Multi-attribute Counterfeiting Tag Identification Protocol in Large-Scale RFID System

Dali Zhu[1,2], Wenjing Rong[1,2(✉)], Di Wu[1], and Na Pang[1,2]

[1] Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China
{zhudali, rongwenjing, wudi, pangna}@iie.ac.cn
[2] School of Cyber Security, University of Chinese Academy of Sciences, Beijing, China

Abstract. Counterfeiting products identification is the main application of RFID technology. Among all the RFID security problems, counterfeiting tag identification is an urgent issue with rapid growth of counterfeiters. In this paper, a multi-attribute counterfeiting tag identification protocol based on multi-dimension dynamic bloom filter in large-scale RFID system is proposed. Dynamic bloom filters for tag's attributes: identity information ID and location information angle value, are first brought as criterion of counterfeiting tag identification. Different from previous probabilistic approaches, our protocol not only identifies unknown tags, but also first solves problem that counterfeiters hold the same ID with genuine ones. Furthermore, our protocol can detect and verify counterfeiting tags' identity. Performance analysis shows that especially with huge amount of tags, our protocol can achieve higher identification efficiency with reasonable time cost.

Keywords: Multi-attribute · Location · Identification
Bloom filter · Security · RFID

1 Introduction

Radio frequency identification (RFID) is a ubiquitous technology applied in numerous automated identification systems such as supply chain, manufacturing management, pharmaceuticals and many other everyday life applications. So security of large-scale RFID system becomes quite important. Among all the security problems, counterfeiting tag identification is an urgent issue since the quantity of counterfeiting products grows dramatically in recent years [1]. For example, counterfeiting products can forge a tag to sneak into genuine products which results in great economic loss. According to survey in [2], economic loss leads by counterfeiting products is more than $600 billion and is growing with yearly progressive increase. So accurate and fast counterfeiting tag identification is very important to many applications.

In this paper, a multi-attribute counterfeiting tag identification protocol based on framed slotted ALOHA algorithm in large-scale RFID system is proposed. Different from other framed slotted ALOHA based schemes, multi-dimension dynamic bloom

S. Qing et al. (Eds.): ICICS 2017, LNCS 10631, pp. 352–362, 2018.
https://doi.org/10.1007/978-3-319-89500-0_31

filter is applied in our protocol, which indicates that tag has more than one attribute. When talked about tag's attribute, the only one comes to mind is tag's identity ID. In fact, reader can measure angle between tag and itself after scanning. So, our protocol first utilizes two attributes: tag identity ID and angle value. In previous works [1, 17, 18], counterfeiting tag is defined as one which is not in back-end server's database. However, there exists a condition that a tag which holds the same ID with a genuine one is attached to a counterfeiting item. In this condition, tag's angle value is a good criterion to point out counterfeiting tags. Our protocol is the first one to solve problem that counterfeiting tag forges the same ID with a genuine one. That is to say, our protocol can not only point out unknown tags, but also counterfeiting goods with genuine tag IDs. Also our protocol is suit for tag identification in large-scale RFID system. Even if quantity of RFID tags grows rapidly, identification efficiency can still be kept around an acceptable range. Compared with recently proposed methods, it can achieve higher identification efficiency, especially with huge amount of tags. And the time cost of our protocol is controlled in a reasonable range.

2 Related Works

The main usage of RFID tags in practice is identifying counterfeiting goods. In previous works like [1], counterfeiting tag is defined as one which is not in back-end server's database. Other studies [2, 3] call tags under this condition unknown tags. In previous studies, counterfeiting tag detection or they call it unknown tag detection, is classified into two categories: deterministic authentication and probabilistic estimation.

Deterministic authentication is mainly proposed in early works [5–8]. Weis et al. [5] propose a hash lock authentication scheme to protect tags from tracked. As its searching complexity is $O(N)$, where N is number of tags, it suffers from poor efficiency in large-scale RFID system. In order to reduce search complexity, Lu et al. [6] introduce a tree-based method with complexity of $O(log(N))$. Then they propose a new scheme which can achieve complexity of $O(1)$ in [7]. Recently, Chen et al. [8] introduce a token-based protocol whose overhead in both tag and reader is $O(1)$. However, schemes [6–8] are both tree-based protocols whose number of keys increases logarithmically with growth of tags.

