Unreconciled Collisions Uncover Cloning Attacks in Anonymous RFID Systems

Kai Bu, Xuan Liu, Jiaqing Luo, Bin Xiao*, *Senior Member, IEEE*, and Guiyi Wei

***Abstract*—Cloning attacks threaten Radio-Frequency Identification (RFID) applications but are hard to prevent. Existing cloning attack detection methods are enslaved to the knowledge of tag identifiers (IDs). Tag IDs, however, should be protected to enable and secure privacy-sensitive applications in anonymous RFID systems. In a first step, this paper tackles cloning attack detection in anonymous RFID systems without requiring tag IDs as a priori. To this end, we leverage unreconciled collisions to uncover cloning attacks. An unreconciled collision is probably due to responses from multiple tags with the same ID, exactly the evidence of cloning attacks. This insight inspires GREAT, our pioneer protocol for cloning attack detection in anonymous RFID systems. We evaluate the performance of GREAT through theoretical analysis and extensive simulations. The results show that GREAT can detect cloning attacks in anonymous RFID systems fairly fast with required accuracy. For example, when only six out of $50{,}000$ tags are cloned, GREAT can detect the cloning attack in 75.5 seconds with probability at least 0.99.**

***Index Terms*—anonymous RFID system, cloning attack detection, unreconciled collision, security, privacy.**

I. Introduction

CLONING attacks threaten Radio-Frequency Identification (RFID) applications but existing cloning attack detection methods are enslaved to the knowledge of tag identifiers (IDs). In a cloning attack, an attacker compromises genuine tags and produces their replicas (*cloned tags*) [1]. Holding replicated information of compromised tags, cloned tags behave exactly the same as genuine tags [1]. Cloning attacks thus threaten many RFID applications that use the genuineness of tags to validate the quality or authenticity of tagged objects. For example, carrying cloned tags, products in an RFID-enabled supply chain lead to financial losses [2], healthcare facilities in RFID-aided hospitals jeopardize personal safety [3], while RFID-incorporated passport cards even threaten national security [4]. Existing cloning attack detection methods leverage data redundancy corresponding to tag IDs. Since normally a tag has a unique ID [5], [6], if an ID associates simultaneously with different values of a certain attribute (e.g., tag location [7], [8], [9], [10] or synchronized secret [11]), the ID relates to multiple tags and reveals a cloning attack.

K. Bu, X. Liu, and B. Xiao* are with the Department of Computing, The Hong Kong Polytechnic University, Hung Hom, Kowloon, Hong Kong. E-mail: {cskbu, csxuanliu, csbxiao}@comp.polyu.edu.hk.

J. Luo is with the School of Computer Science & Engineering, University of Electronic Science and Technology of China, Chengdu, China. E-mail: csjluo@hotmail.com.

G. Wei is with the School of Computer Science and Information Engineering, Zhejiang Gongshang University, Hangzhou, China. E-mail: weigy@zjgsu.edu.cn.

EDICS: SEC-NETW Network security; **SYS-PROT** Protocols.

In a first step, this paper tackles cloning attack detection in anonymous RFID systems without requiring tag IDs as a priori. More specifically, the anonymity requires that readers cannot query tag IDs from tags or backend servers. Anonymous RFID systems enable privacy-sensitive applications [12], [13]. In such applications, communicating tag IDs either between backend servers and readers or between readers and tags risks leakage of tag IDs, which are private information or can be easily used to infer other private information [12]. Private information of concern is, for example, trade secrets in RFID-enabled supply chains [10], personal privacy in RFID-incorporated passports or driver licenses [4], and military strength in RFID-enabled weapon tracking systems [14], [15]. Requiring the awareness of tag IDs, existing cloning attack detection methods are therefore not applicable in anonymous RFID systems.

Forget about seemingly better intuitions. Before we introduce our method to cloning attack detection in anonymous RFID systems, let us first walk through some intuitive approaches and shake off the reverie in which they seem to be better.

Prevention? Only if we could. Of course, if we could prevent tags from being cloned, we would not bother to detect cloning attacks at all. A disappointing fact is, however, that no prevention scheme claims to completely defeat cloning attacks yet [11]. Most existing prevention protocols use cryptography and encryption to make tags hard to clone [16], [17], [18]. Apart from possible failures [11], they require additional hardware resources and key management strategies [19], which are hardly affordable to low-cost tags that cannot support any operation beyond hashes [20]. A more promising prevention scheme resorts to unclonable physical architecture of tags [21]. However, even if tags armed with cloning-resistant architectures arrive in the near future, it is still not practical either to replace off-the-shelf tags with cloning-resistant tags or to recall them for upgrade—already 1.3 billion tags were in the market in 2005, and even 33 billion were expected in 2010 [22]. All the preceding concerns raised by cloning attack prevention necessitate cloning attack detection.

Authentication? No. Since cloned tags are not genuine tags after all, some may resort to tag authentication. Authentication is a sharp weapon against counterfeit tags that carry valid IDs but forged keys [1], [23], [24], [25]. Different from counterfeit tags, cloned tags hold not only valid IDs but also valid keys. Cloned tags, therefore, can pass authentication as can genuine tags.

Tag cardinality estimation? No. Since cloning attacks make the number of tags (*tag cardinality*) exceed the number of

IDs (*ID cardinality*), some may suggest first estimating tag cardinality and then leveraging the difference between those two cardinalities. If the difference exceeds a certain threshold, chances are that cloned tags exist. But adopting the suggestion faces two major hindrances, the privacy of ID cardinality and the accuracy of tag cardinality estimation. First, ID cardinality is probably as privacy-sensitive as tag IDs in anonymous RFID systems. Consider, for example, a military anonymous RFID system that tracks weapons such as firearms and shells [14], [15]. In such a system, tag IDs may reveal categories and models of tagged weapons, and ID cardinality indicates exactly how many weapons therein. To avoid exposing military strength through tag IDs and ID cardinality, both of them should be protected in the considered system.

Second, even if ID cardinality is known, we still cannot simply rely on the difference between it and tag cardinality estimation. Considering inaccuracy of tag cardinality estimation protocols, we sometimes cannot determine that the difference is due to cloning attacks or tag cardinality estimation error. Even worse, when cloned tags exist, tag cardinality estimation protocols may encounter large estimation errors [26], [27], [28], [29], [30]. They estimate tag cardinality using the distribution of the number of tag responses in a frame of time slots. But this distribution is likely to be disturbed by responses from cloned tags and thus to induce a large estimation error.

Our approach and contributions. We propose leveraging *unreconciled collisions* for cloning attack detection in anonymous RFID systems. An unreconciled collision cannot be reconciled through arbitrating channel access among tags whose responses cause the collision. The motivation for leveraging unreconciled collisions lies in how RFID tags compete for channel access. In an RFID system, tags decide when to respond according to the value of their IDs [5], [6]. In other words, multiple tags with the same ID simultaneously respond to a query message and thus induce an unreconciled collision. Since multiple tags having the same ID is exactly the evidence of cloning attacks, we can leverage unreconciled collisions to uncover cloning attacks yet not require the knowledge of tag IDs.

Taking the first step toward cloning attack detection in anonymous RFID systems, the paper makes the following contributions:

- Leverage unreconciled collisions to uncover cloning attacks without requiring tag IDs as a priori. This countermeasure against cloning attacks can enable and secure privacy-sensitive applications in anonymous RFID systems.
- Propose GREAT, a pioneer protocol leveraging unreconciled collisions for cloning attack detection in anonymous RFID systems.
- Analyze theoretically GREAT's detection accuracy and execution time. The analysis results can guide protocol configuration for satisfying required detection accuracy.
- Validate the performance of GREAT through extensive simulations. The results show that GREAT can detect cloning attacks in anonymous RFID systems fairly fast with required accuracy. When, for example, six cloned IDs hide among up to $50{,}000$ tag IDs, GREAT can detect the cloning attack in only 75.5 seconds with probability at least 0.99.

