the total time cost $\mathcal{T}_{AF}^n + \mathcal{T}_{PL}^n$. In this figure, $n = 0$ means that we do not perform the *AF* protocol at all, and directly use *PL* to verify the target tags one by one. We observe that directly executing *PL* on the target set T is not time-efficient because T is relatively large at the very beginning. Alternatively, we can repeat *AF* for several frames, then execute *PL* on the remaining target set T whose size is significantly reduced. Fundamentally, spending a small amount of time on *AF* can significantly accelerate the execution of *PL*. We observe from Fig. 4 that the total time cost of *AF+PL* decreases as the frame number n increases within the range of $[0, 20]$. However, repeating *AF* for excessive frames will reduce the time-efficiency of *AF+PL* instead. The underlying reason is as follows. In this case study, after 20 Aloha frames of *AF*, most of the unblocked target tags have been filtered out already, and thus repeating more frames of *AF* will no longer effectively shrink the target tag set. In this case, it is better to terminate the *AF* protocol and turn to invoke the *PL* protocol.

Next, we present how to optimize the frame count n to minimize the total time cost of *AF+PL*. Let $|T_i|$ (or $|U_i|$) denote the number of remaining target tags (or remaining unknown tags) after the i-th Aloha frame of *AF*, where $i \in [0, n-1]$. For a special case $i = 0$, we have $|T_0| = |T|$ and $|U_0| = |U|$. We use f_i' and f_i to respectively represent the executed frame size and broadcasted frame size that are used in the i-th Aloha frame of *AF*. To find the optimal value of frame number n that minimizes the total time $\mathcal{T}_{AF}^n + \mathcal{T}_{PL}^n$, we need to solve the optimization problem formulated as follows:

$$
\begin{aligned}
&\textit{Minimize } \mathcal{T}_{AF}^n + \mathcal{T}_{PL}^n \qquad (6)\\
&\textit{subject to } |T_0| = |T| \text{ and } |U_0| = |U|\\
&\quad |T_i| = (|T_{i-1}| - |B|) \times \left\{1 - \frac{f'_{i-1}}{f_{i-1}} e^{-\frac{|T_{i-1}|+|U_{i-1}|}{f_{i-1}}}\right\} + |B|\\
&\quad |U_i| = |U_{i-1}| \times \left\{1 - \frac{f'_{i-1}}{f_{i-1}} e^{-\frac{|T_{i-1}|}{f_{i-1}}}\right\}\\
&\quad f_i = |T_i| + |U_i| \text{ and } f'_i = \min\{f_i, 512\}\\
&\quad \mathcal{T}_{AF}^n = \sum_{i=0}^{n-1} (t_{qry} + f'_i \times t_{rn})\\
&\quad \mathcal{T}_{PL}^n = |T_n| \times (t_{id} + t_{qry} + t_{rn})
\end{aligned}
$$

In the above optimization problem, the second constraint is obtained according to Eq. (1); the third constraint is obtained according to Eq. (2); the values of f_i and f_i' in the fourth constraint are according to Theorem 1. Since the Aloha frame number n is bounded integer, we can find the optimal value for n by an exhaustive searching method, which occurs offline before executing our *AF+PL* protocol.

3 Estimation of $|B|$ and $|U|$: *SEBU*

The optimization of the proposed hybrid approach *AF+PL* depends on the set sizes $|T|$, $|B|$, and $|U|$. For example, when the set of the target tag set T is very small, directly performing *PL* may be best choice; on the contrary, when only a small ratio of valid tags in a large target tag set are blocked, we should invoke *PL* after repeating several rounds of *AF*. However, except for $|T|$, the other two variables $|B|$ and $|U|$ are not known in advance. Hence, this section proposes an estimation protocol called *Simultaneous Estimation of the Blocked tag size and the Unknown tag size (SEBU)* to estimate these two set sizes. Different from prior estimation problem, we studies how to estimate two variables at the same time. In this section, we first describe the detailed design of SEBU, and then propose theoretical analysis to give the quantified variance in the estimator. After that, we investigate how many rounds of estimation are required to guarantee the predefined accuracy, and how the involved parameters should be optimized to minimize the time cost of SEBU.

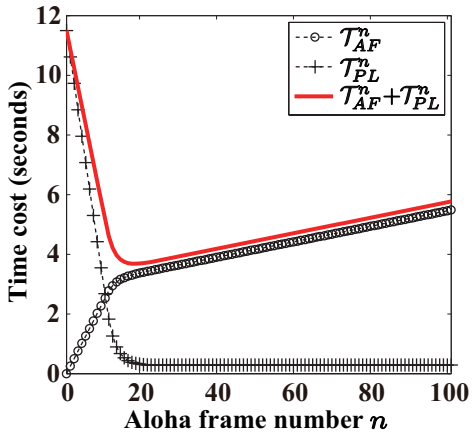


Fig. 4. The number of frames n repeated by *AF* trades off between the time costs $\mathcal{T}_{AF}^n$ and $\mathcal{T}_{PL}^n$. $|T| = 2000$, $|U| = 400$, $|B| = 50$.

3.1 Estimators and Variances

In what follows, we first present the detailed design of SEBU, which is stilled based on the framed slotted Aloha communication mechanism. Recall that we can obtain an array $\mathbb{T}[0..f'-1]$ by virtually executing the Aloha protocol on the target tag set T, and the array $\mathbb{TU}[0..f'-1]$ by using the same parameters R and f to actually execute Aloha protocol on the tag set $T \cup U$. We refer to the two bits that have the same index in $\mathbb{T}[0..f'-1]$ and $\mathbb{TU}[0..f'-1]$ as a *bit pair*, which is represented by $\langle \mathbb{T}[i], \mathbb{TU}[i] \rangle$, $i \in [0, f'-1]$. For the slot pair with index of i, it is $\langle 1, 1 \rangle$ when $\mathbb{T}[i] = 1$ and $\mathbb{TU}[i] = 1$; it is $\langle *, 0 \rangle$ when $\mathbb{TU}[i] = 0$. Here $*$ means the wildcard, *i.e.*, $\mathbb{T}[i]$ could be any value within $\{$'0','1','c'$\}$. Inspired by [42], *SEBU* compares two arrays and leverages the numbers of $\langle 1, 1 \rangle$ slots and $\langle *, 0 \rangle$ slots to estimate the set sizes $|B|$ and $|U|$. Here, slot j is $\langle 1, 1 \rangle$ when $\mathbb{T}[j] = 1$ and $\mathbb{TU}[j] = 1$; or $\langle *, 0 \rangle$ when $\mathbb{TU}[j] = 0$. Intuitively, when the number of tags $|T \cup U|$ is large, the ratio of empty slots in the array $\mathbb{TU}[0..f'-1]$ will be small. Hence, we can leverage the number of $\langle *, 0 \rangle$ slots to estimate the set size $|T \cup U|$, and further obtain the set size $|U|$ by calculating $|T \cup U| - |T|$. On the other hand, since the blocked tags can change some $\langle 1, 1 \rangle$ slots to $\langle 1, c \rangle$ slots, the ratio of $\langle 1, 1 \rangle$ slots will be less than expected. Hence, we can leverage the number of $\langle 1, 1 \rangle$ slots to estimate the blocked set size $|B|$. Note that, different from [42], this paper aims at simultaneously estimating the set sizes $|B|$ and $|U|$, *i.e.*, killing two birds with one stone. The new technical challenge we face

here is to find an optimal parameter pair $\langle f', f\rangle$ to *minimize the maximum* time of the two estimators.

Let $\mathcal{P}_{11}$ represent the probability that an arbitrary slot in the executed frame is a $\langle 1,1\rangle$ slot, which happens when this slot is only chosen by a tag in $T-B$. Hence, we have:

$$\mathcal{P}_{11}=\binom{|T-B|}{1}\left(\frac{1}{f}\right)\left(1-\frac{1}{f}\right)^{|T+U|-1}\approx\frac{|T-B|}{f}e^{-\frac{|T+U|}{f}} \tag{7}$$

The number of $\langle 1,1\rangle$ slots in the executed frame, denoted as $\mathcal{N}_{11}$, follows the distribution of *Bernoulli*$(f', \mathcal{P}_{11})$. Hence, we calculate the expectation of the variable $\mathcal{N}_{11}$ as follows.

$$E(\mathcal{N}_{11})=f'\times\mathcal{P}_{11}=\frac{f'|T-B|}{f}e^{-\frac{|T+U|}{f}} \tag{8}$$

Similarly, we use $\mathcal{P}_{*0}$ to denote the probability that an arbitrary slot in $\mathbb{TU}[0..f'-1]$ is empty, which happens when no tag in $T\cup U$ is hashed to this slot. Then, we have:

$$\mathcal{P}_{*0}=\left(1-\frac{1}{f}\right)^{|T+U|}\approx e^{-\frac{|T+U|}{f}} \tag{9}$$