In recent years, probabilistic estimation schemes [9–12] are gradually proposed. However, these methods are focus on estimating cardinality of tags. They cannot announce identities of counterfeiting tags. Also, there are several identity detection schemes [13–16]. But they are aimed to find missing tags. Yang et al. [17] first offer a framed slotted ALOHA based solution to detect counterfeiting tags or they call them unknown tags. Bianchi et al. [18] further improve this by introducing a standard bloom filter structure. Then Liu et al. [4] propose sampling filtering techniques based on bloom filter. However all these bloom filter based methods which leads to more collisions, haven't well utilized space of frame. Further, Gong et al. [1] provide a counterfeiting tag estimation scheme. But it cannot figure out counterfeiting tag. Later, schemes [3, 19] offer an indicator vector for tags which results in more overhead in tags. In contrast, our protocol not only points out unknown tags, but also counterfeiting goods with genuine tags. What's more, it can achieve a high detection efficiency with reasonable time cost.

3 Preliminary

3.1 System Model and Assumption

A typical RFID system consists of three entities: tags, readers and a back-end server. Reader is connected to back-end server through wired or wireless link with high computational ability. RFID tags are divided into three types: active, semi-active and passive tags. Our protocol mainly talks about passive tags. A reader interrogates and receives responses from a tag via transmitting a radio-frequency (RF) signal. Each tag is associated with identity information ID and location information angle value.

In our large-scale system model, reader is in the center and periodically scans tags. All tags are within reader's interrogation range. Tags include genuine ones and counterfeits. If identity and angle value of a tag are both stored in back-end server, this tag is a genuine one. The existence of counterfeiting tags includes two conditions. The first one is neither tag's identity or angle value is stored in back-end server, while the second one is a tag which holds the same ID with a genuine one is attached to a counterfeiting item. The first condition is usually proposed in previous works [1, 3, 17, 18]. However, problem in the second condition is first proposed and solved in this paper.

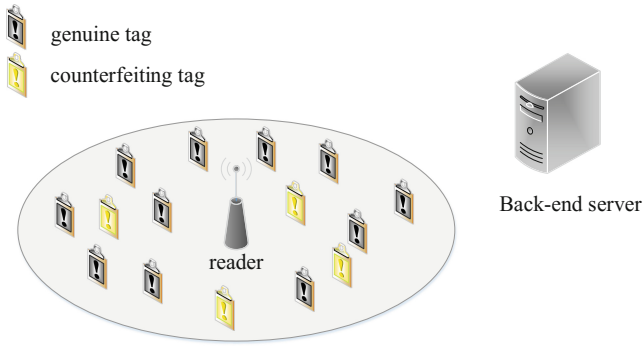


Fig. 1. System model

The whole process is divided in two interrogations by reader. When tag settles down in reader's interrogation range, it assumes that tags are all genuine ones and tags will be not transferred to another place before the second interrogation. Then reader scans tags and measures angle value between tag and itself by RSSI information which we will not describe in this paper. Afterwards, reader writes the corresponding angle value on each tag. So tag's attributes stores in tag are identity ID and angle value. As tag does not change places before the second interrogation, actual angle value between reader and tag will be identical with the angle value stored in tag. During period between the two interrogations, counterfeits can move into interrogation range. Counterfeit can forge the same ID with genuine one, however, it cannot forge actual angle value since counterfeit does not know accurate location of the one it forges in a large-scale RFID system. In the second interrogation, reader will authenticate tag's identity and angle value to find out counterfeits. The scenario is illustrated in Fig. 1.

3.2 Framed Slotted ALOHA Algorithm

Our protocol is based upon framed slotted ALOHA algorithm which is widely used in EPC Global C1G2 standard as its MAC-layer communication protocol. In framed slotted ALOHA algorithm, reader first broadcasts frame size f and random seed r. Each tag within interrogation range of the reader evaluates a hash function $h(f, r, ID)\ mod\ f$ to select a slot in frame. Slot is classified into three categories. Empty slot means that there is no reply in this slot, while singleton slot denotes that only one reply is in this slot, and collision slot indicates that there are two or more replies in this slot.

3.3 Problem Formulation

Assume that there is one reader and N tags and all the tags are within the range of reader. Some counterfeiting tags may be moved in due to some reasons. So among N tags, there are n counterfeits after the first interrogation. Each genuine tag holds tag's attributes which includes tag's identity information ID and tag's location information angle value written by reader. For counterfeiting tags, it can forge genuine tag's identity by following some regulations like EPC standard, and location information by randomly guess. However it's hard for counterfeits to map identity information to location information since they are in a large-scale RFID system.

