Fuzzy Systems and Data Mining VIII
A.J. Tallón-Ballesteros (Ed.)

doi:10.3233/FAIA220375

An Accurate Cardinality Estimation Scheme for Cloned Tags Under the Capture Effect

Bin WANG [1], Tiancong WANG
School of Information Engineering, Yangzhou University, Jiangsu, China

Abstract. The cloning attack is harmful to RFID systems. So, estimating the number of cloned tags is helpful to evaluate potential security risks for RFID systems. This paper studies the problem of estimating the number of cloned tags to present a cardinality estimation scheme CECT when there exist unknown tags and the capture effect. CECT scheme requires a RFID reader to first predict responses of the known tags by a virtual frame executed in terms of the ALOHA protocol. Then the reader collects responses from active tags over a channel with the capture effect. Simulation results show that under the given number of unknown tags and capture effect parameter, CECT can meet the required estimation accuracy and reliability. Under the same parameters, the accuracy is improved by more than 20%.

Keywords. RFID, cloning attack, cardinality estimation, the capture effect

1. Introduction

1.1. Background

As a kind of data communication technology with the advantage of Non-line-of-sight automatic identification [1], RFID based applications have been popular with the development of the Internet of things. Recently, as the unit cost of RFID tags is greatly reduced, RFID technology has been widely used in various fields such as retail stores [2,3], warehouse management [4,5], etc.

A typical RFID system consists of a reader, RFID tags and a back-end system. A reader communicates with RFID tags using radio waves over UHF channel [6]. Tags transmit responses by harvesting energy from the wireless signal transmitted by the reader. The reader relays the received responses to a back-end system for further processing.

This paper proposed a CECT (Cardinality Estimation for Cloned Tags) scheme, this scheme is designed to accurately estimate the number of cloned tags under the capture effects in RFID systems. The contributions of this design are as follows. First, we con-

[1]Corresponding Author: Bin WANG, Associate professor of Department of Electronics and Communication Engineering, Information Engineering College, Yangzhou University, Jiangsu, China; E-mail: bwang@yzu.edu.cn

sider how to overcome the interference from unknown tags and the capture effect when considering the response slot distribution. Second, we derive the necessary number of rounds to meet the given accuracy and reliability parameters when estimating the number of cloned tags. The reliability and accuracy of the scheme can be proved by the simulation results.

1.2. Related Work

At present, in spite of popularity of RFID systems, there are still some issues to be addressed, such as the cloning attack [7]. Solution to this issue is helpful for reducing system administration cost and security risk. This paper focuses on estimation of the number of cloned tags, when there exist unknown tags and the impact of capture effect cannot be ignored over the tag-to-reader channel.

As RFID tags may be compromised by an adversary, internal information kept by tags may be disclosed. Furthermore, an adversary can mount the cloning attack to generate replicas with the same IDs as the compromised genuine tags [8]. The cloning attack will seriously interfere with normal operations of RFID systems and lead to potential financial loss and security risks. As a result, a lot of research works are concerned with detecting or identifying cloning tags for RFID system [9,10,11]. The concept of blocker tags is similar to cloning tags [12]. That is, blocker tags will be added into the current system and equipped with some genuine tags' IDs. Then blocker tags interfere with the interaction between the corresponding genuine tags and a reader. For example, information about some high-valued goods should be kept confidential, etc. Xie et al. [13] proposed the SEBU (Simultaneous Estimation of the Blocked tag size and the Unknown tag size) protocol to estimate the number of blocker tags and unknown tags simultaneously over a perfect tag-to-reader channel. When the number of unknown tags is large, the ratio of empty slots in the response frame will be small. Hence, they can estimate the total set size, and obtain the unknown tags set size. Then, the SEBU protocol estimates the number of blocked tags by analyzing the collision probability of a slot. When two or more RFID tags respond in the same time slot, it is generally assumed that communication collision occurs. However, the signal strength of the tag most close to the reader will be stronger than that of other tags. So, the signal from the tag most close to the reader can be successfully decoded by the reader with a certain probability and an assumed collision slot will be considered to be a singleton slot. This phenomenon is known as the capture effect [14]. Thus, the capture effect will interfere with the accuracy of the estimated result of SEBU. We provide simulation results to show the impact of the capture effect on SEBU in section 3.