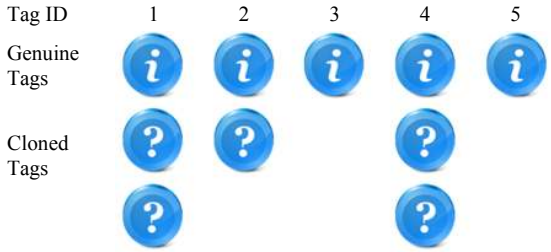
Paper organization. The rest of this paper is organized as follows. Section II defines the problem of cloning attack detection in anonymous RFID systems. Section III provides an overview of our method. Section IV presents protocol design and theoretical analysis. Section V reports simulation results. Finally, Section VI concludes the paper and indicates future work.

II. System and Problem

We consider an anonymous RFID system that consists of a reader and many tags. The reader can communicate with all tags. Normally a tag attached to an object has a unique ID. Tag IDs may directly reveal private information of tagged objects or indirectly link to such information stored on a backend server. To satisfy privacy-sensitive applications, the anonymous RFID system should strictly control granting the reader access to the server and transmitting tag IDs (encrypted or not) between the reader and tags. We are concerned with cloning attacks in which an attacker clones genuine tags and attaches cloned tags to objects with questionable authenticity [1]. Using only the genuineness of tags to validate the authenticity of tagged objects, we cannot distinguish objects attached with genuine tags from objects attached with cloned tags. The problem is therefore to detect whether cloned tags exist in an anonymous RFID system. An implicit constraint we would like to emphasize here is that, to participate in system operations, all tags reside in the communication region of the reader. This applies to also cloned tags if any; otherwise, they may fail the cloning attack.

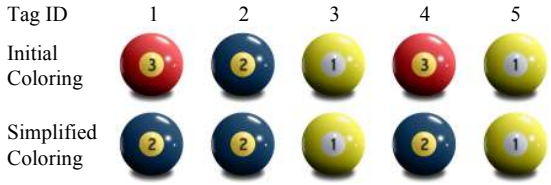
We formulate the problem using a probabilistic model: If the number of cloned IDs exceeds a given tolerance number, detect the cloning attack with a probability no less than a given detection accuracy. A *cloned ID* corresponds to a genuine tag and some cloned tag(s). Both tolerance number and detection accuracy are set according to application requirements. By the intrinsic property of probabilistic methods, a higher tolerance number and a lower detection accuracy yield faster detection with less certainty. With detection accuracy and tolerance number set to 1 and 0, respectively, the problem is specialized to deterministic detection of the cloning attack.

We do not assume the knowledge of tag IDs or of their cardinality. As we discussed, both tag IDs and their cardinality may induce privacy leakage. To best support privacy-sensitive RFID applications, we do not allow our cloning attack detection method to collect tag IDs or to gain access to them on the backend server. We assume that the reader and tags communicate using a power level high enough to drown background noise; error correction coding against channel errors [31] is beyond the scope of this paper. (As we will show at the end of Section IV-C, channel errors may induce false positives to cloning attack detection. A feasible countermeasure against false positives is also investigated therein.) We consider a general scenario where a reader can communicate with all tags in an anonymous RFID system using a single channel [11], [26], [32]. Adaptation of our cloning attack detection



(a) Cloning attack instance with 5 genuine tags and 5 cloned tags.

(b) Each tag is mapped to a ball. An ID is assigned with a unique color. Detecting cloned tags is transformed into the problem of drawing two balls in the same color.



(c) Each tag ID is mapped to a ball. A ball is colored according to the number of tags with the ID mapped to the ball. Detecting cloned tags is transformed into the problem of drawing a ball not in type 1 color.

Fig. 1. Cloning attack detection in identifiable RFID systems modeled by the ball drawing game.

method to scenarios with multiple readers, multiple channels, or multiple subsystems for accommodating all tags is left for future work.

III. Methodology Overview

In this section, we provide an overview of cloning attack detection using unreconciled collisions in anonymous RFID systems. We first discuss the motivation of unreconciled collisions by lessons from cloning attack detection in identifiable RFID systems. We then discuss how to explore unreconciled collisions for uncovering cloning attacks in anonymous RFID systems.

A. Lessons from Identifiable RFID Systems

We start exploring the methodology by a warmup of cloning attack detection in identifiable RFID systems. Figure 1(a) illustrates a cloning attack instance with ten tags including five genuine tags (i.e., icons with symbol *i*) and five cloned tags (i.e., icons with question mark). For ease of presentation, we assign tag IDs 1 through 5. (But we do not assume that, given n genuine tags, tag IDs simply range from 1 to n.) Cloned IDs 1, 2, and 4 correspond to two, one, and two cloned tags, respectively. We will discuss two ideas of detecting the cloning attack, through identification and through polling. To visualize the ideas, we transform the cloning attack detection problem into the *ball drawing game* [33] as in Figures 1(b) and (c).

1) Detection through identification: The intuition is that we can identify tags and detect the cloning attack if a tag has the same ID as that of an identified tag. Figure 1(b) models this intuition by the ball drawing game, in which we map each tag to a ball and assign a unique color to balls mapped from tags with the same ID. The goal is to draw two balls in the same color without replacement. Observing Figure 1(b), we can infer that it is more likely to achieve the goal when many balls are in the same color than to achieve it when otherwise. However, since it is not practical to identify tags in anonymous RFID systems [12], [13], we in this game can hardly find any clues to detecting anonymous cloned tags.

2) Detection through polling: The intuition is that, if we know tag IDs in advance, we can verify whether one or more tags correspond to the same ID through polling. Figure 1(c) models a straightforward implementation of the intuition by the ball drawing game, in which we map each ID to a ball and assign type i color to the ball whose associated ID corresponds to i tags (we call this *initial coloring*). The goal is therefore to draw a ball not in type 1 color without replacement. Initial coloring, however, faces a dilemma: It requires in advance the number of cloned tags corresponding to each ID while those numbers are yet to obtain. Fortunately, we can escape from the dilemma by leveraging wireless broadcast. As each ID is mapped to a ball, drawing a ball is identical to a reader broadcasting a query message containing the ball's associated ID. Upon receiving the query message, a tag responds to the reader if its ID is identical to the contained one. The reader then verifies whether one or more tags respond if it receives an intact response or a collided one, respectively. The latter case reveals that multiple tags have the same ID and thus the reader detects the cloning attack. We thus refine initial coloring to *simplified coloring* with only two types of colors in Figure 1(c)—Type 1 color for an ID corresponding to only one tag and type 2 color for an ID corresponding to multiple tags. The goal is still to draw a ball not in type 1 color without replacement; we can achieve it by leveraging wireless broadcast and response states (i.e., collision or non-collision).

So what can we learn from polling-based cloning attack detection? Being optimistic, we could expect tag information (e.g., IDs and keys stored on a backend server) to be known also in an anonymous RFID system. Then we can simply apply polling-based detection. A likely modification is encrypting the broadcast IDs, which are usually protected in anonymous systems. But being realistic, we have to prepare for no access to registered tag information. This concern is necessary because any granted access to them risks potential privacy leakage [12]. Such privacy leakage occurs when, for example, encrypted IDs are eavesdropped and decrypted [1], or the detection protocol is manipulated [34]. The challenge is therefore to detect cloning attacks among anonymous tags without knowing their IDs. Borrowing ideas from polling-based detection, if we could verify that whether a collision is caused by responses from tags with the same ID even if the ID is unknown, we can still detect cloning attacks. We will shortly illustrate this idea and how we leverage it for cloning attack detection in anonymous RFID systems.

B. Unreconciled Collisions in Anonymous RFID Systems

To implement the preceding idea, we expect tags to decide when to respond according to their IDs such that tags with the same ID always simultaneously respond. Tags with different IDs could, however, respond either simultaneously or asynchronously. If tags with different IDs respond simultaneously and cause a collision, we are likely to reconcile the collision by further arbitrating access to the channel among them. On the other hand, if a collision is due to responses from tags with the same ID, it is hard to reconcile. We refer to a collision that cannot be reconciled through arbitrating channel access among tags whose responses cause the collision as an *unreconciled collision*. Intuitively, an unreconciled collision is probably caused by a genuine tag and its cloned peer(s), that is, multiple tags with the same ID. Unreconciled collisions, therefore, enable us to uncover cloning attacks in anonymous RFID systems.