The number of $\langle *,0\rangle$ slots in the executed frame, denoted as $\mathcal{N}_{*0}$, follows *Bernoulli*$(f', \mathcal{P}_{*0})$. Then, we calculate the expectation of the variable $\mathcal{N}_{*0}$ as follows.

$$E(\mathcal{N}_{*0})=f'\times\mathcal{P}_{*0}=f'e^{-\frac{|T+U|}{f}} \tag{10}$$

Based on Eqs. (8)(10), we get the expressions of $|B|$ and $|U|$:

$$|B|=|T|-\frac{fE(\mathcal{N}_{11})}{E(\mathcal{N}_{*0})}\text{ and }|U|=-f\ln\frac{E(\mathcal{N}_{*0})}{f'}-|T| \tag{11}$$

Substituting $\mathcal{N}_{11}$ for $E(\mathcal{N}_{11})$ and $\mathcal{N}_{*0}$ for $E(\mathcal{N}_{*0})$ in Eq. (11), we obtain the estimators $\widehat{|B|}$ and $\widehat{|U|}$ below:

$$\widehat{|B|}=|T|-\frac{f\mathcal{N}_{11}}{\mathcal{N}_{*0}}\text{ and }\widehat{|U|}=-f\ln\frac{\mathcal{N}_{*0}}{f'}-|T| \tag{12}$$

To evaluate the accuracy of the estimators $\widehat{|B|}$ and $\widehat{|U|}$, Lemmas 1 and 2 calculate their variances, respectively.

Lemma 1. *Let f and f' be the broadcasted frame size and the executed frame size, respectively, T be the target tag set, B be the blocked tag set, and U be the unknown tag set; the variance of the estimate $\widehat{|B|}$ is given by the following equation:*

$$Var(\widehat{|B|})=\frac{1}{f'}\left(|T-B|^2+f|T-B|\right)e^{\frac{|T+U|}{f}} \tag{13}$$

Proof. Eq. (12) infers that $\widehat{|B|}$ is function of $\mathcal{N}_{*0}$ and $\mathcal{N}_{11}$. Hence, we can represent $\widehat{|B|}$ by $\phi(\mathcal{N}_{*0},\mathcal{N}_{11})$. In what follows, we calculate its Taylor's series expansion around (θ_0,θ_1), where $\theta_0=E(\mathcal{N}_{*0})$ and $\theta_1=E(\mathcal{N}_{11})$.

$$\widehat{|B|}=\phi(\theta_0,\theta_1)+\left\{(\mathcal{N}_{*0}-\theta_0)\frac{\partial\phi}{\partial\mathcal{N}_{*0}}+(\mathcal{N}_{11}-\theta_1)\frac{\partial\phi}{\partial\mathcal{N}_{11}}\right\} \tag{14}$$

Taking the expectation of both sides of the above equation, we have $E(\widehat{|B|})=\phi(\theta_0,\theta_1)=|B|$. Since $Var(\widehat{|B|})=E\left\{\widehat{|B|}-E(\widehat{|B|})\right\}^2$, we calculate its expression as follows.

$$\begin{aligned}Var(\widehat{|B|})=&\left(\frac{\partial\phi}{\partial\mathcal{N}_{*0}}\right)^2Var(\mathcal{N}_{*0})+\left(\frac{\partial\phi}{\partial\mathcal{N}_{11}}\right)^2Var(\mathcal{N}_{11})\\&+2Cov(\mathcal{N}_{*0},\mathcal{N}_{11})\frac{\partial\phi}{\partial\mathcal{N}_{*0}}\frac{\partial\phi}{\partial\mathcal{N}_{11}}\end{aligned} \tag{15}$$

As required by Eq. (15), we calculate the the following items.

$$\begin{cases}Var(\mathcal{N}_{*0})=f'e^{-\frac{|T+U|}{f}}\left(1-e^{-\frac{|T+U|}{f}}\right)\\Var(\mathcal{N}_{11})=\dfrac{f'|T-B|e^{-\frac{|T+U|}{f}}}{f}\left(1-\dfrac{|T-B|e^{-\frac{|T+U|}{f}}}{f}\right)\\\dfrac{\partial\phi}{\partial\mathcal{N}_{*0}}=\dfrac{|T-B|}{f'}e^{\frac{|T+U|}{f}}\text{ and }\dfrac{\partial\phi}{\partial\mathcal{N}_{11}}=-\dfrac{f}{f'}e^{\frac{|T+U|}{f}}\\Cov(\mathcal{N}_{*0},\mathcal{N}_{11})=-\dfrac{f'|T-B|}{f}e^{-\frac{2|T+U|}{f}}\end{cases}$$

Substituting the above items into Eq. (15), we get Eq. (13). □

Lemma 2. *Let f and f' be the broadcasted frame size and the executed frame size, respectively, T be the target tag set, B be the blocked tag set, and U be the unknown tag set; the variance of the estimate $\widehat{|U|}$ is given as follows:*

$$Var(\widehat{|U|})=\frac{f^2}{f'}\left(e^{\frac{|T+U|}{f}}-1\right) \tag{16}$$

Proof. Eq. (12) infers that $\widehat{|U|}$ is function of $\mathcal{N}_{*0}$. Hence, we can represent $\widehat{|U|}$ by $\varphi(\mathcal{N}_{*0})$. The Taylor's series expansion of $\varphi(\mathcal{N}_{*0})$ around $\rho=E(\mathcal{N}_{*0})$ is given as follows:

$$\widehat{|U|}=\varphi(\mathcal{N}_{*0})=\varphi(\rho)+(\mathcal{N}_{*0}-\rho)\frac{\partial\varphi}{\partial\mathcal{N}_{*0}} \tag{17}$$

Taking expectation of both sides of the above equation, we have $E(\widehat{|U|})=\varphi(\rho)$. Since $Var(\widehat{|U|})=E\left\{\widehat{|U|}-E(\widehat{|U|})\right\}^2$, we can calculate its expression as follows.

$$Var(\widehat{|U|})=\left(\frac{\partial\varphi}{\partial\mathcal{N}_{*0}}\right)^2Var(\mathcal{N}_{*0}) \tag{18}$$

As required by Eq. (18), we calculate that $\frac{\partial\varphi}{\partial\mathcal{N}_{*0}}=-\frac{f}{f'}e^{\frac{|T+U|}{f}}$. Recall that $Var(\mathcal{N}_{*0})=f'e^{-\frac{|T|+|U|}{f}}(1-e^{-\frac{|T+U|}{f}})$. Substituting them into Eq. (18), we obtain Eq. (16). □

3.2 Number of Frames k

Due to the probabilistic nature of the proposed *SEBU* method, the estimates $\widehat{|B|}$ and $\widehat{|U|}$ obtained from one frame may differ from their real values. Hence, a single round of estimation can hardly ensure the predefined accuracy requirement. To relieve such estimation deviation, we repeat *SEBU* for $k\geq 1$ frames each with a fresh seed R, and use the average value of the estimates to refine the estimation results. The estimates averaged from k frames, *i.e.*, $\mathcal{A}^k_{|B|}=\frac{1}{k}\sum_{x=1}^{k}\widehat{|B|}_x$ and $\mathcal{A}^k_{|U|}=\frac{1}{k}\sum_{x=1}^{k}\widehat{|U|}_x$, serve as the fine-grained estimation results. Here, $\widehat{|B|}_x$ and $\widehat{|U|}_x$ are the estimates obtained from the x-th frame. The relative error tolerance $\alpha\in(0,1]$ and the required reliability $\beta\in[0,1)$ are used to measure the accuracy of the estimates $\mathcal{A}^k_{|B|}$ and $\mathcal{A}^k_{|U|}$. Since the relative values of $|B|$ and $|U|$ compared with $|T|$ dominate the optimal solution to the problem formulated in Eq. (6), we use the known value $|T|$ as the benchmark. Specifically, the average estimates should satisfy $Pr\{|\mathcal{A}^k_{|B|}-|B||\leq\alpha|T|\}\geq\beta$ and $Pr\{|\mathcal{A}^k_{|U|}-|U||\leq\alpha|T|\}\geq\beta$, respectively. In the following, we propose two theorems to calculate the round count k that can ensure the above two accuracy constraints.