1.3. Basic Method

When there exist unknown tags and the capture effect in RFID systems, we propose a scheme CECT (Cardinality Estimation for Cloned Tags) to estimate the number of cloned tags in RFID system. Assuming that there exists one or more cloning tag for a genuine tag, CECT adopts the framed ALOHA protocol as the communication paradigm between readers and RFID tags. A reader selects r and f for the set X of known tags. r is a random number, f is the frame length. The time slots selected by the known tags in a virtual frame V is also random. The status of each slot in the virtual frame is recorded

by a prediction vector F. If there is only one tag assigned to a slot $V[w]$, it recorded as $F[w] =$'1' and called a singleton slot; If there are at least two tags assigned to slot $V[w]$, it recorded as $F[w] =$'c' and called a collision slot; If there is no tag assigned to slot $V[w]$, it recorded as $F[w] =$'0' and called an empty slot.

The reader executes the ALOHA protocol with the active tags by broadcasting the parameters r and f. Having decoded the received tags' response as a response frame R, an execution vector G is generated. Each component $G[w]$ of the vector G is defined in the same way as the prediction vector F. By comparing status of the prediction vector F with the execution vector G, an estimator for the number of cloned tags is designed in this paper by taking into account the impact of the capture effect on the tags' response.

The following parts of this paper are arranged as follows. In Section 2, the system model is described and the detail of CECT is introduced. In Section 3, we analyzed the impact of the capture effect on the accuracy of the estimated result of CECT. Finally, we perform simulation experiments to evaluate the performance of CECT and make comparison with SEBU. This paper is concluded in Section 4.

2. The CECT Scheme

In this section, we describe the presented CECT scheme in detail by taking into account the influence of unknown tags and the capture effect. The CECT estimation process needs to be executed R rounds.

Table 1. The symbols used in this paper.

Symbol	description
n	the number of known tags
m	the number of cloned tags
p	the number of unknown tags
q_c	the probability of the capture effect
f	the frame length
r	the random number
m^*	the estimated value of m

2.1. System Model

In a RFID system, the known tags set is set to $X = \{x_1, x_2, \ldots, x_n\}$, the unknown tags set is set to $Z = \{z_1, z_2, \ldots, z_p\}$, $Y = \{y_1, y_2, \ldots, y_m\} \subset X$ is the subset of cloned tags in X. We assume that the attacker duplicates some cloning tag(s) for each cloned tag. When the reader interacts with a cloned tag by the ALOHA protocol, the corresponding cloning tag(s) will also send response(s) in the same time slot by the ALOHA protocol. n is the known quantity and m, p are unknown. Assuming there is exists the capture effect in the tag-to-reader channel, a real collision slot may have q_c probability to be decoded into a singleton slot mistakenly by the reader. The estimation accuracy and estimation reliability are recorded as ε and δ, respectively. The estimator (ε, δ) of the number m of cloned tags needs to compute $\widehat{m}$ and satisfy:

$$\Pr\left[\frac{|\widehat{m} - m|}{m} \leq \varepsilon\right] \geq 1 - \delta \tag{1}$$

2.2. Estimation framework

At each round of execution, active tags interact with the reader via the slotted ALOHA protocol. For ease of demonstration, we assume an expected tag set $T_t = \{0,1,2,3,4,5,6\}$, in which $\{5,6\}$ is the set of cloned tags and $\{7,8\}$ is the set of unknown tags. The cloning tag(s) for a specific genuine tag t is denoted by (t). For instance, the cloning tag(s) for the genuine tag 5 is denoted by (5). Then, the set of active tags is $A_t = \{0,1,2,3,4,5,(5),6,(6),7,8\}$. In Figure 1, we use '0', '1' , 'c' to denote an empty slot, a singleton slot, a collision slot respectively. Due to the existence of unknown tags and cloning tags, the actual response will be different from the expected result.

It is shown in Figure 1 that the genuine tag 5 picks a singleton slot with index 0 in the virtual frame, while the corresponding slot in the response frame is a collision slot. The reason is that the cloning tag(s) (5) also selects the same slot to respond. As far as the 6th slot in the response frame is concerned, the unknown tag 8 and the genuine tag 2 pick the same slot to respond to yield a collision slot.