Making tags decide when to respond according to their IDs, we do not have to know the IDs in advance. Take, for example, a simple injection from a tag's ID to the index of the time slot in which the tag responds. Surely this straightforward injection is not desirable due to privacy leakage. Overhearing whether there is any response in each time slot, an attacker can easily infer tag IDs. Moreover, the injection method may take an unacceptable long time. Consider a general system configuration with 96-bit IDs, a 10-bit string with CRC embedded for verifying a collision, and 25 μs for transmitting a single bit [5], [6]. Under such configuration, the injection method takes about $\frac{25\times10\times2^{96}}{10^6\times3600\times24\times365}$ (year), which is over 0.6 billion billion years!

Collision arbitration protocols are well-investigated for arbitrating channel access among tags [35], [36]. Such protocols are initially used to improve time efficiency of tag identification, which collects tag IDs without them being known in advance. Now we wonder that collision arbitration protocols may adapt to cloning attack detection in anonymous RFID systems. To answer this conjecture, we will continue to review collision arbitration protocols and discuss which of them is of our interest.

C. Choice of Collision Arbitration Protocol

We briefly review two typical categories of collision arbitration protocols, *framed Aloha* [35] and *tree traversal* [36]. In framed Aloha, a reader creates a query frame with a number of time slots. The number of time slots within a query frame is usually called *frame size*. The reader then broadcasts the frame size and also a random seed. Using a hash function of the frame size, the random seed, and its ID, a tag decides the index of the time slot in which it sends a response. A time slot chosen by no tag, only one tag, or multiple tags is known as an *empty slot*, a *singleton slot*, or a *collision slot* [26]. Only in singleton slots can a reader correctly receive tag responses. In tree traversal, to collect l-bit tag IDs, a reader first creates a binary tree of height l and with each l-bit string mapped to a leaf. The reader then collects tag IDs through traversing the binary tree in a depth-first order. Specifically, the reader broadcasts the bit string corresponding to the current tree node; tags respond if their IDs are prefixed with the bit string. If no collision occurs, the reader can correctly receive the response. Otherwise, the reader continues to collect tag IDs by broadcasting the bit string of the current tree node's child.

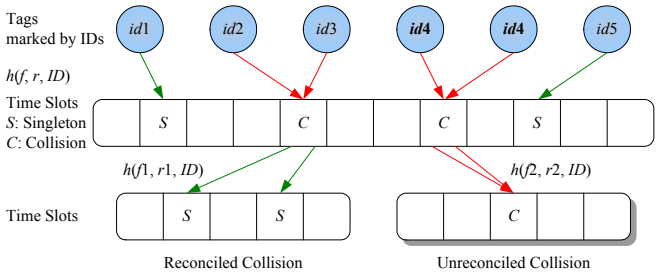


Fig. 2. An example of unreconciled collision caused by responses from two tags with the same ID $id4$ (i.e., a genuine tag and its cloned peer).

Adapting collision arbitration protocols to cloning attack detection in anonymous RFID systems, we choose framed Aloha over tree traversal. The reason for this choice is that tree traversal is susceptible to leaking a section of a tag ID or even an entire one. Overhearing the string s broadcast by a reader, an attacker can easily infer that at least one tag ID is prefixed with s after it overhears any response. Consider again the aforementioned RFID-enabled weapon tracking system [14], [15]. A section of the tag ID, say s, may reveal weapon information (e.g., category and model) and thus expose military strength. When s is of length $l-1$, the attacker can even infer that either $s0$ or $s1$ must be a tag ID if there is only one response, or both if a collision occurs. Such leakages are, of course, against the purpose of privacy-sensitive applications in anonymous RFID systems [12], [13]. In framed Aloha, the attacker, however, can hardly infer a tag's ID using the hash result [37], that is, the index of the time slot in which the tag responds.

D. Illustrative Example of Unreconciled Collisions

Having walked through the basics of unreconciled collisions and the choice of collision arbitration protocols for exploring unreconciled collisions, we now provide the big picture of how unreconciled collisions uncover cloning attacks in anonymous RFID systems. Figure 2 illustrates a sample of six tags with IDs $id1$ through $id5$, among which $id4$ associates with two tags (i.e., a genuine tag and its cloned peer). For better illustration of unreconciled collisions, we deliberately make the ID of each tag explicit. In the first frame with frame size f and random seed r, a tag responds in a time slot with index decided by hash function $h(f, r, ID)$. Tags with $id1$ and $id5$ respond in two distinct singleton slots, while tags with $id2$ and $id3$ respond in the first collision slot and tags with $id4$ in the second collision slot. To reconcile the first collision, we let tags that responded in this slot (i.e., tags with $id2$ and $id3$) respond in the second frame with frame size $f1$ and random seed $r1$. We successfully reconcile the first collision because no collision occurs in the second frame. It is, however, not hard to imagine that the second collision is unreconciled: Tags with the same ID $id4$ will still choose the same time slot to

respond in the third frame with frame size $f2$ and random seed $r2$, causing a collision again.

But, of course, scenarios in anonymous RFID systems are a different story from the example in Figure 2—as we discussed, we are not aware of the IDs of anonymous tags in advance. Without knowing tag IDs, we can ensure only that a successfully reconciled collision is due to responses from genuine tags, whereas we cannot ensure that an unreconciled collision is due to responses from multiple tags with the same ID. So the challenge is to infer the probability of an unreconciled collision being caused by responses from multiple tags with the same ID, the very evidence of a cloning attack. We next delve into leveraging unreconciled collisions to detect cloning attacks with high probability in anonymous RFID systems.

IV. GREAT: Greedy Collision-Slot–Reframing Detection Protocol

In this section, we propose the Greedy collision-slot–REfrAming deTection protocol (*GREAT*) against cloning attacks in anonymous RFID systems. GREAT reframes collision slots to find unreconciled collisions and thus to detect cloning attacks. We will also theoretically analyze GREAT's detection accuracy and execution time.

A. GREAT Design

GREAT detects a cloning attack in an anonymous RFID system if an unreconciled collision occurs. To find an unreconciled collision, GREAT reconciles collisions in a greedy manner: After reconciling a collision, if both some singleton slot(s) and some collision slot(s) show up, GREAT continues to reconcile the newly shown collision(s). GREAT reconciles collisions through *collision slot reframing*, an adaptation of framed Aloha. As will be detailed shortly, to reframe a collision slot, GREAT requires tags chose the slot to further respond in a new frame, as in Figure 2. In the new frame, if only one slot is collision and the others are empty, GREAT finds an unreconciled collision and therefore detects a cloning attack.

During collision slot reframing, a challenge arises in a new frame when the first non-empty slot is collision: How can we decide whether or not to reframe the collision slot? We should reframe the collision slot if it is followed by some non-empty slot(s). We need not reframe the collision slot if it is followed by only some empty slot(s) or by no slot, because in both cases the collision slot exposes an unreconciled collision. To address the challenge, we quickly determine the number of non-empty slots in the new frame using 1-bit responses. If the new frame contains only one non-empty slot, it will contain only one collision slot under 10-bit responses, exactly the condition for an unreconciled collision. If the new frame contains multiple non-empty slots, we decide to reframe the collision slot under concern.