4 Multi-attribute Counterfeiting Tag Identification Protocol

4.1 Multi-dimension Dynamic Bloom Filter

In a standard bloom filter, each element in a given set $S = \{x_1, x_2, \ldots, x_N\}$ is mapped to filter using k hashing functions $h_1, h_2, \ldots, h_k$. When checking whether an element x belongs to S, it needs to find whether the bits $h_1(x), h_2(x), \ldots, h_k(x)$ of bloom filter are set to 1. For multi-dimension dynamic bloom filter [20], set S becomes a dynamic set with a dynamic $s \times N$ bit matrix where s represents s attributes of element. As N is a dynamic number and length of standard bloom filter f is a static one, multi-dimension dynamic bloom filter (MDBF) will add numbers of standard bloom filter with the variation of N. Suppose that N is mapped to L standard bloom filters. To check whether an element x belongs to S in multi-dimension dynamic bloom filter, it need to map $s \times L \times k$ bits are set to 1 in corresponding bloom filter.

4.2 Protocol Design

In our protocol, each tag has two attributes {ID, angle}: identity information ID and location information angle value. The angle value is written by the reader after the first interrogation. Also, tag will not change place before the next interrogation, which means that angle value written in tag is identical with tag's real-time location information. All tag's information is stored in back-end sever which can be access by reader. For tag T_i's attribute identity information ID_i, there are k uniform hashing functions to map it to k locations $\{ld_{i1}, ld_{i2}, \ldots, ld_{iu}, \ldots, ld_{ik}\}$ in bloom filter for ID, where $ld_{iu} = H_u(ID_i, r, f)\ mod\ f$, $u \in [1, k]$, and r is a random seed. Similarity, tag T_i's attribute

location information $angle_i$ can be mapped to k locations $\{la_{i1}, la_{i2}, ..., la_{iu}, ..., la_{ik}\}$ in bloom filter for angle, where $la_{iu} = H_u(ID_i, r, f) \bmod f$, $u \in [1, k]$, and r is a random seed. Since there are L standard filters in multi-dimension dynamic bloom filter, tags need to choose one to join in. So different from the previous multi-dimension dynamic bloom filter [20], our protocol introduces participation probability p ($p \leq 1$) for tags to determine which bloom filter to take part.

Our protocol consists of two parts: counterfeiting tag detection and counterfeiting tag verification. In detection part, multi-dimension dynamic bloom filter is used to find counterfeiting tag whose ID or angle value is not identical with the one stored in back-end server. This includes two conditions. The first one is neither tag's identity or angle value is stored in back-end server, while the second one is a tag which holds the same ID with a genuine one is attached to a counterfeiting item. According to these conditions, counterfeiting tag verification will announce their identity and verify their angle value.

Algorithm 1 protocol for reader

```
collect tag angle information and write angle information on tags
get two attributes ID and angle for MATI
for i = 0 to 1 do
MATI ← CreateDBF(i)
end for
CreateDBF()
if N≤f_t then
   return standard bloom filter
else
   m = ceil(N/f)
      for j = 1 to m do
            DBF← standard bloom filter
      end for
end else
```

Counterfeiting Tag Detection. Reader collects tag's identity information ID and location information in the first interrogation. Then it writes corresponding angle value on tag. According to tag's attributes array $A[] = [ID, angle]$, the attribute number s of multi-attribute counterfeiting tag identification (short for MATI) is set to 2. For each attribute, Algorithm 1 generates dynamic bloom filter for N tags. The length of a standard bloom filter is f, and f_t is threshold of tags that standard bloom filter can contain subjected to constraints (f, k). So, if $N \leq f_t$, it just needs one standard bloom filter, otherwise Algorithm 1 should create m standard bloom filters where $m = \lfloor N/f_t \rfloor + 1$. Then reader calculates participation probability p for each tag and broadcasts frame size f, random seed r, participation probability p. When tag receives above information, it first chooses to response in one of m frames based on probability p. Then it initializes its own attribute array $A[] = [ID, angle]$ and computes $S[i][j] = H_j(f, r_i, A[i]) \bmod f$, where $0 \leq i \leq 1, 1 \leq j \leq k$. In Algorithm 2, $S[0][j]$ represents k slots in bloom filter for identity ID, while $S[1][j]$ is mapped to k slots in bloom filter for angle value.