Theorem 2. *Given that a required confidence interval α, a required reliability β, a broadcasted frame size f, and an executed frame size f'; the estimates $\mathcal{A}^k_{|B|}$ and $\mathcal{A}^k_{|U|}$ meet the required*

(α, β) *accuracy, when the number of frames* k *executed by SEBU satisfies* $k \geq \max\{k_B, k_U\}$*, where*

$$k_B = \left\{ \frac{\text{erf}^{-1}(\beta)}{\alpha|T|\sqrt{f'}} \right\}^2 \left(|T-B|^2 + f|T-B|\right) e^{\frac{|T+U|}{f}} \quad (19)$$

$$k_U = \left\{ \frac{\text{erf}^{-1}(\beta) f}{\alpha|T|\sqrt{f'}} \right\}^2 \left(e^{\frac{|T+U|}{f}} - 1 \right) \quad (20)$$

Proof. Assume k independent rounds of estimation are executed by *SEBU*. Then, the variance of $\mathcal{A}^k_{|B|}$ is reduced k times, *i.e.*, $Var(\mathcal{A}^k_{|B|}) = \frac{1}{k} Var(|\widehat{B}|)$. Let $\mathcal{N}$ represent $\frac{\mathcal{A}^k_{|B|} - |B|}{\sqrt{\frac{1}{k} Var(|\widehat{B}|)}}$. The accuracy requirement $P\{|\mathcal{A}^k_{|B|} - |B|| \leq \alpha|T|\} \geq \beta$ can be transformed, as seen below.

$$Pr\left\{ \frac{-\alpha|T|}{\sqrt{\frac{1}{k} Var(|\widehat{B}|)}} \leq \mathcal{N} \leq \frac{\alpha|T|}{\sqrt{\frac{1}{k} Var(|\widehat{B}|)}} \right\} \geq \beta \quad (21)$$

By the central limit theorem, $\mathcal{N}$ approximates a standard normal distribution, and its cumulative distribution function is denoted as Φ. We can find a constant ε such that $Pr\{-\varepsilon \leq \mathcal{N} \leq \varepsilon\} = \Phi(\varepsilon) - \Phi(-\varepsilon) = \text{erf}(\frac{\varepsilon}{\sqrt{2}}) = \beta$. Here, erf$(\cdot)$ is the standard error function. By solving this equation, we get $\varepsilon = \text{erf}^{-1}(\beta)$. For example, if $\beta = 99\%$, $\varepsilon = 2.576$. To ensure the probability in Eq. (21), we only need to guarantee the following inequalities.

$$\frac{\alpha|T|}{\sqrt{\frac{1}{k} Var(|\widehat{B}|)}} \geq \text{erf}^{-1}(\beta) \quad (22)$$

Substituting the expression of $Var(|\widehat{B}|)$ into the above inequalities and solving them, we know that the value of k should be no less than k_B in Eq. (19). Similarly, to ensure that $\mathcal{A}^k_{|U|}$ meets the required (α, β) accuracy, value of k should be no less than k_U in Eq. (20). Then, we know that k should be no less than $\max\{k_B, k_U\}$. □

3.3 Parameter Optimization: Minimizing the Maximum

In the following, we will optimize the values of the broadcasted frame size f and the executed frame size f' to minimize the estimation time of the proposed *SEBU*. Let $\mathcal{T}_{SE}$ be the time cost of *SEBU*. According to Theorems 2, we have $\mathcal{T}_{SE} = \max\{\mathcal{T}_B, \mathcal{T}_U\}$, where $\mathcal{T}_B = k_B(t_{qry} + f' t_{rn})$ and $\mathcal{T}_U = k_U(t_{qry} + f' t_{rn})$. The detailed expressions of $\mathcal{T}_B$ and $\mathcal{T}_U$ are calculated as follows:

$$\mathcal{T}_B = \frac{\{\text{erf}^{-1}(\beta)\}^2 (t_{qry} + f' t_{rn})}{\alpha^2 |T|^2 f'} \left(|T-B|^2 + f|T-B|\right) e^{\frac{|T+U|}{f}} \quad (23)$$

$$\mathcal{T}_U = \frac{\{\text{erf}^{-1}(\beta)\}^2 f^2 (t_{qry} + f' t_{rn})}{\alpha^2 |T|^2 f'} \left(e^{\frac{|T+U|}{f}} - 1 \right) \quad (24)$$

Optimize the value of f'. We fix the value of f, and investigate the optimization of f'. Theorem 3 infers that the execution time of *SEBU* is a monotonously decreasing function of the executed frame size f'. Therefore, f' should be set as large as possible. Since the executed frame size f' is limited by the broadcasted frame size f and 512, we set $f' = \min\{f, 512\}$. In large-scale RFID systems that contain thousands of tags, the broadcasted frame size f should be large accordingly, otherwise there will be a lot of collision slots in the frame, which is obviously not conducive to *SEBU*. For simplicity, we assume that the broadcasted frame size f is larger than 512. Then, *SEBU* simply sets f' to 512 without otherwise specified.

Theorem 3. *Given that a required confidence interval* α*, a required reliability* β*, a broadcasted frame size* f*, and an executed frame size* f'*; the total time cost of SEBU* $\mathcal{T}_{SE} = \max\{\mathcal{T}_B, \mathcal{T}_U\}$ *is a monotonously decreasing function of* f'*.*

Proof. We give the first order derivatives $\frac{\partial \mathcal{T}_B}{\partial f'}$ and $\frac{\partial \mathcal{T}_U}{\partial f'}$ below:

$$\begin{aligned} \frac{\partial \mathcal{T}_B}{\partial f'} &= -\frac{\{\text{erf}^{-1}(\beta)\}^2 t_{qry} \left(|T-B|^2 + f|T-B|\right) e^{\frac{|T+U|}{f}}}{f'^2 \alpha^2 |T|^2} \\ \frac{\partial \mathcal{T}_U}{\partial f'} &= -\frac{\{\text{erf}^{-1}(\beta)\}^2 f^2 t_{qry}}{f'^2 \alpha^2 |T|^2} \left(e^{\frac{|T+U|}{f}} - 1 \right) \end{aligned} \quad (25)$$

We observe from Eq. (25) that $\frac{\partial \mathcal{T}_B}{\partial f'}$ and $\frac{\partial \mathcal{T}_U}{\partial f'}$ are always less than 0, which infers that both $\mathcal{T}_B$ and $\mathcal{T}_U$ are monotonously decreasing function of f'. Then, we assert that $\max\{\mathcal{T}_B, \mathcal{T}_U\}$ is still a monotonously decreasing functions of f'. □

Optimize the value of f. Next, we will optimize the value of the broadcasted frame size f to minimize the time cost $\mathcal{T}_{SE} = \max\{\mathcal{T}_B, \mathcal{T}_U\}$. We obviously can use the exhausting searching method to find the optimal value for the broadcasted frame size f. However, such a straightforward method begets high complexity. In the following, Theorem 4 proves that $\mathcal{T}_{SE}$ is a convex function of f. Here, we conduct a set of simulations as illustrated in Fig. 5. The specific simulation settings are as follows. In Fig. 5(a), we set the $|T| = 9000$, $|U| = 1000$, and $|B| = 95\%|T| = 8500$; and in Fig. 5(b), we set the $|T| = 5000$, $|U| = 5000$, and $|B| = 50\%|T| = 2500$. We can observe from the simulation results that the execution time of *SEBU* $\mathcal{T}_{SE} = \max\{\mathcal{T}_B, \mathcal{T}_U\}$ is indeed a convex function with respect to the broadcasted frame size f, which coincides with the statement claimed in the Theorem 4. By the convex property, we propose a binary-search algorithm to find the optimal f that minimizes $\mathcal{T}_{SE} = \max\{\mathcal{T}_B, \mathcal{T}_U\}$. First, we initialize f_{low} to f', and f_{high} to $3|T+U|$. We have observed through simulations that $3|T+U|$ is a good upper bound on the broadcasted frame size. Second, we calculate the first-order derivative of $\max\{\mathcal{T}_B, \mathcal{T}_U\}$ at $\frac{f_{low}+f_{high}}{2}$. If this derivative is less than 0, it updates f_{low} to $\frac{f_{low}+f_{high}}{2}$; otherwise, it updates f_{high} to $\frac{f_{low}+f_{high}}{2}$. The algorithm recursively performs this search until $f_{low} = f_{high}$, at which point it stops and returns the value of f as $f = f_{low} = f_{high}$.

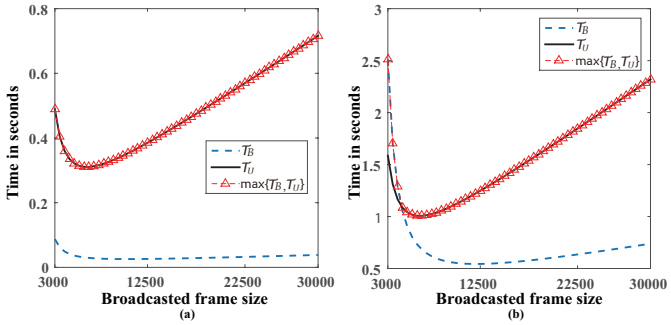


Fig. 5. Impact of the broadcast frame size f on the time cost of *SEBU*. $(\alpha, \beta) = (0.1, 90\%)$. (a) $|T| = 5000$, $|U| = 5000$, $|B| = 2500$; (b) $|T| = 9000$, $|U| = 1000$, $|B| = 8500$.