In the following subsection, we describe the principle behind the CECT scheme.

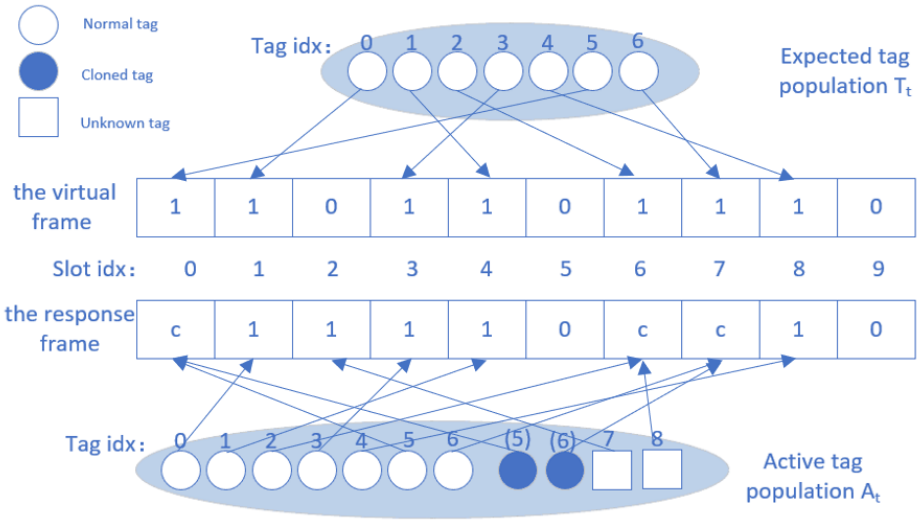

Figure 1. Simple schematic diagram of CECT.

2.3. Detailed Process of CECT

In any round k, in the first step, the reader selects a r_k and f to construct a virtual frame. There are several time slots in the virtual frame, and the index of a time slots ranges from 0 to $f-1$. Computes the index $w = H(t_{id}, r_k)$ of the expected tags $t_{id} \in X$ selection slot by the hash function $H(\cdot)$.

The vectors for all f entries are generated as F_k by the reader, and all entries are initialized to '0's. The subsequent settings of F_k in the virtual frame are as follows:

(1) If only one expected tag is assigned to the wth time slot, it is a singleton slot and $F_k[w]$ ='1'.

(2) If more than one expected tags are assigned to the wth time slot, it is a collision slot and $F_k[w]=$'c'.

Next, the reader broadcasts r_k and f to active tags. Computes the index $w = H(t_{id}, r_k)$ of each tags $t_{id} \in X$. A 10-bit response message is transmitted in the wth slot $R_k[w]$ in the response frame to distinguish a collision slot from a singleton slot. Perform the same steps for each cloning tag (resp., unknown tag).

The vectors with f entries are generated as G_k by the reader when receives the response frame, and all entries are initialized to '0's. G_k is set according to the reader's sequential scan of the time slots in the response frame R_k:

(3) If the wth time slot is detected as a singleton slot, set $G_k[w]$='1'.

(4) If the wth time slot is detected as a collision slot, set $G_k[w]$='c'.

Let $S_{00}^k = \{w|0 \le w \le f-1, F_k[w]=0 \cap G_k[w]=0\}$ and $N_{00}^k = |S_{00}^k|$ be the number of elements in set S_{00}^k. S_{00}^k records the index w of the time slots where the event $[F_k[w]=0 \cap G_k[w]=0]$ occurs.

The event $[F_k[w]=0 \cap G_k[w]=0]$ means there is no expected tag $t_{id} \in X$ and unknown tag responding in the time slot $R_k[w]$. Its probability can be expressed by $\Pr[F_k[w]=0 \cap G_k[w]=0] = \left(1-\frac{1}{f}\right)^{n+p}$.