We now detail the GREAT design. The reader first broadcasts a query message containing the frame size f and a random seed r. Upon receiving the query message, a tag responds in the time slot with index $h(f, r, ID)$. The hash function $h(\cdot)$ implemented on tags enables a tag to choose

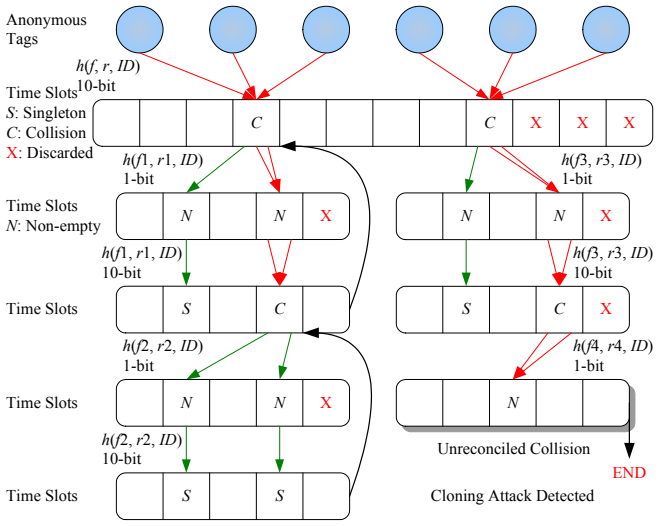


Fig. 3. GREAT execution instance for cloning attack detection in an anonymous RFID system.

in which time slot to respond uniformly at random [5], [6], [26]. The response is a 10-bit string with CRC embedded for the reader to verify collisions [6]. After verifying an empty slot or a singleton slot, the reader issues a slot end command to trigger the next time slot. After verifying a collision slot, the reader reframes the collision slot with a new frame size f_{r} (*reframing size*) and a new random seed r_{r}, requiring 1-bit responses for quickly counting the number of non-empty slots. If the new frame contains only one non-empty slot, GREAT finds an unreconciled collision, detects a cloning attack, and terminates. Otherwise, once the reader verifies the second non-empty slot, it reframes the collision slot again with f_{r} and r_{r}, requiring 10-bit responses. Then the reader greedily reframes a collision slot whenever it verifies one. After verifying all non-empty slots (and reframing collision slots if any) in an f_{r}-slotted frame, the reader traces back to the collision slot it just frames, and issues a slot end command to trigger the following time slot.

For ease of understanding the GREAT design, Figure 3 illustrates a GREAT execution instance. After verifying the first collision slot in the f-slotted frame, the reader reframes it with $f_{\mathrm{r}} = f1$ and $r_{\mathrm{r}} = r1$, requiring 1-bit responses. After verifying the second non-empty slot in the $f1$-slotted frame, the reader again reframes the collision slot with $f1$ and $r1$, but requiring 10-bit responses. Using another frame with $f_{\mathrm{r}} = f2$ and $r_{\mathrm{r}} = r2$ to successfully reconcile the collision, the reader traces back to the first collision slot in the f-slotted frame, issues a slot end command, and continues to verify remaining slots. Similarly, the reader reframes the second collision slot in the f-slotted frame with $f_{\mathrm{r}} = f3$ and $r_{\mathrm{r}} = r3$ and reframes the first collision slot in the $f3$-slotted frame with $f_{\mathrm{r}} = f4$ and $r_{\mathrm{r}} = r4$. Since only one non-empty slot shows up in the $f4$-slotted frame, GREAT finds an unreconciled collision and detects the cloning attack.

B. False Negative Rate

We analyze the maximum number $s_{\max}$ of slots in the f-slotted frame that GREAT needs to verify (and to reframe if

any collision slot) to satisfy a false negative rate α. Note that in what follows, the analysis reckons hash values of tag IDs as following a uniform distribution, as considered in established literature (e.g., references [12], [26], [27], [28], [30], [32], to name a few). More specifically, a tag ID has the same probability of being hashed into each time slot in a frame.

Lemma 1: Given the frame size f, the tolerance number m of cloned IDs, when GREAT verifies up to s slots in the f-slotted frame, the false negative rate $P_{\text{fn}}(f, m, s)$ is upper bounded as the following:

$$P_{\text{fn}}(f, m, s) \leq (1 - \frac{s}{f})^{m+1}. \tag{1}$$

Proof: Since GREAT detects cloning attacks through greedy collision-slot reframing, GREAT can find an unreconciled collision and detect the cloning attack if at least one cloned tag responds in the s slots. A false negative thus occurs when all cloned tags respond in the last $f - s$ slots. Let m', where $m' > m$, denote the number of cloned IDs. The false negative rate $P_{\text{fn}}(f, m, s)$ can be defined as

$$P_{\text{fn}}(f, m, s) = (\frac{f - s}{f})^{m'} = (1 - \frac{s}{f})^{m'}. \tag{2}$$

Given certain f and s, $P_{\text{fn}}(f, m, s)$ in Equation 2 is a monotonically decreasing function of m'. Because $m' = m+1$ is the first integer that satisfies $m' > m$, we have

$$P_{\text{fn}}(f, m, s) = (1 - \frac{s}{f})^{m'} \leq (1 - \frac{s}{f})^{m+1},$$

using the monotonicity of $P_{\text{fn}}(f, m, s)$. ■

Theorem 1: Given the frame size f, the tolerance number m of cloned IDs, the maximum number s_{max} of slots in the f-slotted frame GREAT verifies to satisfy a false negative α is as the following:

$$s_{\text{max}} = \lceil (1 - \alpha^{\frac{1}{m+1}}) f \rceil.$$

Proof: By Equation 2, the false negative rate $P_{\text{fn}}(f, m, s)$ is a monotonically decreasing function of s. To minimize the execution time, GREAT should terminate right after it verifies the sth slot where $P_{\text{fn}}(f, m, s) \leq \alpha$, that is,

$$s_{\text{max}} = \min\{s \mid P_{\text{fn}}(f, m, s) \leq \alpha\}. \tag{3}$$

By Lemma 1, $P_{\text{fn}}(f, m, s)$ is upper bounded. To satisfy $P_{\text{fn}}(f, m, s) \leq \alpha$, we must satisfy that the upper bound of $P_{\text{fn}}(f, m, s)$ is less than or equal to α. By plugging the upper bound in Formula 1 into Equation 3, we thus have

$$\begin{aligned} s_{\text{max}} &= \min\{s \mid (1 - \frac{s}{f})^{m+1} \leq \alpha\} \\ &= \min\{s \mid s \geq (1 - \alpha^{\frac{1}{m+1}}) f\} \\ &= \lceil (1 - \alpha^{\frac{1}{m+1}}) f \rceil. \end{aligned}$$

■

C. False Positive Rate

We now analyze the minimum reframing size f_{rmin} that GREAT uses for collision slot reframing to satisfy a false positive rate β.

Lemma 2: Given an unreconciled collision reframed by GREAT with an f_{r}-slotted frame, the false positive rate $P_{\text{fp}}(f_{\text{r}})$ is upper bounded as the following:

$$P_{\text{fp}}(f_{\text{r}}) \leq \frac{1}{f_{\text{r}}^2}. \tag{4}$$

Proof: Let n_{c} denote the number of the IDs of tags that cause the unreconciled collision. When $n_{\text{c}} = 1$, the unreconciled collision is due to responses from a genuine tag and its cloned peer(s), inducing no false positives. A false positive, however, occurs when $n_{\text{c}} \geq 2$ and all n_{c} IDs fall into the same slot in the f_{r}-slotted frame. The false positive rate $P_{\text{fp}}(f_{\text{r}})$ thus can be defined as

$$P_{\text{fp}}(f_{\text{r}}) = \sum_{i=0}^{f_{\text{r}}-1} \frac{1}{f_{\text{r}}} \frac{1}{f_{\text{r}}^{n_{\text{c}}}} = \frac{1}{f_{\text{r}}^{n_{\text{c}}}}. \tag{5}$$

Given a certain f_{r}, $P_{\text{fp}}(f_{\text{r}})$ in Equation 5 is a monotonically decreasing function of n_{c}. Because $n_{\text{c}} = 2$ is the first integer that satisfies $n_{\text{c}} \geq 2$, we have

$$P_{\text{fp}}(f_{\text{r}}) = \frac{1}{f_{\text{r}}^{n_{\text{c}}}} \leq \frac{1}{f_{\text{r}}^2},$$

using the monotonicity of $P_{\text{fp}}(f_{\text{r}})$. ■

Theorem 2: Given an unreconciled collision, the minimum reframing size f_{rmin} for GREAT to satisfy a false positive rate β is as the following:

$$f_{\text{rmin}} = \lceil \beta^{-\frac{1}{2}} \rceil.$$

Proof: By Equation 5, the false positive rate $P_{\text{fp}}(f_{\text{r}})$ is a monotonically decreasing function of f_{r}. To minimize the time for reframing a collision slot, GREAT should set the minimum f_{r} that satisfies $P_{\text{fp}}(f_{\text{r}}) \leq \beta$, that is,

$$f_{\text{rmin}} = \min\{f_{\text{r}} \mid P_{\text{fp}}(f_{\text{r}}) \leq \beta\}. \tag{6}$$

By Lemma 2, $P_{\text{fp}}(f_{\text{r}})$ is upper bounded. To satisfy $P_{\text{fp}}(f_{\text{r}}) \leq \beta$, we must satisfy that the upper bound of $P_{\text{fp}}(f_{\text{r}})$ is less than or equal to β. By plugging the upper bound in Formula 4 into Equation 6, we thus have

$$\begin{aligned} f_{\text{rmin}} &= \min\{f_{\text{r}} \mid \frac{1}{f_{\text{r}}^2} \leq \beta\} \\ &= \min\{f_{\text{r}} \mid f_{\text{r}} \geq \beta^{-\frac{1}{2}}\} \\ &= \lceil \beta^{-\frac{1}{2}} \rceil. \end{aligned}$$

■

Corollary 1: Given an unreconciled collision reframed by GREAT with an f_{r}-slotted frame, $f'_{\text{rmin}} = 2$ is the minimum f_{r} to satisfy that the probability of a cloning attack is greater than the probability of a false positive.