Theorem 4. *Given that a required confidence interval* α*, a required reliability* β*, a broadcasted frame size* f*, and an executed frame size* f'*; the total time cost of SEBU* $\mathcal{T}_{SE} = \max\{\mathcal{T}_B, \mathcal{T}_U\}$ *is a convex function of* f*.*

Proof. We calculate the second-order derivative $\frac{\partial^2 \mathcal{T}_B}{\partial f^2}$ below:

$$\frac{\partial^2 \mathcal{T}_B}{\partial f^2} = \frac{\left\{\text{erf}^{-1}(\beta)\right\}^2 (t_{qry}+f' t_{rn})|T+U| \cdot |T-B| e^{\frac{|T+U|}{f}}}{\alpha^2 |T|^2 f' f^3} \times \left(\frac{|T-B| \cdot |T+U|}{f} + |U| + 3|T| - 2|B| \right) \tag{26}$$

We observe from Eq. (26) that $\frac{\partial^2 \mathcal{T}_B}{\partial f^2}$ is always larger than 0, hence, $\mathcal{T}_B$ is a convex function of f. Similarly, we calculate the second-order derivatives $\frac{\partial^2 \mathcal{T}_U}{\partial f^2}$ below:

$$\frac{\partial^2 \mathcal{T}_U}{\partial f^2} = \frac{\left\{\text{erf}^{-1}(\beta)\right\}^2 (t_{qry}+f' t_{rn})}{f' \alpha^2 |T|^2} \times \aleph, \text{ where } \aleph = e^{\frac{|T+U|}{f}} \left(\frac{|T+U|^2}{f^2} - \frac{2|T+U|}{f} + 2 \right) - 2 \tag{27}$$

Using the fourth-order Taylor series expansion, we have:

$$e^{\frac{|T+U|}{f}} > 1 + \frac{|T+U|}{f} + \frac{|T+U|^2}{2f^2} + \frac{|T+U|^3}{6f^3} + \frac{|T+U|^4}{24f^4} \tag{28}$$

Note that, $\frac{|T+U|^2}{f^2} - \frac{2|T+U|}{f} + 2$ in Eq. (27) is always larger than 0 because it can be transformed as $\left(\frac{|T+U|}{f} - 1\right)^2 + 1$. Substituting $e^{\frac{|T+U|}{f}}$ with its fourth-order Taylor series expansion in Eq. (28) and rearranging, we have:

$$\frac{\partial^2 \mathcal{T}_U}{\partial f^2} = \frac{\left\{\text{erf}^{-1}(\beta)\right\}^2 (t_{qry}+f' t_{rn})}{f' \alpha^2 |T|^2} \left(\frac{|T+U|^3}{3f^3} + \frac{|T+U|^4}{4f^4} + \frac{|T+U|^5}{12f^5} + \frac{|T+U|^6}{24f^6} \right) \tag{29}$$

We observe that $\frac{\partial^2 \mathcal{T}_U}{\partial f^2} > 0$, which infers that $\mathcal{T}_U$ is a convex function of f. Since both $\mathcal{T}_B$ and $\mathcal{T}_U$ are convex functions of f, $\max\{\mathcal{T}_B, \mathcal{T}_U\}$ is also a convex function of f. □

Here, we need to emphasize that the proposed *AF+PL+SEBU* protocol works efficiently only when the ratio of blocked tags is small. The underlying reason is explained as follows. we conducted two new sets of simulations, one for a small-scale RFID system in which $|T| = 2000$, $|U| = 2000$, and the ratio of blocked target tags varies from 0% to 100%; the other for a large-scale RFID system in which $|T| = 20000$, $|U| = 20000$, and the ratio of blocked target tags also varies from 0% to 100%. We observed from the simulation results in Fig. 6 (a) and (b) that, the time cost of the proposed *AF+PL+SEBU* protocol gets close to (or even a little higher than) that of the *PL* protocol as the ratio of blocked tags increases. We use a special example to explain the underlying reasons. For example, if the ratio of blocked tags is 100%, *i.e.*, all target tags are blocked. We cannot benefit from the *AF* protocol, because there is no non-blocked target tags at all. Hence, the *AF+PL* protocol degenerate into the *PL* protocol. Recall that, we need to execute the *SEBU* protocol to estimate the sizes of B and U at the every beginning, for the purpose of determining how many rounds of *AF* should be executed before invoking the *PL* protocol. When the ratio of blocked target tags is 100%, the *AF* protocol will not be invoked. Therefore, the actual time cost of *AF+PL+SEBU* is equal to that of *PL+SEBU*, which will be a bit higher than that of directly running *PL*. Hence, the proposed *AF+PL+SEBU* protocol is not always efficient. It is only quite efficient when the ratio of blocked tags is relatively small.

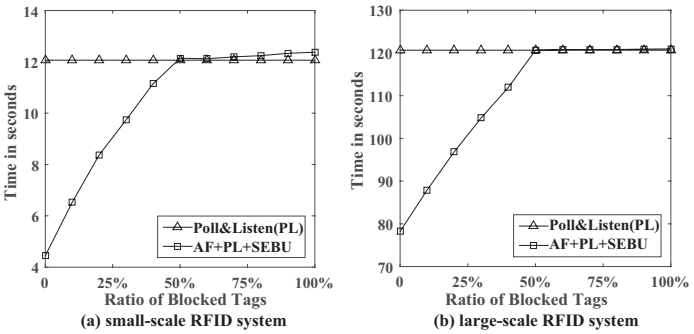


Fig. 6. Investigating the impact of blocking ratio on the performance of the proposed protocol. (b) $|T| = 2,000$, $|U| = 2,000$; (b) $|T| = 20,000$, $|U| = 20,000$.

4 Performance Evaluation

We use Matlab to implement *AF+PL+SEBU* as well as two prior state-of-the-art protocols, *i.e.*, *Tree Hopping* and *S-BID*. Unlike *AF+PL+SEBU* and *S-BID*, *Tree Hopping* is sensitive to the distribution of tag IDs, and it works well when the tag IDs are uniformly distributed. For its sake, we simulate the tag IDs following uniform distribution, *i.e.*, each bit of the tag ID string has a 50/50 chance of being 0 or 1. The slot length settings are based on the transmission rate specified in the RFID standard. It takes 18.9*us* to transmit one bit from the tag to the reader (uplink rate is 53*Kb/s*); 37.7*us* to transmit 1 bit from the reader to the tag (downlink rate is 26.5*Kb/s*). Besides, it requires a waiting time 302*us* [29] between any two consecutive data transmissions from the reader to the tags and vice versa. Our protocol can work seamlessly in single as well as multi-reader environments, we simulate a single reader here following the benchmark literature. For clarity, we consider an error-free communication channel [15], [44]. Extensive simulations are conducted to evaluate the identification accuracy and time-efficiency of the protocols. Each numerical result is averaged from 500 independent simulations.

4.1 Impact of Number of Unknown Tags

With varying value of $|U|$, AF+PL+SEBU is the fastest protocol among all the protocols that can identify the blocked tags with no false positive. The actual time cost of AF+PL+SEBU is very close to its optimal theory value. Figs. 7(a)(b) are plotted using $|T| = 20000$, $|B| = 500$, and $|U|$ varies from 0 to 20000. We observe from Fig. 7(a) that *S-BID* identifies the blocked tags with no false positive only when there is no unknown tags (*i.e.*, $|U| = 0$). As the number of unknown tags $|U|$ increases, the false positive probability of *S-BID* sharply increases. The underlying reason is that an expected singleton slot of an unblocked target tag is more likely to be changed into a collision slot when there are more unknown tags. Except for *S-BID*, the other protocols can identify the blocked tags with no false positive.

The time cost of *Tree Hopping* increases with respect to $|U|$ because it needs to identify more tags. The time cost of *PL* remains stable because the number of target tags that need to be queried (*i.e.*, $|T|$) does not change. The time cost of *AF+PL+SEBU* also increases against $|U|$ because the unknown tags hinder the verification of unblocked target tags, which begets more time frames to filter out the unblocked target tags. Here, the accuracy of *SEBU* is set to $(0.1, 90\%)$, which is sufficient to guide the optimization of *AF+PL* according to the following observations. The simulation results demonstrate that our *AF+PL+SEBU*

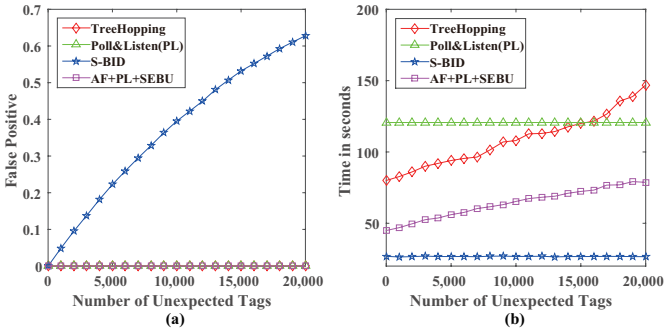


Fig. 7. Impact of the unknown tag size $|U|$ on the protocols. (a) False positive vs. $|U|$. (b) Execution time vs. $|U|$. $|T| = 20000$, $|B| = 500$.