So the expectation value of N_{00}^k is: $E\left[N_{00}^k\right] = f\left(1-\frac{1}{f}\right)^{n+p} \approx f \cdot e^{-\left(\frac{n+p}{f}\right)}$, we obtain:

$$e^{\left(\frac{n+p}{f}\right)} = \frac{f}{E\left[N_{00}^k\right]} \tag{2}$$

Let $N_{00} = \frac{1}{R}\sum_{k=1}^{R} N_{00}^k$, $p_{00} = e^{-\left(\frac{n+p}{f}\right)}$, $\mu_{00} = E[N_{00}] \approx f \cdot p_{00}$, $\sigma_{00} = Var[N_{00}] \approx \frac{Var\left[N_{00}^k\right]}{R} = \frac{f}{R} \cdot p_{00} \cdot (1-p_{00})$. Replace $E\left[N_{00}^k\right]$ with N_{00} in Eq. (2). We get an estimator $\widehat{s}$ for $s = e^{\left(\frac{n+p}{f}\right)}$:

$$\widehat{s} = \frac{f}{N_{00}} \tag{3}$$

Let $S_{1c}^k = \{w|0 \le w \le f-1, F_k[w]=1 \cap G_k[w]=c\}$ and $N_{1c}^k = |S_{1c}^k|$ be the number of elements in set S_{1c}^k. S_{1c}^k records the index w of the time slots where the event $[F_k[w]=1 \cap G_k[w]=c]$ occurs.

$[F_k[w]=1 \cap G_k[w]=c]$ means one of the following two events occurs:

E_1:The supposed singleton slot picked by some uncloned tag $t_{id} \in X/Y$ is also picked by some unknown tag(s) to respond and the slot $R_k[w]$ is not affected by the capture effect in the response frame;

E_2:The supposed singleton slot is actually picked by some cloned tag $t_{id} \in Y$ and the slot $R_k[w]$ is not affected by the capture effect;

$$\Pr[E_1] = \binom{n-m}{1}\frac{1}{f}\left(1-\frac{1}{f}\right)^{n-1}\left(1-\left(1-\frac{1}{f}\right)^{p}\right)(1-q_c) \approx \frac{n-m}{f}e^{-\left(\frac{n}{f}\right)}\left(1-e^{-\left(\frac{p}{f}\right)}\right)(1-q_c)$$

$$\Pr[E_2] = \binom{m}{1}\frac{1}{f}\left(1-\frac{1}{f}\right)^{n-1}(1-q_c) \approx \frac{m}{f}e^{-\left(\frac{n}{f}\right)}(1-q_c)$$

$$E\left[N_{1c}^k\right] = f \cdot [\Pr[E_1] + \Pr[E_2]] = \left((n-m)\,e^{-\left(\frac{n}{f}\right)}\left(1-e^{-\left(\frac{p}{f}\right)}\right) + me^{-\left(\frac{n}{f}\right)}\right) \tag{4}$$

By Eq. (4), we obtain: $n-m=\left(ne^{-\left(\frac{n}{f}\right)}-\frac{E\left[N_{1c}^{k}\right]}{1-q_c}\right)\cdot e^{\left(\frac{n+p}{f}\right)}$, $m=n-u\cdot s$, where

$$u=\left(ne^{-\left(\frac{n}{f}\right)}-\frac{E\left[N_{1c}^{k}\right]}{1-q_c}\right). \tag{5}$$

Let $N_{1c}=\frac{1}{R}\sum_{k=1}^{R}N_{1c}^{k}$, $p_{1c}=\left(ne^{-\left(\frac{n}{f}\right)}-(n-m)\,e^{-\left(\frac{n+p}{f}\right)}\right)\cdot\frac{(1-q_c)}{f}$, $E\left[N_{1c}^{k}\right]=\mu_{1c}\approx f\cdot p_{1c}$, $\sigma_{1c}=Var\left[N_{1c}\right]\approx\frac{Var\left[N_{1c}^{k}\right]}{R}=\frac{f}{R}\cdot p_{1c}\cdot(1-p_{1c})$. Replace $E\left[N_{1c}^{k}\right]$ with N_{1c} in Eq. (5) to get the unknown tags estimator $\widehat{u}$:

$$\widehat{u}=\left(ne^{-\left(\frac{n}{f}\right)}-\frac{N_{1c}}{1-q_c}\right) \tag{6}$$

Use $\widehat{u}$ and $\widehat{s}$ defined in Eqs. (6) and (3) to replace u and s defined in $m=n-u\cdot s$ respectively to yield $\widehat{m}=n-\widehat{u}\cdot\widehat{s}$ as an estimator for m.