Proof: Given the false positive rate $P_{\text{fp}}(f_{\text{r}})$, the probability that the unreconciled collision is due to a cloning attack is $1 - P_{\text{fp}}(f_{\text{r}})$. By Lemma 2, $P_{\text{fp}}(f_{\text{r}})$ is upper bounded. $1 - P_{\text{fp}}(f_{\text{r}})$ is, therefore, lower bounded. To guarantee that $(1 - P_{\text{fp}}(f_{\text{r}})) > P_{\text{fp}}(f_{\text{r}})$, we derive f'_{rmin} as follows:

$$\begin{aligned} f'_{\text{rmin}} &= \min\{f_{\text{r}} \mid \min(1 - P_{\text{fp}}(f_{\text{r}})) > \max(P_{\text{fp}}(f_{\text{r}}))\} \\ &= \min\{f_{\text{r}} \mid 1 - \frac{1}{f_{\text{r}}^2} > \frac{1}{f_{\text{r}}^2}\} \\ &= \min\{f_{\text{r}} \mid f_{\text{r}} > \sqrt{2}\} \\ &= 2. \end{aligned}$$

■

Post-detection operations, such as cloned-tag identification, can eliminate false positives. Following cloning attack detection, cloned-tag identification aims to identify all cloned IDs and thus to identify cloned tags with certainty. Toward

certainty, cloned-tag identification must be granted an access to tag IDs and keys. Based on the accessed tag information, a straightforward cloned-tag identification is through polling, as we discussed in Section III-A2. To avoid privacy leakage and time inefficiency by transmitting encrypted IDs during polling, a better method is to adapt GREAT. Given accessed IDs, GREAT can pre-hash the IDs and ensure in advance exactly which IDs are in which slots. During tags respond to the reader, if a collision occurs in a slot into which only one ID is pre-hashed, the ID must correspond to some cloned tag(s). Thus we can identify all cloned tags within a number of iterations, and in return, eliminate false positives if any. It is worth mentioning also that the above adaptation of GREAT is analogous to the information collection problem [32] that collects data from tags of which the IDs are known a priori. The data for GREAT to collect from a tag are just a random bitstring long enough for detecting a collision. For interested readers wondering whether verifying a number of tag IDs is time-consuming, the approximate execution time if leveraging the proposal in [32] is about 1.6 times the lower bound—$1.6nt_{\mathrm{c}}$, where n represents the ID cardinality and t_{c} denotes the time to detect a collision slot. Note that the above discussed cloned-tag identification can also combat false positives due to channel errors or noises. Such false positives occur when channel errors or noises turn an intact response in a singleton slot into a collided one.

D. Detection Accuracy

We now analyze the detection accuracy measured by the probability of detecting an existing cloning attack.

***Theorem** 3:* Given an f-slotted frame and the tolerance number m of cloned IDs, when GREAT detects an existing cloning attack by verifying the first s slots and reframing collision slots with the reframing size f_{r}, the detection accuracy $P_{\mathrm{d}}(f, m, s, f_{\mathrm{r}})$ is lower bounded as the following:

$$P_{\mathrm{d}}(f, m, s, f_{\mathrm{r}}) \geq 1 - (1 - \frac{s}{f})^{m+1} + P'_{\mathrm{d}}(f, m, s, f_{\mathrm{r}}), \quad (7)$$

where $0 \leq P'_{\mathrm{d}}(f, m, s, f_{\mathrm{r}}) \leq (1 - \frac{s}{f})^{m+1} \frac{1}{f_{\mathrm{r}}^2}$.

Proof: GREAT can detect an existing cloning attack in two cases. First, if at least one cloned ID corresponds to responses in the first s slots, GREAT can find an unreconciled collision and detect the cloning attack. The first case, therefore, occurs when no false negative occurs. Second, if no cloned ID corresponds to responses in the first s slots, GREAT can also find an unreconciled collision due to a false positive and thus detect the cloning attack. Combining detection probabilities in these two cases, we have

$$P_{\mathrm{d}}(f, m, s, f_{\mathrm{r}}) = (1 - P_{\mathrm{fn}}(f, m, s)) \cdot 1 + P_{\mathrm{fn}}(f, m, s) \cdot P_{\mathrm{fp}}(f_{\mathrm{r}}).$$

$P_{\mathrm{fn}}(f, m, s)$ and $P_{\mathrm{fp}}(f_{\mathrm{r}})$ as in Lemma 1 and Lemma 2, respectively, are both upper bounded. Using the upper bounds therein, we can derive that

$$1 - P_{\mathrm{fn}}(f, m, s) \geq 1 - (1 - \frac{s}{f})^{m+1},$$

$$P_{\mathrm{fn}}(f, m, s) \cdot P_{\mathrm{fp}}(f_{\mathrm{r}}) \leq (1 - \frac{s}{f})^{m+1} \frac{1}{f_{\mathrm{r}}^2}.$$

Let $P'_{\mathrm{d}}(f, m, s, f_{\mathrm{r}}) = P_{\mathrm{fn}}(f, m, s) \cdot P_{\mathrm{fp}}(f_{\mathrm{r}})$. Plugging the above two inequalities into the expression of $P_{\mathrm{d}}(f, m, s, f_{\mathrm{r}})$, we derive Formula 7 and prove Theorem 3. ■

To satisfy required false negative rate α and false positive rate β, from Theorem 3 follows easily Corollary 2.

***Corollary** 2:* Given an f-slotted frame and the tolerance number m of cloned IDs, when GREAT detects an existing cloning attack by verifying the first $s_{\max}$ slots and reframing collision slots with the reframing size f_{rmin} to satisfy a false negative rate α and a false positive rate β, the detection accuracy $P_{\mathrm{d}}(f, m, s_{\max}, f_{\mathrm{rmin}})$ is lower bounded as

$$P_{\mathrm{d}}(f, m, s_{\max}, f_{\mathrm{rmin}}) \geq 1 - \alpha + \varphi(\alpha, \beta),$$

where $\varphi(\alpha, \beta) = P'_{\mathrm{d}}(f, m, s_{\max}, f_{\mathrm{rmin}})$ and $0 \leq \varphi(\alpha, \beta) \leq \alpha\beta$.

E. Execution Time

As we will show, the expected execution time of GREAT is upper bounded by a function of ID cardinality n. Although GREAT does not require n to be known, system managers or whoever adopt GREAT and know the value of n can benefit from the expected execution time upper bound. A possible benefit is, for example, to facilitate scheduling multiple tag monitoring operations [32], [38], [39], [40], [41].

***Theorem** 4:* Given the ID cardinality n, the frame size f, the number of slots s in the f-slotted frame GREAT verifies, and the reframing size f_{r}, the expected execution time of GREAT $E[T(n, f, s, f_{\mathrm{r}})]$ is upper bounded as

$$E[T(n, f, s, f_{\mathrm{r}})] \leq \frac{nsf_{\mathrm{r}}}{f} t_{\mathrm{e}} + (\frac{nsf_{\mathrm{r}}}{f} + s) t_{\mathrm{c}},$$

where t_{e} denotes the time to detect an empty slot, and t_{c} denotes the time to detect a collision slot.