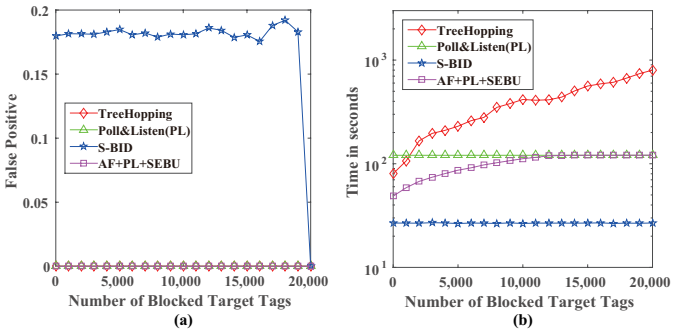


Fig. 8. Impact of the blocked tag size $|B|$ on the protocols. (a) False positive vs. $|B|$. (b) Execution time vs. $|B|$. $|T| = 20000$, $|U| = 4000$.

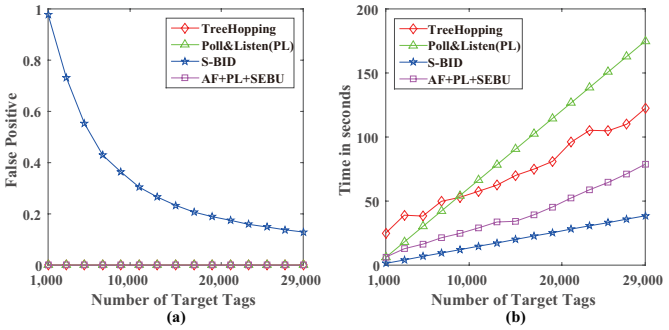


Fig. 9. Impact of the target tag size $|T|$ on the protocols. (a) False positive vs. $|T|$. (b) Execution time vs. $|T|$. $|B| = 500$, $|U| = 4000$.

protocol outperforms the the *Tree Hopping* and *PL* protocols by significantly reducing the execution time. For example, when $|U| = 20000$, the execution time of *Tree Hopping* and *PL* is 147 seconds and 120 seconds, respectively. And the execution time of *AF+PL+SEBU* is just 78 seconds, representing a reduction of 47% and 35% when compared with the *Tree Hopping* and *PL* protocols, respectively. In what follows, we will explain why our *AF+PL+SEBU* scheme is better than the existing schemes, *e.g.*, *TreeHopping*, and *Poll&Listen(PL)*. Intuitively, *TreeHopping* needs the reader to send multiple long prefix strings (nearly or exactly 96-bit) to determine whether a target tag is blocked or not. *Poll&Listen(PL)* needs the reader to send 96-bit tag ID to determine whether a target tag is blocked or not. Compared with *TreeHopping* and *Poll&Listen(PL)*, our *AF+PL+SEBU* only needs small transmission cost (just 10-bit) to determine most of the non-blocked target tags. And only a small subset of target tags need to use the heavy *PL* protocol to determine whether they are blocked or not. Hence, our *AF+PL+SEBU* protocol is better than the above two mentioned protocols.

4.2 Impact of Number of Blocked Tags

With varying value of $|B|$, AF+PL+SEBU is the fastest protocol among all the protocols that can identify the blocked tags with no false positive when the blocked tag ratio $|B|/|T|$ is small. The performance of AF+PL+SEBU goes back to PL when the blocked tag ratio $|B|/|T|$ is large. Figs. 8(a)(b) are plotted using $|T| = 20000$, $|U| = 4000$, and $|B|$ varies from 0 to 20000. We observe from Fig. 8(a) that *S-BID* consistently suffers from a false positive error when $|B| < |T|$ due to the existence of unknown tags. An interesting observation is that the false positive of *S-BID* seemingly equals 0 when $|B| = |T|$. The reason of this illusion is as follows. False positive occurs when any unblocked target tags are identified as blocked tags. However, when $|B| = |T|$ (*i.e.*, all target tags are blocked), the false positive has no way of happening. Except for *S-BID*, the other protocols are of no false positive.

The execution time of *Tree Hopping* sharply increases with respect to the number of blocked tags because the existence of blocked tags incurs a large number of collision tag querying. For example, when $|B| = 20000$, the execution time of *Tree Hopping* is nearly 800 seconds. From Fig. 8(b), we can also observe that *AF+PL+SEBU* runs faster than *PL* when the number of blocked tags $|B|$ is relatively small. On the contrary, when the number of blocked tags $|B|$ is relatively large, the execution time of *AF+PL+SEBU* is almost the same as that of *PL*. The underlying reason is elaborated as follows. When the blocked tag ratio $\frac{|B|}{|T|}$ is small, the *AF* scheme can efficiently filter out a large fraction of the unblocked target tags, the effectiveness of *AF* is well highlighted and the time of *AF+PL* is smaller than *PL*. On the contrary, when $\frac{|B|}{|T|}$ is relatively large, the time cost of performing *AF* will overwhelm the brought benefits, and thus, it is time-efficient to directly invoke the *PL* protocol. As a result, *AF+PL+SEBU* goes back to *PL* when $|B|$. We observe from Fig. 8(b) that the time cost of *AF+PL+SEBU* is just a bit larger than *PL* due to the small amount of time taken by *SEBU*. The above observations also demonstrate that *AF+PL+SEBU* can flexibly gear the Aloha frame number n according to the blocked tag ratio.

4.3 Impact of Number of Target Tags

With varying value of $|T|$, the AF+PL+SEBU is the fastest protocol among all the protocols that can identify the blocked tags with 100% accuracy. Figs. 9(a)(b) are plotted using $|B| = 500$, $|U| = 4000$, and $|T|$ varies from 1000 to 29000. We observe from Fig. 9(a) that the false positive of S-BID decreases as the number of target tags $|T|$ increases. The underlying reason is elaborated as follows. Recall that the false positive of *S-BID* occurs when the expected singleton slots picked by unblocked target tags are also picked by the unknown tags. Since the number of unknown tags $|U|$ is fixed to 4000, increasing the value of $|T|$ means that more expected singleton slots of unblocked target tags will not be covered by the unknown tags, and then the false positive will decrease. Except for *S-BID*, the other protocols are of no false positive.

As the number of target tags $|T|$ increases, the execution time of all the concerned protocols increase because more tags are required to be tackled. Specifically, *Tree Hopping* needs to identify more tags; *S-BID* needs to devote more slots to ensure that each target tag picks the expected singleton slots once; *PL* needs to poll more target tags; *AF+PL+SEBU* needs to

filter out more unblocked target tags before performing the *PL* protocol. We observe that, except for *S-BID* that suffers from false positive, *AF+PL+SEBU* is the fastest protocol. For example, when $|T| = 29000$, the time cost of *Tree Hopping* and *PL* is 122.4 seconds and 174.9 seconds, respectively. The time cost of *AF+PL+SEBU* is just 78.8 seconds, representing the time reduction of 35.6% and 54.9%, respectively.

4.4 Drawbacks of *AF+PL+SEBU*

Although the proposed *AF+PL+SEBU* protocol shows significant improvement over the existing protocol under some conditions, it may have drawbacks under some specific scenarios. In the following, we discuss the drawbacks of our *AF+PL+SEBU* protocol from two perspectives. First, The simulation results in Fig. 7 reveal that, when $|U| = 0$, the S-BID protocol [27] will not suffer any false positive, meanwhile running much faster than our *AF+PL+SEBU* protocol. Hence, in the scenario where the users are aware of each tag ID, we should suggest the users choose the S-BID protocol instead of our *AF+PL+SEBU* protocol. Second, in the system that contains unexpected tags, the *S-BID* protocol [27] suffers from false positive. In fact, we can execute *S-BID* for multiple rounds to reduce the false positive. Specifically, a non-blocked tag may be mistakenly recognized as the blocked one (*i.e.*, false positive happens) in a round of S-BID, but it has a chance to be correctly recognized as the non-blocked one in the other rounds of *S-BID*. And a target tag is eventually recognized as the blocked one only when *S-BID* always asserts that it is blocked in *each* round. We conducted a new set of simulations to investigate the impact of round count of *S-BID* on its final false positive and time cost. We can observe from the simulation results in Fig. 10 that, as the round count of *S-BID* increases, its final false positive decreases and its time cost increases linearly. For example, if we require that the false positive ratio should be no more than 0.1, we need to execute *S-BID* for 5 rounds at least, and the corresponding time cost are more than 120 seconds. But if we use the *AF+PL+SEBU* protocol, it only costs 81 seconds. In this case, we suggest the users choose our *AF+PL+SEBU* protocol. In contrary, if we do not have too much requirement on the false positive ratio (*e.g.*, a false positive ratio of 0.4 is fine), the time cost of *S-BID* is just 50 seconds, which is much smaller than that of our *AF+PL+SEBU* protocol. In this case, we will suggest the use of S-BID protocol.