We omit the details to derive the necessary number of rounds to satify the required estimation accuracy for the number of cloned tags. The number of rounds R shall satisfy the following: $R=\max\left[\frac{f\cdot e^{\left(\frac{n+p}{f}\right)}\cdot c_{1c}}{4(n-m)\cdot\varepsilon\cdot(1-q_c)},\frac{e^{\left(\frac{n+p}{f}\right)}c_{00}}{4\eta}\right]$. We can obtain a (ε,δ) estimator for the number of cloned tag m. c_{00} is a constant satisfy: $\Pr\left[-c_{00}\le\frac{N_{00}-\mu_{00}}{\sigma_{00}}\le c_{00}\right]=1-\delta$, c_{1c} is a constant satisfy: $\Pr\left[-c_{1c}\le\frac{N_{1c}-\mu_{1c}}{\sigma_{1c}}\le c_{1c}\right]=1-\delta$, $\eta=\min\left(\left(\frac{1}{1-\varepsilon}-1\right),\left(1-\frac{1}{1+\varepsilon}\right)\right)$.

3. Simulation Results

In this section, we will evaluate the performance of the CECT scheme through python simulation experiments, and compare the estimation accuracy of CECT with SEBU under the specified parameter settings. Our simulations will choose $\varepsilon=0.1,\delta=0.1$ as the target estimation accuracy and reliability parameters respectively.

$E\left[m^*/m\right]$ is the estimation accuracy computed by our simulations where m^* is our simulations estimation result of the number of cloned tags.

3.1. Impact of Total Tags Changes

In order to see the impact of the total number of tags on estimation accuracy, let the set of total tags is $[3000,10000]$. Both the unknown tags and cloned tags are set to 500. The parameter of capture effect is set to 0.1. We can see from Figure 2 that our scheme is about 20% more accurate than SEBU under the capture effect. As SEBU does not consider the capture effect, the estimation accuracy is lower. On the other hand, the estimation accuracy of CECT fluctuates around the ideal value 1, which is better than SEBU under the capture effect.

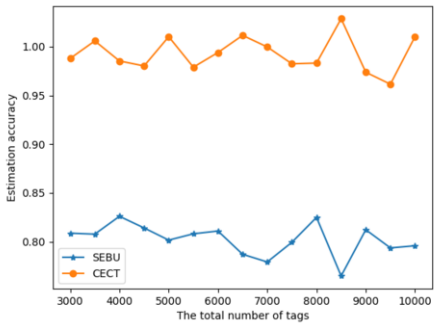

Figure 2. Impact of the total number of tags.

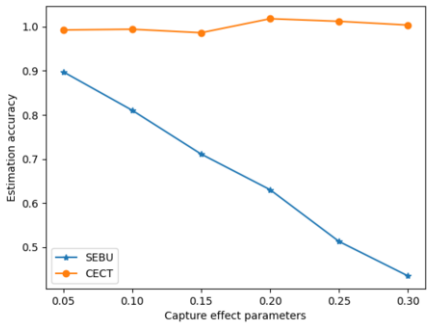

Figure 3. Influence of capture effect parameters.

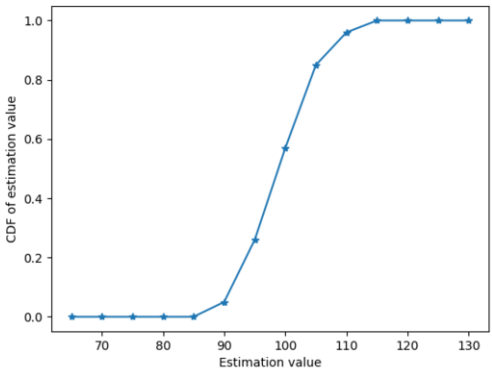

Figure 4. The Cumulative Distribution Function of CECT.