After Algorithms 1 and 2, reader receives responses from all tags in its interrogation range. Obviously, if either k slots for identity or k slots for angle value is not in database of back-end server, it must be a counterfeit. Reader notes the counterfeiting tags in this condition. There exists a condition that two tags hold the same k slots in bloom filter for identity, it means that a counterfeiting tag may be there. Since bloom filter has false positive probability, it cannot conclude that two tags with same k slots for identity hold the same identity. It needs to be confirmed in counterfeiting tag verification.

Algorithm 2 protocol for tag

```
receive frame start command
receive frame size f, random seed r, participation probability p.
choose to participate in one of m frames or sleep based on the probability p
if not participate, sleep until another frame starts.
initialize attribute array A[]=[ID, angle]
for i = 0 to 1 do
    for j = 1 to k do
        S[i][j]= Hj(f, ri, A[i]) mod f
    end for
end for
response slot numbers S[i][j] (0≤i≤1,1≤j≤k)
```

Counterfeiting Tag Verification. This phase mainly verifies tags in the second condition of counterfeiting tag detection. Reader first seeks database in back-end server to find identity matched to the k slots. If there are two identities mapped, reader looks up tags' k slots for angle value. On condition that two tags matches two genuine tags in database of back-end server, there exists no counterfeits. Otherwise, tag which is not matched should be a counterfeit.

If there is only one identity matched, reader will broadcast the identity and wait for tags' response. According to the response, reader measures two tags' angle value. Tag with whose measured angle value is not identical with the one in database of back-end server should be a counterfeit. To now, all counterfeiting tags have been confirmed.

5 Performance Analysis

5.1 Identification Efficiency

Our protocol is based on multi-dimension dynamic bloom filter, which can yield a false positive p_{MATI}. So identification efficiency in this protocol equals to 1-p_{MATI}, which means our protocol can achieve a higher identification efficiency when the false positive probability is low. False positive is due to a case that all k bits in both bloom filter for identity and bloom filter for angle value are set to 1 by other element previously. False positive probability in our protocol will be analyzed as follows.

Different from previous multi-dimension dynamic bloom filter, our protocol introduces participation probability p in Algorithm 2. Each tag need to choose a frame from m standard bloom filters based on the probability p. Probability p_z represents that one slot in a bloom filter is still zero after N tags' responses.

$$p_z = \left(1 - p\frac{1}{f}\right)^{kN} \approx e^{-\frac{pkN}{f}} \tag{1}$$

Then a standard bloom filter's false positive probability p_s is:

$$p_s = (1 - p_z)^k \approx \left(1 - e^{-\frac{pkN}{f}}\right)^k \tag{2}$$

For our protocol, $m = \lfloor N/f_t \rfloor + 1$ is a dynamic number. In a single standard bloom filter, there are only f_t tags. So standard bloom filter's false positive probability p_s in dynamic bloom filter should be $\left(1 - e^{-\frac{pkf_t}{f}}\right)^k$. As probability that there is no false positive in all m bloom filters is $(1 - p_s)^m$, false positive probability p_{DBF} of dynamic bloom filter can be denoted as:

$$p_{DBF} = 1 - (1 - p_s)^m \approx 1 - \left(1 - \left(1 - e^{-\frac{pkf_t}{f}}\right)^k\right)^m \tag{3}$$

Since tag's information includes identity ID and angle value, attribute number of MATI s is set to 2. Probability p_{DBF-ID} and $p_{DBF-angle}$ represents false positive in dynamic bloom filter for identity and angle value respectively. If a false positive event happens in our protocol, it should satisfy that all k slots in both dynamic bloom filter for identity and dynamic bloom filter for angle value are set to 1. So false positive probability p_{MATI} is denoted as:

$$p_{MATI} = p_{DBF\_ID} p_{DBF\_angle} \approx \left(1 - \left(1 - \left(1 - e^{-\frac{pkf_t}{f}}\right)^k\right)^m\right)^2 \tag{4}$$