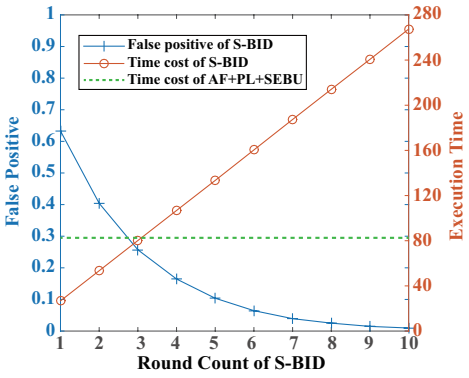


Fig. 10. Performance comparison: *AF+PL+SEBU vs. S-BID*. $|T| = 20,000$, $|U| = 20,000$, $|B| = 1,000$.

4.5 Energy-efficiency for Active RFID tags

There are two types of tags: passive tags that do not have their own power sources and are powered up by harvesting the radio frequency energy from readers, and active tags that have their own power sources. The proposed protocol, which can be used for passive RFID systems, can be definitely used for active RFID systems because active tags have better computation/communication capabilities than the passive tags. For active RFID tags, we need to consider *energy-efficiency*, which is important to ensure long service time. Since battery of a reader can be easily recharged or the reader may even use an external power source, the energy consumed by the reader is ignored in this paper. We only consider the energy consumption of the battery-powered active tags, particularly, the target tags. An active tag has two types of states: awake state (*i.e.*, its CPU works at full energy and the radio remains active) and sleep state. A target tag, which has not been determined blocked (or non-blocked), should keep in awake state for communication until it is determined. When a tag is awake, we use ω to denote the consumed energy per second. We conducted simulations to compare the proposed *AF+PL+SEBU* and *Poll&Listen(PL)* in terms of energy-efficiency. The results in Fig. 11 reveal that the proposed *AF+PL+SEBU* significantly outperforms *Poll&Listen(PL)* under different conditions.

5 Related Work

One of the most important functionalities in RFID systems is tag identification, which is to use the reader to identify the tag IDs of a given set of tags. In the infancy stage of RFID research, a great deal of effort was devoted to the identification of RFID tags. The existing solutions can be generally classified into two categories: Aloha-based approaches [20] and tree-based approaches [19]. The Aloha-based protocol is a kind of Time Division Multiple Access (TDMA) mechanism. The reader broadcasts a value f to the tags in its interrogation range where f indicates the number of slots in the forthcoming time frame. Then, each tag randomly picks a time slot in the frame and responds during that slot. In any slot, if one and only one tag responds, the reader is able to successfully identify this tag. If two tags respond simultaneously in a slot, the reader cannot derive any tag IDs due to signal corruption. The unidentified tags will participate in the next frame. Such an iterative identification process will not terminate until all the tags are identified. Quan *et al.* indicated that the identification efficiency is maximized when the frame size is equal to the number of tags that participate in the current frame [45]. The tree-based protocol is also a fundamental multiple access protocol, which was first invented by U.S. Army for testing soldiers for syphilis during World War II [46]. In the tree-based protocol, the reader first queries 0 and all the tags whose IDs start with 0 respond with their IDs. If the reader successfully identifies a tag (*i.e.*, only one tag responds) or just reads an empty slot (*i.e.*, no tag responds), it queries 1 and all the tags whose IDs start with 1 respond. On the contrary, if the reader senses a collision, which means that there are two or more tags whose IDs start with 0, it generates two new query strings ***0 and ***1 by appending a 0 and a 1 to the previous query string ***. Then, the reader sequentially uses these two strings to query the tags. This process continues until all the tags have been identified. The tree-based protocols can be interpreted as a depth-first-search query mechanism.

Privacy concerns have been raised about the widely used RFID tags, because the C1G2-compliant RFID tags broadcast their ID

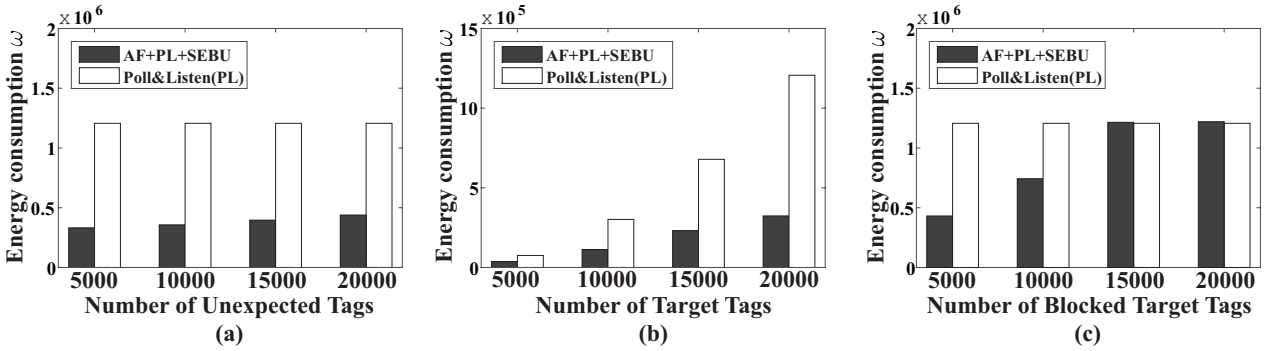


Fig. 11. Investigating energy-efficiency of proposed protocol under different tag ratio for active RFID tags. (a) varying unknown tag size $|U|$. (b) varying blocked tag size $|B|$. (c) varying target tag size $|T|$.

serial numbers to any nearby reader, regardless whether the reader is authorized [34]. The risk we face is that the privacy information embedded in the RFID tags, *e.g.*, dress size, medicine brand, may be eavesdropped by attackers. To prevent from malicious interrogations, an effective solution is to use the commercially available *blocker tag* [47], [48]. Liu *et al.* investigated classical RFID estimation problem for privacy-sensitive scenarios where blocker tags are used to protect the privacy of tagged items [42].

Every coin has two sides. The blocker tag can also be used by attackers to mount denial-of-service (DoS) attacks against RFID systems [34]. The malicious blocker tag can prevent the legitimate readers from querying information from the RFID tags. Ehsan Vahedi *et al.* proposed a probabilistic blocker tag detection (P-BTD) algorithm to detect the presence of an attacker in the RFID system [34]. However, we think the boolean answer (yes or no) returned by such a detection protocol is insufficient because we sometimes want to exactly know which tags are blocked so as to accurately measure the adverse affect of the blocking attacks on the RFID system. Wang *et al.* focused on identifying the blocking range for tree-based RFID systems. However, the most popular C1G2 standard adopts the framed slotted Aloha mechanism [35]. The work closest to ours is [27] that investigated the cloned tag identification. The cloned tags are replicated from the valid tags and have the same IDs as valid tags. It seems that we can borrow their solutions to address the problem of blocked tag identification defined in this paper. Unfortunately, they made an unrealistic assumption that all the valid tag IDs should be known apriori, which is not true as we have exemplified. Extensive simulation results demonstrated that their solutions are of serious false positives with the existence of unknown tags. Through a comprehensive overview of the previous literature, we did not find any existing RFID protocols that can well address the problem of blocked tag identification for Aloha-based RFID systems.

A fact is that the existing RFID solutions [19], [29] are designed either for the Aloha-based RFID systems or binary tree walking RFID systems. Since the most popular EPC C1G2 RFID standard exploits the Aloha-based MAC layer communication mechanism, this paper aims at proposing a blocking identification protocol for Aloha-based RFID systems.

6 Conclusion

This paper makes the following four key contributions. First, we formulate a new practical problem of blocked tag identification with the presence of unknown tags that usually appear in practice. Second, we propose a hybrid approach that jointly uses two complementary protocols called *Aloha Filtering (AF)* and *Poll&Listen (PL)*. The technical novelty is in investigating the frame count repeated by *AF* that trades off between the time costs of *AF* and *PL*. Third, the optimization of *AF+PL* requires the sizes of blocked target set and unknown tag set, which, however, are not known in advance. Hence, we propose the protocol called *Simultaneous Estimation of the Blocked tag size and the Unknown tag size (SEBU)*. The technical depth is in finding the optimal frame size to minimize the maximum time of estimating these two set sizes. The proposed approach is compliant with the C1G2 standard. It does not require any modifications to be made to the commercial RFID tags, and only needs to be installed on readers as a software module. Finally, extensive simulations are conducted to evaluate the performance of the proposed approach. The simulation results reveal that *AF+PL+SEBU* can identify the blocked tags with an accuracy of 100%, and significantly reduces the execution time when compared with the state-of-the-art protocols.