Proof: When GREAT verifies only the first s slots in the f-slotted frame, we expect $\frac{s}{f}n$ IDs in s slots. To detect cloned IDs among these $\frac{s}{f}n$ IDs, GREAT takes the maximum execution time when it verifies all $\frac{s}{f}n$ IDs, in two cases. The first case is when there is no cloned ID among the $\frac{s}{f}n$ ones. The second case is when there is only one cloned ID among the $\frac{s}{f}n$ IDs but the cloned ID is the $\frac{s}{f}n$th one for GREAT to verify.

The proof turns to finding the maximum time for GREAT to verify all $\frac{s}{f}n$ IDs. By the GREAT design (Section IV-A), GREAT normally ends empty and singleton slots, and further reframes collision slots. The maximum number of collision slots to reframe thus yields the maximum execution time. For $\frac{s}{f}n$ IDs to yield the maximum number of collision slots, there should be no singleton slot among the s ones. The proof turns to making IDs in each collision slot to yield the maximum number of collision slots to reframe. Let s_{c} denote the number of collision slots in the s ones. Given n_j IDs in a collision slot, where $0 \leq j \leq s_{\mathrm{c}} - 1$ and $\sum_{j=0}^{s_{\mathrm{c}}-1} n_j = \frac{s}{f}n$, the maximum time for reconciling it occurs when there are only two non-empty slots under 1-bit responses and there are one singleton slot and one collision slot with $n_j - 1$ IDs under 10-bit responses. The same scenario applies to reframing the collision slot with $n_j - 1$ IDs, that is, there are two non-empty slots under 1-bit

responses and there are one single slot and one collision slot with $(n_j - 1) - 1$ IDs under 10-bit responses. Following this recursion, we conclude that it maximally takes $n_j(t_e + t_c)$ to reconcile a collision caused by n_j IDs. Combining st_c taken by s slots, we have

$$\begin{aligned} E[T(n, f, s, f_r)] &\leq st_c + \sum_{j=0}^{s_c - 1} n_j f_r (t_e + t_c) \\ &= st_c + \frac{s}{f} n f_r (t_e + t_c) \\ &= \frac{n s f_r}{f} t_e + (\frac{n s f_r}{f} + s) t_c. \end{aligned}$$

■

From Theorems 1, 2, and 4 follows easily the following Corollary 3.

***Corollary** 3:* Given the ID cardinality n, the tolerance number m of cloned IDs, and the frame size f, to satisfy a false negative rate α and a false positive rate β, the expected execution time of GREAT $E[T(n, f, m, \alpha, \beta)]$ is upper bounded as the following:

$$E[T(n, f, m, \alpha, \beta)] \leq \frac{n s_{\max} f_{\text{rmin}}}{f} t_e + (\frac{n s_{\max} f_{\text{rmin}}}{f} + s_{\max}) t_c,$$

where $s_{\max} = \lceil (1 - \alpha^{\frac{1}{m+1}}) f \rceil$, $f_{\text{rmin}} = \lceil \beta^{-\frac{1}{2}} \rceil$, t_e denotes the time to detect an empty slot, and t_c denotes the time to detect a singleton or a collision slot.

F. Limitation: Generating Tag Profiles

A potential limitation of GREAT is that several runs of GREAT with a tag may generate the tags's profile. Specifically, a tag profile consists of a series of vectors comprising frame size f_i, random seed r_i, and slot index $h(f_i, r_i, ID)$ corresponding to the ith run. Tag profiles may be exploited to track certain behaviors of tagged objects. The reader can thus leverage tag profiles to monitor tags of interest without using exact tag IDs. If, however, manipulated by malicious readers, tag profiles may indirectly reveal some sensitive information of tagged objects (e.g., locations inferred from where tag profiles are extracted). Against this challenging issue, we can resort to a pioneer proposal in [42]. For conciseness, we (1) emphasize here the primary finding that the proposal in [42] can detect and jam signals from unauthorized readers without interfering the communication between reliable readers and tags, and (2) refer interested readers to [42] for more advanced details.

V. Performance Evaluation

In this section, we evaluate the performance of GREAT through simulations. Since GREAT is, to the best of our knowledge, the first protocol for cloning attack detection in anonymous RFID systems, we conduct simulations with no comparison other. Simulation results show that GREAT can detect cloning attacks in an anonymous RFID system fairly fast with required accuracy. When, for example, six cloned IDs hide among 50,000 tag IDs, GREAT can detect the cloning attack in only 75.5 seconds with probability at least 0.99.

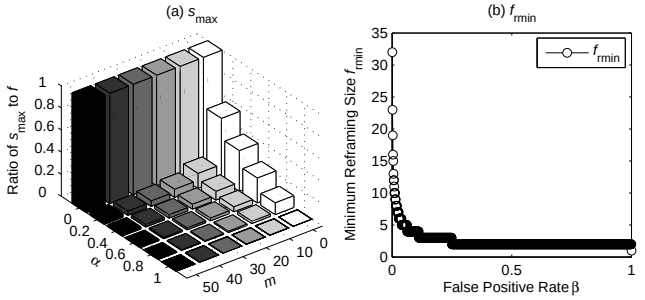


Fig. 4. Parameter setting. (a) The maximum number $s_{\max}$ of slots in an f-slotted frame to verify for satisfying tolerance number m of cloned IDs and false negative rate α. (b) The minimum reframing size f_{rmin} to reframe collision slots for satisfying false positive rate β.

A. Environment Configuration

We simulate the anonymous RFID system defined in Section II: An RFID reader and many tags, including genuine tags and cloned tags, communicate via a single channel, using a power level high enough to drown background noise [11], [26], [32]. This scenario is not that complex but general enough for us to acquire insights for cloning attack detection in anonymous RFID systems and to validate the proposed detection protocol. Scenarios of our future interest are, for example, with channel errors, multiple readers, multiple channels, or multiple subsystems for accommodating all tags [31], [43].

The primary performance metric is the execution time of GREAT for satisfying required detection accuracy. Slot timings are set according to the Philips I-CODE specification [6]: A reader requires $t_e = 0.4$ ms to detect an empty slot or a non-empty slot, and $t_c = 0.8$ ms to detect a singleton slot or a collision slot. Detection accuracy, by Corollary 2, is lower bounded by a function of false negative rate α and false positive rate β, $1 - \alpha + \varphi(\alpha, \beta)$, where $0 \leq \varphi(\alpha, \beta) \leq \alpha\beta$. Therefore, given required false negative rate α, GREAT is expected to detect the cloning attack with accuracy no less than $1 - \alpha$. The maximum number $s_{\max}$ of slots in an f-slotted frame to verify for satisfying α and the minimum reframing size f_{rmin} to reframe collision slots for satisfying β are determined by Theorem 1 and Theorem 2, respectively. As shown in Figure 4(a), $s_{\max}$ is equal to f for $\alpha = 0$ and decreases with both α and tolerance number m of cloned IDs for $0 < \alpha \leq 1$. Figure 4(b) plots f_{rmin} with varying β; $f_{\text{rmin}} = 32$ is enough for GREAT to satisfy $\beta = 0.001$. It is worth mentioning that in Figure 4(b) the fat segments are due to overlapping circles. We sample the false positive rate β with a relatively high density so that interested readers can easily capture the varying trend of the initial statistics.