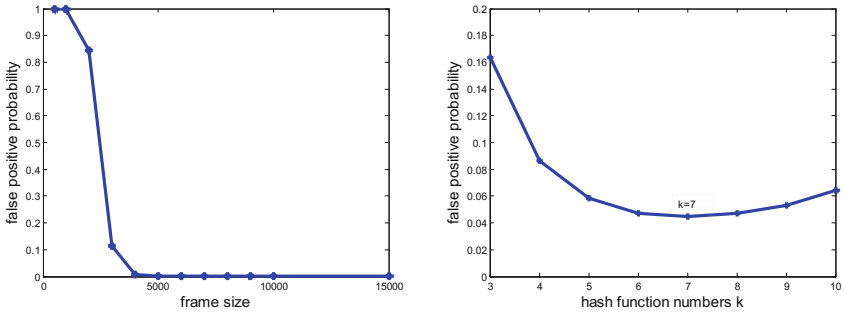
As our protocol is based on framed slotted ALOHA algorithm, longer frame size can decrease collisions. Figure 2(a) shows that our protocol acquires better identification efficiency with increase of frame size in large-scale RFID system. In order to minimize false positive probability, ratio of f and N should be optimized. According to previous work [21], it can be concluded that false positive probability p_s is minimized when ratio of f and N satisfies Eq. (5). From Fig. 2(b), the result is clearly depicted.

$$k = \frac{f_t}{pN} ln2 \tag{5}$$

As p_{DBF_ID} and p_{DBF_angle} are false positive probability in dynamic bloom filter for identity and angle value respectively, it's obviously that they are all below 1. So it can be concluded that either p_{DBF_ID} or p_{DBF_angle} is greater than p_{MATI}, which indicates

that multi-attribute counterfeiting tag identification can achieve better identification efficiency than dynamic bloom filter.

$$p_{MATI} < p_{DBF\_ID} \text{ or } p_{DBF\_angle} \tag{6}$$



(a) (b)

Fig. 2. (a) When $N = 15000$, $k = 7$, $f_t = 300$, $p = 1$, the false probability of MATI; (b) When $N = 15000$, $f = 5000$, $f_t = 495$, $p = 1$, the false probability of MATI.

Compared with standard bloom filter, multi-attribute counterfeiting tag identification has efficiency superiority. Standard bloom filter has space constraints with the growth of tag number, while multi-attribute counterfeiting tag identification defines a threshold for a single standard bloom filter which can reduce collisions and enhance space utilization. Figure 3 with settings that hash function number k is 7, participation probability p is 1 and frame size f is 5000, shows that multi-attribute counterfeiting tag identification has apparent identification efficiency advantage over standard and

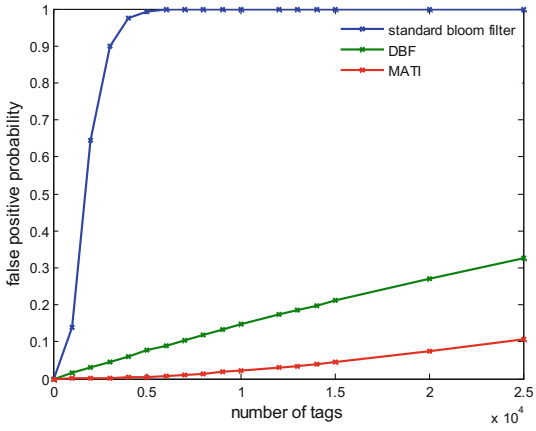


Fig. 3. When $f = 5000$, $f_t = 495$, $k = 7$, $p = 1$, the false probability of standard bloom filter, dynamic bloom filter and MATI respectively.

dynamic bloom filter with the increment of tag numbers. Then false positive probability of SEBA+ [18], WP [3] and our protocol is examined in Fig. 4. We fix number of tags $N = 1000$, participation probability $p = 1$, hash function number $k = 7$. As shown in Fig. 4, when frame size is greater than 2000, our protocol's false positive probability is approached to zero, which means identification efficiency is almost up to 1. In contrast, false positive probability of SEBA and WP is still greater than 0.4, which has huge difference with our protocol. In conclusion, compared with other methods, our protocol achieves better identification efficiency in large-scale RFID system.

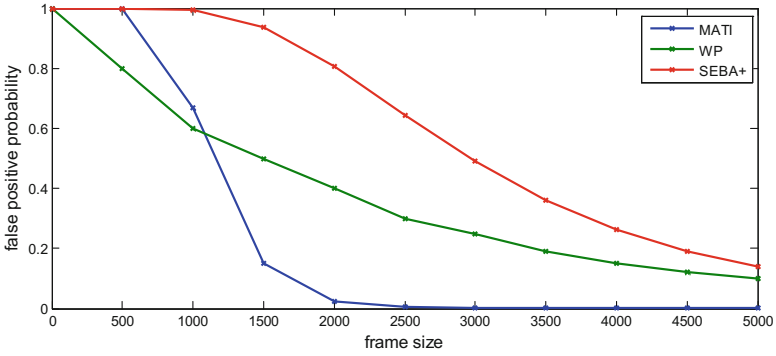


Fig. 4. When $N = 1000$, $f_t = 300$, $k = 7$, $p = 1$, the false probability of WP, SEBA+ and MATI respectively.