Acknowledgment

This work is supported by the National Key Research and Development Program of China No. 2016YFB1000205; the State Key Program of National Natural Science of China under Grant 61432002; the NSFC under Grant Numbers U1701262, 61672379, 61772112, 61370199 and 61702365; the Dalian High-level Talent Innovation Program under Grant 2015R049; the Natural Science Foundation of Tianjin under Grant 17JCQNJC00700; the Strategic Information and Communications R&D Promotion Programme (SCOPE No.162302008), MIC, Japan; NSF grants CNS 1629746, CNS 1564128, CNS 1449860, CNS 1461932, CNS 1460971, CNS 1439672, and CNS 1301774.

References

[1] K. Xie, X. Wang, J. Wen, and J. Cao, "Cooperative Routing with Relay Assignment in Multi-radio Multi-hop Wireless Networks," *IEEE/ACM Transactions on Networking*, vol. 24, no. 2, pp. 859–872, 2016.

[2] X. Liu, J. Cao, K. Li, J. Liu, and X. Xie, "Range Queries for Sensor-augmented RFID Systems," *Proc. of IEEE INFOCOM*, 2018.

[3] T. Qiu, R. Qiao, M. Han, A. K. Sangaiah, and I. Lee, "A Lifetime-Enhanced Data Collecting Scheme for Internet of Things," *IEEE Communications Magazine*, vol. 55, no. 11, pp. 132–137, 2017.

[4] X. Liu, K. Li, A. X. Liu, S. Guo, A. L. Wang, X. Xie, and J. Wu, "Multi-category RFID Estimation," *IEEE/ACM Transactions on Networking*, vol. 25, no. 5, pp. 264–277, 2017.

[5] K. Xie, X. Wang, X. Liu, J. Wen, and J. Cao, "Interference-aware Cooperative Communication in Multi-radio Multi-channel Wireless Networks," *IEEE Transactions on Computers*, vol. 65, no. 5, pp. 1528–1542, 2016.

[6] X. Liu, K. Li, S. Guo, A. X. Liu, P. Li, K. Wang, and J. Wu, "Top-k Queries for Categorized RFID Systems," *IEEE/ACM Transactions on Networking*, vol. 25, no. 5, pp. 2587–2600, 2017.

[7] T. Qiu, R. Qiao, and D. O. Wu, "EABS: An Event-Aware Backpressure Scheduling Scheme for Emergency Internet of Things," *IEEE Transactions on Mobile Computing*, vol. 17, no. 1, pp. 72–84, 2018.

[8] K. Xie, X. Ning, X. Wang, D. Xie, J. Cao, G. Xie, and J. Wen, "Recover Corrupted Data in Sensor Networks a Matrix Completion Solution," *IEEE Transactions on Mobile Computing*, vol. 16, no. 5, pp. 1434–1448, 2017.

[9] X. Liu, K. Li, J. Wu, A. X. Liu, X. Xie, C. Zhu, and W. Xue, "TOP-k Queries for Multi-category RFID Systems," *Proc. of IEEE INFOCOM*, 2016.

[10] T. Qiu, A. Zhao, F. Xia, W. Si, and D. O. Wu, "ROSE: Robustness Strategy for Scale-Free Wireless Sensor Networks," *IEEE/ACM Transactions on Networking*, vol. 25, no. 5, pp. 2944–2959, 2017.

[11] 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*, vol. 25, no. 1, pp. 224–237, 2017.

[12] L. Kong, L. He, Y. Gu, M.-Y. Wu, and T. He, "A Parallel Identification Protocol for RFID Systems," *Proc. of IEEE INFOCOM*, 2014.

[13] 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, no. 1, pp. 278–291, 2017.

[14] Y. Shu, P. Cheng, Y. Gu, J. Chen, and T. He:, "Minimizing communication delay in RFID-based wireless rechargeable sensor networks," *Proc. of IEEE SECON*, 2014.

[15] W. Gong, K. Liu, X. Miao, Q. Ma, Z. Yang, and Y. Liu, "Informative Counting: Fine-grained Batch Authentication for Large-Scale RFID Systems," *Proc. of ACM MobiHoc*, 2013.

[16] L. Shangguan, Z. Yang, A. X. Liu, Z. Zhou, and Y. Liu, "Relative Localization of RFID Tags using Spatial-Temporal Phase Profiling," *Proc. of USENIX NSDI*, 2015.

[17] 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," *Proc. of ACM MobiCom*, 2014.

[18] "http://www.idtechex.com/research/reports/rfid-forecasts-players-and-opportunities-2014-2024-000368.asp."

[19] M. Shahzad and A. X. Liu, "Probabilistic optimal tree hopping for rfid identification," *IEEE/ACM Transactions on Networking*, vol. 23, no. 3, pp. 796–809, 2015.

[20] S.-R. Lee, S.-D. Joo, and C.-W. Lee, "An Enhanced Dynamic Framed Slotted ALOHA Algorithm for RFID Tag Identification," *Proc. of ACM MobiQuitous*, 2005.

[21] J. Myung and W. Lee, "Adaptive splitting protocols for RFID tag collision arbitrationn," *Proc. of ACM MobiHoc*, 2006.

[22] C. Qian, H. Ngan, Y. Liu, and L. M. Ni, "Cardinality Estimation for Large-scale RFID Systems," *IEEE Transactions on Parallel and Distributed Systems*, vol. 22, no. 9, pp. 1441–1454, 2011.

[23] B. Chen, Z. Zhou, and H. Yu, "Understanding RFID Counting Protocols," *Proc. of ACM MobiCom*, 2013.

[24] B. Sheng, C. C. Tan, Q. Li, and W. Mao, "Finding Popular Categories for RFID Tags," *Proc. of ACM Mobihoc*, 2008.

[25] T. Li, S. Chen, and Y. Ling, "Efficient Protocols for Identifying the Missing Tags in a Large RFID System," *IEEE/ACM Transactions on Networking*, vol. 21, no. 6, pp. 1974–1987, 2013.

[26] C. C. Tan, B. Sheng, and Q. Li, "Efficient techniques for monitoring missing rfid tags," *IEEE Transactions on Wireless Communications*, vol. 9, no. 6, pp. 1882–1889, 2010.

[27] K. Bu, X. Liu, and B. Xiao, "Fast Cloned-Tag Identification Protocols for Large-Scale RFID Systems," *Proc. of IEEE IWQOS*, 2012.

[28] L. Yang, J. Han, Y. Qi, and Y. Liu, "Identification Free Batch Authentication for RFID Tags," *Proc. of IEEE ICNP*, 2010.

[29] M. Shahzad and A. X. Liu, "Fast and Accurate Estimation of RFID Tags," *IEEE/ACM Transactions on Networking*, vol. 23, no. 1, pp. 241–254, 2015.

[30] X. Liu, K. Li, G. Min, K. Lin, B. Xiao, Y. Shen, and W. Qu, "Efficient Unknown Tag Identification Protocols in Large-Scale RFID Systems," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 12, pp. 3145–3155, 2014.

[31] M. Shahzad and A. X. Liu, "Expecting the Unexpected: Fast and Reliable Detection of Missing RFID Tags in the Wild," *Proc. of IEEE INFOCOM*, 2015.

[32] X. Liu, K. Li, G. Min, Y. Shen, A. X. Liu, and W. Qu, "Completely Pinpointing the Missing RFID Tags in a Time-Efficient Way," *IEEE Transactions on Computers*, vol. 64, no. 1, pp. 87–96, 2015.

[33] W. Luo, S. Chen, T. Li, and Y. Qiao, "Probabilistic Missing-tag Detection and Energy-Time Tradeoff in Large-scale RFID Systems," *Proc. of ACM MobiHoc*, 2012.

[34] E. Vahedi, V. Shah-Mansouri, V. W. S. Wong, I. F.Blake, and R. K. Ward, "Probabilistic Analysis of Blocking Attack in RFID Systems," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 3, pp. 803–817, 2011.

[35] F. Wang, B. Xiao, K. Bu, and J. Su, "Detect and Identify Blocker Tags in Tree-based RFID Systems," *Proc. of IEEE ICC*, 2013.

[36] W. Luo, S. Chen, T. Li, and S. Chen, "Efficient Missing Tag Detection in RFID Systems," *Proc. of IEEE INFOCOM*, 2011.

[37] Y. Zheng and M. Li, "Fast Tag Searching Protocol for Large-Scale RFID Systems," *IEEE/ACM Transactions on Networking*, vol. 21, no. 3, pp. 924–934, 2013.

[38] L. Yang, Q. Lin, C. Duan, and Z. An, "Analog On-Tag Hashing: Towards Selective Reading as Hash Primitives in Gen2 RFID Systems," *Proc. of ACM Mobicom*, 2017.