B. Varying Frame Size f

We first investigate the impact of frame size f on the execution time of GREAT. Figure 5(a) shows the results under scenarios with false negative rate $\alpha = 0$, false positive rate $\beta = 0.001$, $m + 1 = 1$ cloned IDs, and ID cardinality $n =$ 1,000, 1,500, and 2,000. An interesting finding is that, given a certain n, the execution time of GREAT is not a monotonically increasing function of f. As f increases, the

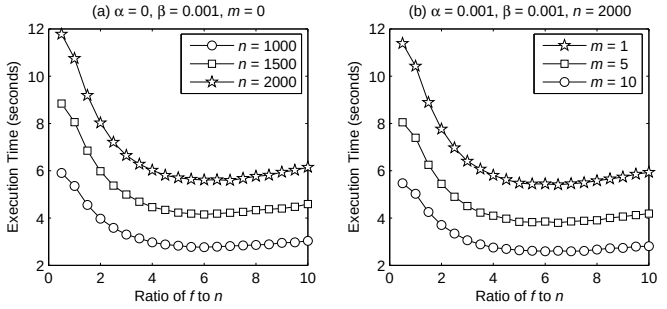


Fig. 5. Execution time of GREAT with varying frame size f under given ID cardinality n, tolerance number m of cloned IDs, false negative rate α, and false positive rate β.

execution time first decreases and then increases, approaching the minimum at $f \approx 6n$. Such variation of the execution time is essentially related to the variation of the numbers of empty, singleton, and collision slots. Intuitively, as f increases, the number of empty slots increases, the number of singleton slots increases up to $n - (m + 1) = n - 1$, while the number of collision slots decreases down to $m + 1 = 1$. By the GREAT design (Section IV-A), collision slot reframing makes a collision slot take more time than does an empty or a single slot. The execution time of GREAT thus decreases if the time reduction by collision slots exceeds the time increase by empty and singleton slots, and increases otherwise.

C. Varying Tolerance Number m of Cloned IDs

We now investigate the impact of tolerance number m of cloned IDs on the execution time of GREAT. Figure 5(b) shows the results under scenarios with false negative rate $\alpha = 0.001$, false positive rate $\beta = 0.001$, ID cardinality $n = 2{,}000$, and $m + 1 = 2$, 6, and 11 cloned IDs. An obvious observation on the results is that, when $m > 0$, the execution time varies following the same trend as when $m = 0$ (Figure 5(a)) with varying f. As f increases, the execution time first decreases and then increases, approaching the minimum at $f \approx 6n$. Another observation on the results is that a higher m yields faster detection. The execution time of GREAT depends on how many slots among f ones to verify. By Theorem 1, given certain α and f, the maximum number of slots to verify is $s_{\max} = \lceil (1-\alpha^{\frac{1}{m+1}})f \rceil$ and decreases with m; so the execution time decreases with m.

D. Varying ID Cardinality n

We further evaluate the execution time of GREAT in larger anonymous RFID systems with ID cardinality $n = 5,000$ to $50,000$. For ease of presentation, we report the results under scenarios only when frame size $f = 6n$ in Tables I and II. Table I reports the execution time with false negative rate $\alpha = 0.001$, false positive rate $\beta = 0.001$ and varying tolerance number m of cloned IDs. Given a certain m, the execution time increases with n; given a certain n, the execution time decreases with m. Table II reports the execution time with $\beta = 0.001$, $m = 5$, and varying α. Given a certain α, the execution time increases with n; given a certain n, the execution time decreases with α. In summary, (1) given certain α and m, the execution time increases with n; and (2) given a certain n, higher α and m yield faster detection.

TABLE I
Execution Time of GREAT with varying ID cardinality n, varying tolerance number m of cloned IDs, frame size $f = 6n$, false negative rate $\alpha = 0.001$, and false positive rate $\beta = 0.001$

n	Execution Time in Seconds				
	$m = 2$	$m = 4$	$m = 6$	$m = 8$	$m = 10$
5,000	12.6	10.5	8.8	7.5	6.5
10,000	25.3	21.0	17.6	15.1	13.1
15,000	38.0	31.6	26.5	22.6	19.7
20,000	50.7	42.2	35.3	30.2	26.2
25,000	63.3	52.7	44.1	37.7	32.8
30,000	76.0	63.3	53.0	45.3	39.4
35,000	88.7	73.8	61.8	52.8	45.9
40,000	101.4	84.3	70.6	60.3	52.5
45,000	114.0	94.9	79.5	67.9	59.1
50,000	126.8	105.4	88.3	75.4	65.6

TABLE II
Execution Time of GREAT with varying ID cardinality n, tolerance number $m = 5$ of cloned IDs, frame size $f = 6n$, varying false negative rate α, and false positive rate $\beta = 0.001$

n	Execution Time in Seconds			
	$\alpha = 0.002$	$\alpha = 0.003$	$\alpha = 0.005$	$\alpha = 0.010$
5,000	9.0	8.7	8.2	7.5
10,000	18.1	17.4	16.5	15.1
15,000	27.3	26.2	24.7	22.6
20,000	36.3	34.9	33.0	30.2
25,000	45.4	43.7	41.3	37.7
30,000	54.5	52.4	49.5	45.3
35,000	63.6	61.1	57.8	52.8
40,000	72.7	69.9	66.0	60.3
45,000	81.7	78.6	74.3	67.9
50,000	90.8	87.3	82.6	75.5

VI. Conclusion and Future Work

We have studied cloning attack detection in anonymous RFID systems. To enable and secure privacy-sensitive applications in anonymous RFID systems, we cannot simply turn to existing cloning attack detection protocols that require the knowledge of tag IDs. We therefore tackle cloning attack detection in anonymous RFID systems without requiring tag IDs as a priori and propose a pioneer protocol. The proposed protocol leverages unreconciled collisions to uncover cloning attacks. Simulation results show that the proposed protocol can detect cloning attacks in anonymous RFID systems fairly fast with required accuracy. Future work lies in error correction coding against channel errors [31] and adaptation of the proposed protocol to multi-reader, multi-channel, or multi-subsystem scenarios [43]. Of conceivable challenge is the adaptation to multi-reader scenarios. As when multiple readers are necessary for monitoring tags, it is possible that no reader covers some cloned tag(s) and corresponding genuine tag(s) in its communication region. If this is the case, readers may hardly find any reconciled collision and therefore the proposed protocol fails to detect cloning attacks. Further efforts are thus dedicated primarily to cloning attack detection in multi-reader anonymous RFID systems.

Acknowledgment

This work is partially supported by HK RGC PolyU 5299/11E and ZJNSF LR12F02002. The authors would also

like to sincerely thank Editors and reviewers for their thoughtful, constructive suggestions and comments.

REFERENCES

[1] A. Juels, "RFID security and privacy: A research survey," *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 2, pp. 381–394, 2006.

[2] D. Delen, B. Hardgrave, and R. Sharda, "RFID for better supply-chain management through enhanced information visibility," *Production and Operations Management*, vol. 16, no. 5, pp. 613–624, 2007.

[3] B. Janz, M. Pitts, and R. Otondo, "Information systems and health care-ii: Back to the future with RFID: Lessons learned-some old, some new," *Communications of the Association for Information Systems*, vol. 15, no. 1, pp. 132–148, 2005.

[4] K. Koscher, A. Juels, V. Brajkovic, and T. Kohno, "EPC RFID tag security weaknesses and defenses: passport cards, enhanced drivers licenses, and beyond," in *ACM CCS*, 2009, pp. 33–42.

[5] EPC class-1 generation-2 RFID protocol V.1.0.9, http://www.epcglobalinc.org/home.

[6] Philips Semiconductors, "I-CODE Smart Label RFID Tags". [Online]. Available: http://www.semiconductors.philips.com/acrobat_download/other/identification/SL092030.pdf

[7] R. Koh, E. Schuster, I. Chackrabarti, and A. Bellman, "Securing the pharmaceutical supply chain," *Auto-ID Center MIT, White Paper*, 2003.

[8] L. Mirowski and J. Hartnett, "Deckard: a system to detect change of RFID tag ownership," *International Journal of Computer Science and Network Security*, vol. 7, no. 7, pp. 89–98, 2007.

[9] M. Lehtonen, F. Michahelles, and E. Fleisch, "How to detect cloned tags in a reliable way from incomplete RFID traces," in *IEEE RFID*, 2009, pp. 257–264.

[10] D. Zanetti, L. Fellmann, and S. Capkun, "Privacy-preserving clone detection for RFID-enabled supply chains," in *IEEE RFID*, 2010, pp. 37–44.

[11] M. Lehtonen, D. Ostojic, A. Ilic, and F. Michahelles, "Securing RFID systems by detecting tag cloning," *Pervasive Computing*, vol. 5538, pp. 291–308, 2009.