3.2. Influence of the Parameter of Capture Effect

Next, We set the capture effect parameters to $[0.05, 0.3]$. It can be clearly seen from Figure 3 that when the parameter of capture effect increases, the estimation accuracy of SEBU degrades greatly. The estimation results of CECT under different capture effect parameters are relatively stable and fluctuates around the ideal value 1. Our estimator is designed according to the difference between the virtual frame and the response frame. The expected number of singleton slots in the virtual frame that become collision slots in the response frame reflects the influence of the capture effect. Therefore, it is necessary to consider the capture effect parameter when cardinality estimation for cloned tags.

3.3. The CDF of CECT

We computer the average result of 100 experiments and obtain the CDF (cumulative distribution function) of CECT, which is used to evaluate the estimation reliability. The result is that $\Pr[90 \leq m^* \leq 110] \approx 0.909$. This shows that CECT can meet the estimation reliability requirement.

4. Conclusion

In this paper, we proposes a CECT scheme for estimating the number of cloned tags in an RFID system under the capture effect and the existence of unknown Tags. The empty slots in both the virtual frame and response frame is impacted by the number of unknown tags while the expected singleton slots in the virtual frame that become collision slots in the response frame reflect the influence of the capture effect. Based on these information, CECT computes an estimator of the number of cloned tags. In comparison with SEBU, simulation result shows that CECT is more robust to the capture effect. The cumulative distribution function of CECT demonstrates that CECT can meet the estimation reliability requirement under the capture effect and the existence of unknown tags.

References

[1] Chawla, Vipul, Dong, Sam, Ha. An overview of passive RFID. IEEE Commun Mag. 2007 Sep;45(9):11-17.

[2] Massimo B, Antonio R, Giovanni R, Andrea V. Testing an RFID receiving gate for improving process accuracy in fashion and apparel retail. Proceedings of the 3rd International Forum on Research and Technologiesfor Society and Industry (RTSI); 2017 Sept 1;p. 1-5.

[3] Choi T M, Yeung W K, Cheng T E, Yue X. Optimal scheduling, coordination, and the value of RFID technology in garment manufacturing supply chains. IEEE Transactions on Engineering Management. 2018 Feb;65(1):1-13.

[4] Shen S, Dong W. Research on warehouses management based on RFID and WSN technology. Proceedings of International Workshop on Database Technology & Applications; 2010.

[5] Lian X, Zhang X, Weng Y, Duan Z. Warehouse logistics control and management system based on RFID. Proceedings of IEEE International Conference on Automation & Logistics; 2007 Oct.

[6] Fennani B, Hamam H, Dahmane A O. RFID overview. Microelectronics (ICM) 2011 International Conference on IEEE; 2011;pp. 1-5.

[7] Kasper T , Maurich I V, Oswald D, Paar C. Cloning cryptographic RFID cards for 25$. Proc. 5th Benelux Workshop Inf. Syst. Security. 2010;p. 1-15.

[8] Mirowski L. Exposing clone RFID tags at the reader. Proceedings of the 12th IEEE International Conference Trust, Security and Privacy in Computing and Communications; 2013 Jul 1;p. 1669-1674.

[9] Okpara S O. Detecting cloning sttack in Low-Cost passive RFID tags. An Analytic Comparison between KILL Passwords and Synchronized Secrets Obinna. 2015.

[10] Bu K, Xu M, Liu X, Luo J, Zhang S, Weng M. Deterministic detection of cloning attacks for anonymous RFID systems. Industrial Informatics, IEEE Transactions on. 2015;11(6):1255-1266.

[11] Lehtonen M, F Michahelles, Fleisch E. How to detect cloned tags in a reliable way from incomplete RFID traces. Proceedings of 2009 IEEE International Conference on IEEE; 2009 May 28;p. 257-264.

[12] Liu X, Li K, Jie W, Liu A X, Xin X. RFID cardinality estimation with blocker tags. Proceedings of Computer Communications; 2015 Aug 24;p.1-9.

[13] Liu X, Xie X, Zhao X, Wang K, Li K, Liu A X, Guo S, Wu J. Fast identification of blocked RFID tags. IEEE Transactions on Mobile Computing. 2018:1-1.

[14] Su S L, Chih T H, Tsai Y C, Liao H C, Wang Y C. A power control scheme to exploit capture effect with fairness consideration in WLAN. Wireless Personal Communications. 2021;118(5):1-16.