[39] L. Yang, J. Han, Y. Qi, C. Wang, T. Gux, and Y. Liu, "Season: Shelving Interference and Joint Identification in Large-Scale RFID Systems," *Proc. of IEEE INFOCOM*, 2011.

[40] Y. Zheng and M. Li, "PET: Probabilistic Estimating Tree for Large-scale RFID Estimation," *IEEE Transactions on Mobile Computing*, vol. 11, no. 11, pp. 1763–1774, 2012.

[41] H. Han, B. Sheng, C. C. Tan, Q. Li, W. Mao, and S. Lu, "Counting RFID Tags Efficiently and Anonymously," *Proc. of IEEE INFOCOM*, 2010.

[42] X. Liu, B. Xiao, K. Li, J. Wu, A. X. Liu, H. Qi, and X. Xie, "RFID Cardinality Estimation with Blocker Tags," *Proc. of IEEE INFOCOM*, 2015.

[43] X. Liu, K. Li, H. Qi, B. Xiao, and X. Xie, "Fast Counting the Key Tags in Anonymous RFID Systems," *Proc. of IEEE ICNP*, 2014.

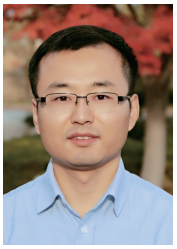
[44] L. Xie, H. Han, Q. Li, J. Wu, and S. Lu, "Efficient Protocols for Collecting Histograms in Large-Scale RFID Systems," *IEEE Transactions on Parallel and Distributed Systems*, vol. 26, no. 9, pp. 2421–2433, 2015.

[45] C.-H. Quan, W.-K. Hong, and H.-C. Kim, "Performance analysis of tag anti-collision algorithms for rfid systems," in *International Conference on Embedded and Ubiquitous Computing*. Springer, 2006, pp. 382–391.

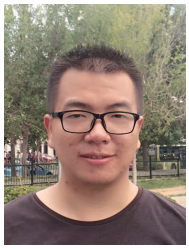
[46] R. Dorfman, "The detection of defective members of large populations," *The Annals of Mathematical Statistics*, vol. 14, no. 4, pp. 436–440, 1943.

[47] "http://www.informationweek.com/rsa-unveils-rfid-tag-blocker/d/d-id/1023433?"

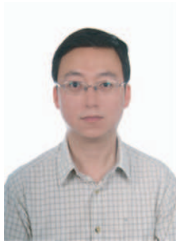
[48] A. Juels, R. L. Rivest, and M. Szydlo, "The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy," *Proc. of ACM CCS*, 2003.



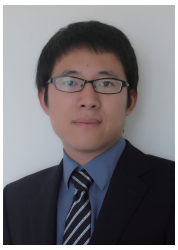
Xiulong Liu received the B.E. degree from the School of Software Technology, Dalian University of Technology, China, in 2010; and the Ph.D. degree from the School of Computer Science and Technology, Dalian University of Technology, China, in 2016. He was a visiting scholar with the Department of Computer and Information Sciences, Temple University, USA, in 2015; and a Postdoctoral Fellow with the School of Computer Science and Engineering, the University of Aizu, Japan, 2016. Currently, he is a Postdoctoral Fellow with the Department of Computing, The Hong Kong Polytechnic University. His research interests include wireless sensing, ubiquitous computing, and internet of things.



Xin Xie received the B.Sc. B.E degree in computer science from Dalian University of Technology, Dalian, China, in 2013. He is currently pursuing the Ph.D in Computer application technology at Dalian University of Technology. His research interests includes RFID technologies and wireless networks.



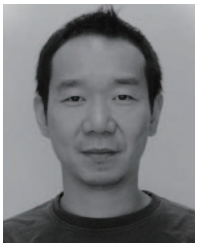
Xibin Zhao is now an associate professor at School of Software, Tsinghua University. He received the BS, M.E and Ph.D degrees in School of Computer Science and Telecommunication Engineering from Jiangsu University in 1994, 2000, 2004 respectively. His research interests include reliability analysis of hybrid network systems and information system security.



Kun Wang received the B. Eng. and Ph.D. degree in the School of Computer, Nanjing University of Posts and Telecommunications, Nanjing, China, in 2004 and 2009, respectively. From 2013 to 2015, he was a Postdoc Fellow in Electrical Engineering Department, University of California, Los Angeles (UCLA), CA, USA. In 2016, he was a Research Fellow in the School of Computer Science and Engineering, the University of Aizu, Aizu-Wakamatsu City, Fukushima, Japan. He is currently a Research Fellow in the Department of Computing, the Hong Kong Polytechnic University, Hong Kong, China, and also an Associate Professor in the School of Internet of Things, Nanjing University of Posts and Telecommunications, Nanjing, China. He has published over 50 papers in referred international conferences and journals. He has received Best Paper Award at IEEE GLOBECOM'16. He serves as Associate Editor of IEEE Access, Journal of Network and Computer Applications, EAI Transactions on Industrial Networks and Intelligent Systems and Editor of Journal of Internet Technology. He was the symposium chair/co-chair of IEEE IECON16, IEEE EEEIC16, IEEE WCSP16, IEEE CNCC17, etc. His current research interests are mainly in the area of big data, wireless communications and networking, smart grid, energy Internet, and information security technologies. He is a member of IEEE and ACM.

Keqiu Li received the bachelor's and master's degrees from the Department of Applied Mathematics at the Dalian University of Technology in 1994 and 1997, respectively. He received the Ph.D. degree from the Graduate School of Information Science, Japan Advanced Institute of Science and Technology in 2005. He also has two-year postdoctoral experience in the University of Tokyo, Japan. He is currently a professor in the School of Computer Science and Technology, Dalian University of Technology, China. He has published more than 100 technical papers, such as IEEE TPDS, ACM TOIT, and ACM TOMCCAP. He is an Associate Editor of IEEE TPDS and IEEE TC. His research interests include data center networks, cloud computing and wireless networks.

Alex X. Liu received the Ph.D. degree in computer science from the University of Texas at Austin in 2006. He is an Associate Professor with the Department of Computer Science and Engineering, Michigan State University. He is an Associate Editor of IEEE/ACM TRANSACTIONS ON NETWORKING and an Area Editor of Journal of Computer Communications (Elsevier). He received the IEEE & IFIP William C. Carter Award in 2004 and an NSF CAREER award in 2009. He received the Withrow Distinguished Scholar Award in 2011 at Michigan State University. He received Best Paper Awards from ICNP-2012, SRDS-2012, and LISA-2010. His research interests focus on networking and security.



Song Guo is a Full Professor at Department of Computing, The Hong Kong Polytechnic University. He received his Ph.D. in computer science from University of Ottawa and was a professor with the University of Aizu. His research interests are mainly in the areas of big data, cloud computing and networking, and distributed systems with over 400 papers published in major conferences and journals. His work was recognized by the 2016 Annual Best of Computing: Notable Books and Articles in Computing in ACM Computing Reviews. He is the recipient of the 2017 IEEE Systems Journal Annual Best Paper Award and other five Best Paper Awards from IEEE/ACM conferences. Prof. Guo was an Associate Editor of IEEE Transactions on Parallel and Distributed Systems and an IEEE ComSoc Distinguished Lecturer. He is now on the editorial board of IEEE Transactions on Emerging Topics in Computing, IEEE Transactions on Sustainable Computing, IEEE Transactions on Green Communications and Networking, and IEEE Communications. Prof. Guo has also served as General, TPC and Symposium Chair for numerous IEEE conferences. He currently serves as an officer for several IEEE ComSoc Technical Committees and a director in the IEEE ComSoc Board of Governors.

Jie Wu is the Associate Vice Provost for International Affairs at Temple University. He also serves as the Chair and Laura H. Carnell professor in the Department of Computer and Information Sciences. Prior to joining Tempe University, he was a program director at the National Science Foundation and was a distinguished professor at Florida Atlantic University. His current research interests include mobile computing and wireless networks, routing protocols, cloud and green computing, network trust and security, and social network applications. Dr. Wu regularly publishes in scholarly journals, conference proceedings, and books. He serves on several editorial boards, including IEEE Transactions on Service Computing and the Journal of Parallel and Distributed Computing. Dr. Wu was general co-chair/chair for IEEE MASS 2006, IEEE IPDPS 2008, IEEE ICDCS 2013, and ACM MobiHoc 2014, as well as program co-chair for IEEE INFOCOM 2011 and CCF CNCC 2013. He was an IEEE Computer Society Distinguished Visitor, ACM Distinguished Speaker, and chair for the IEEE Technical Committee on Distributed Processing (TCDP). Dr. Wu is a CCF Distinguished Speaker and a Fellow of the IEEE. He is the recipient of the 2011 China Computer Federation (CCF) Overseas Outstanding Achievement Award.