[12] M. Kodialam, T. Nandagopal, and W. Lau, "Anonymous tracking using RFID tags," in *IEEE INFOCOM*, 2007, pp. 1217–1225.

[13] E. Vahedi, V. Shah-Mansouri, V. Wong, I. Blake, and R. Ward, "Probabilistic analysis of blocking attack in RFID systems," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 3, pp. 803–817, 2011.

[14] G. Dean, "RFID weapons and armoury management system," *Retrieved August*, vol. 22, 2006.

[15] R. Harris, "Feasibility of radio frequency identification (RFID) and item unique identification (iuid) in the marine corps small arms weapons tracking system," DTIC Document, Tech. Rep., 2008.

[16] T. Dimitriou, "A lightweight RFID protocol to protect against traceability and cloning attacks," in *IEEE SecureComm*, 2006, pp. 59–66.

[17] S. Devadas, E. Suh, S. Paral, R. Sowell, T. Ziola, and V. Khandelwal, "Design and implementation of PUF-based unclonable RFID ICs for anti-counterfeiting and security applications," in *IEEE RFID*, 2008, pp. 58–64.

[18] J. Abawajy, "Enhancing RFID tag resistance against cloning attack," in *IEEE NSS*, 2009, pp. 18–23.

[19] S. Spiekermann and S. Evdokimov, "Privacy enhancing technologies for RFID - A critical investigation of state of the art research," in *IEEE Privacy and Security*, 2009.

[20] S. Sarma, "Introductory Talk: Some issues related to RFID and security," in *Workshop on RFID Security*, 2006.

[21] L. Bolotnyy and G. Robins, "Physically unclonable function-based security and privacy in RFID systems," in *IEEE PerCom*, 2007, pp. 211–220.

[22] Explosive growth projected in next five years for RFID tags, http://www.instat.com/press.asp?ID=1545.

[23] C. Tan, B. Sheng, and Q. Li, "Secure and serverless RFID authentication and search protocols," *IEEE Transactions on Wireless Communications*, vol. 7, no. 4, pp. 1400–1407, 2008.

[24] C. Fan and S. Huang, "RFID authentication protocol in supply chains," in *The 3rd Joint Workshop on Information Security*, 2008.

[25] V. Lakafosis, A. Traille, H. Lee, E. Gebara, M. Tentzeris, G. DeJean, and D. Kirovski, "RFID-CoA: The RFID tags as certificates of authenticity," in *IEEE RFID*, 2011, pp. 207–214.

[26] M. Kodialam and T. Nandagopal, "Fast and reliable estimation schemes in RFID systems," in *ACM MobiCom*, 2006, pp. 322–333.

[27] C. Qian, H. Ngan, and Y. Liu, "Cardinality estimation for large-scale RFID systems," in *IEEE PerCom*, 2008, pp. 30–39.

[28] Y. Zheng, M. Li, and C. Qian, "PET: Probabilistic estimating tree for large-scale RFID estimation," in *IEEE ICDCS*, 2011, pp. 37–46.

[29] V. Shah-Mansouri and V. Wong, "Cardinality estimation in RFID systems with multiple readers," *IEEE Transactions on Wireless Communications*, vol. 10, no. 5, pp. 1458–1469, 2011.

[30] M. Shahzad and A. Liu, "Every bit counts: fast and scalable RFID estimation," in *ACM MobiCom*, 2012, pp. 365–376.

[31] T. Tran, T. Nguyen, B. Bose, and V. Gopal, "A hybrid network coding technique for single-hop wireless networks," *IEEE Journal on Selected Areas in Communications*, vol. 27, no. 5, pp. 685–698, 2009.

[32] S. Chen, M. Zhang, and B. Xiao, "Efficient information collection protocols for sensor-augmented RFID networks," in *IEEE INFOCOM*, 2011, pp. 3101–3109.

[33] G. Owen, *Discrete mathematics and game theory*. Springer, 1999.

[34] N. Kothari, R. Mahajan, T. Millstein, R. Govindan, and M. Musuvathi, "Finding protocol manipulation attacks," in *ACM SIGCOMM*, 2011, pp. 26–37.

[35] L. Roberts, "ALOHA packet system with and without slots and capture," *ACM SIGCOMM Computer Communication Review*, vol. 5, no. 2, pp. 28–42, 1975.

[36] J. Capetanakis, "Tree algorithms for packet broadcast channels," *IEEE Transactions on Information Theory*, vol. 25, no. 5, pp. 505–515, 1979.

[37] A. Broder and M. Mitzenmacher, "Network applications of bloom filters: A survey," *Internet Mathematics*, vol. 1, no. 4, pp. 485–509, 2004.

[38] K. Bu, B. Xiao, Q. Xiao, and S. Chen, "Efficient pinpointing of misplaced tags in large RFID systems," in *IEEE SECON*, 2011, pp. 287–295.

[39] ——, "Efficient misplaced-tag pinpointing in large RFID systems," *IEEE Transactions on Parallel and Distributed Systems*, vol. 23, no. 11, pp. 2094–2106, 2012.

[40] Q. Xiao, K. Bu, B. Xiao, and L. Sun, "Efficient Protocol Design for Dynamic Tag Population Monitoring in Large-Scale RFID Systems," *Concurrency and Computation: Practice and Experience*, no. PrePrints, 2012.

[41] X. Liu, S. Zhang, K. Bu, and B. Xiao, "Complete and fast unknown tag identification in large RFID systems," in *IEEE MASS*, 2012, pp. 47–55.

[42] S. Gollakota, H. Hassanieh, B. Ransford, D. Katabi, and K. Fu, "They can hear your heartbeats: Non-invasive security for implantable medical devices," in *ACM SIGCOMM*, 2011, pp. 2–13.

[43] A.-H. Mohsenian-Rad, V. Shah-Mansouri, V. Wong, and R. Schober, "Distributed channel selection and randomized interrogation algorithms for large-scale and dense RFID systems," *IEEE Transactions on Wireless Communications*, vol. 9, no. 4, pp. 1402–1413, 2010.

Kai Bu received the BSc and MSc degrees in computer science from the Nanjing University of Posts and Telecommunications, Nanjing, China, in 2006 and 2009, respectively. He is currently a PhD candidate in the Department of Computing at The Hong Kong Polytechnic University, Hong Kong. His research interests include RFID and wireless networks. He is a recipient of the Outstanding Master's Thesis Award in Jiangsu Province, China, 2010 and the Best Paper Award of IEEE/IFIP EUC 2011. He is a member of the IEEE Communications Society.

Xuan Liu received the MSc degree from the School of Computer Science and Engineering, National University and Defense, China, in 2008. Currently, she is a PhD candidate in the Department of Computing at The Hong Kong Polytechnic University, Hong Kong. Her research interests include distributed computing systems, mobile computing, focusing on wireless sensor networks and RFID systems.

Jiaqing Luo received the BSc and MSe degrees from the University of Electronic Science and Technology of China (UESTC), in 2004 and 2007, respectively, and the PhD degree from the Hong Kong Polytechnic University in 2011. Currently, he is a postdoctoral fellow at the School of Computer Science & Engineering at UESTC. His research interests include peer-to-peer networks, wireless mobile ad hoc, and RFID systems.

Bin Xiao received the BSc and MSc degrees in electronics engineering from Fudan University, China, in 1997 and 2000, respectively, and the PhD degree in computer science from the University of Texas at Dallas in 2003. After his PhD graduation, he joined the Hong Kong Polytechnic University as an assistant professor. Currently, he is an associate professor in the Department of Computing at The Hong Kong Polytechnic University, Hong Kong. His research interests include mobile cloud computing, data management, network security, wireless sensor networks and RFID systems. He is an associate editor for the International Journal of Parallel, Emergent and Distributed Systems. He is a recipient of the Best Paper Award of IEEE/IFIP EUC 2011. He is a senior member of the IEEE.

Guiyi Wei received his Ph.D. in December 2006 from Zhejiang University. He has research interests in wireless networks, mobile computing, cloud computing, social networks and network security. He is a full professor of the School of Computer Science and Information Engineering at Zhejiang Gongshang University. He is also the director of the Networking and Distributed Computing Laboratory.