5.2 Time Cost

According to Philips I-Code [22], time slots are classified into tag slots, long slots and short slots. Based on length of slot, tag slot which is denoted as t_{id} can transmit a 96-bit message with time consuming of 2.4 ms; while long slot is set to 0.8 ms and affords a 10-bit response. By contrast, short slot, denoted as t_s, is set to 0.4 ms and allows only 1-bit response. As our protocol is consisted of two dynamic bloom filters, time cost is two times larger than single one. Time cost of our protocol can divided into two parts: time cost of reader broadcast and tag response. For tag, it has participation probability $p_i (1 \leq i \leq m)$ to choose one frame to reply. Total probability p of p_i should be $p = p_1 + p_2 + \ldots + p_m = 1$. Then Eq. (7) can be simplified as follow.

$$\begin{aligned} T &= 2\left[m \times \left\lceil \frac{f}{96} \right\rceil \times t_{id} + (p_1 f + p_2 f + \ldots + p_m f) \times N \times t_s\right] \\ &= 2\left[m \times \left\lceil \frac{f}{96} \right\rceil \times 2.4\,\text{ms} + f \times N \times 0.4\,\text{ms}\right] \end{aligned} \tag{7}$$

From Eq. (7), we can compute that time cost is only 10 s when number of tags is up to 10000. Also, when N is up to 50000, the time cost is 40 s. Although our protocol's time cost is not very low, its false positive probability is far less than WP from Fig. 4.

Specially, with the increment of tags, our protocol has apparent advantage in identification efficiency. It's worth to consume more time to achieve better identification efficiency.

6 Conclusion

In this paper, a multi-attribute counterfeiting tag identification protocol based on framed slotted ALOHA algorithm in large-scale RFID system is proposed. Different from previous works, there are two attributes: identity ID and angle value in our protocol. Also, it's the first scheme using multi-dimension dynamic bloom filter to give a solution for RFID security problem that counterfeiting tag forges the same ID with a genuine one. Compared with previous works, our protocol not only points out unknown tags, but also counterfeiting goods with genuine tag ID. What's more, it can achieve a high identification efficiency with reasonable time cost. Future work is to apply our protocol on hardware and examine stability and functionality of our protocol in practice.

Acknowledgement. This work was supported by research of life cycle management and control system for equipment household registration, No. J770011104 and natural science foundation of China (61701494). We also thank the anonymous reviewers and shepherd for their valuable feedback.

References

1. Gong, W., Stojmenovic, I., Nayak, A., et al.: Fast and scalable counterfeits estimation for large-scale RFID systems. IEEE Trans. Netw. (TON) **24**(2), 1052–1064 (2016)
2. The spread of counterfeiting: Knock-offs catch on. The Economist, March 2010
3. Gong, W., Liu, J., Yang, Z.: Fast and reliable unknown tag detection in large-scale RFID systems. In: Proceedings of the 17th ACM International Symposium on Mobile Ad Hoc Networking and Computing, pp. 141–150. ACM (2016)
4. Liu, X., Qi, H., Li, K., et al.: Sampling bloom filter-based detection of unknown RFID tags. IEEE Trans. Commun. **63**(4), 1432–1442 (2015)
5. Weis, S.A., Sarma, S.E., Rivest, R.L., Engels, D.W.: Security and privacy aspects of low-cost radio frequency identification systems. In: Hutter, D., Müller, G., Stephan, W., Ullmann, M. (eds.) Security in Pervasive Computing. LNCS, vol. 2802, pp. 201–212. Springer, Heidelberg (2004). https://doi.org/10.1007/978-3-540-39881-3_18
6. Lu, L., Han, J., Xiao, R., Liu, Y.: ACTION: breaking the privacy barrier for RFID systems. In: INFOCOM 2009, pp. 1953–1961. IEEE (2009)
7. Lu, L., Liu, Y., Li, X.Y.: Refresh: weak privacy model for RFID systems. In: Proceedings of INFOCOM 2010, pp. 1–9. IEEE (2010)
8. Chen, M., Chen, S.: ETAP: enable lightweight anonymous RFID authentication with O(1) overhead. In: 2015 IEEE 23rd International Conference on Network Protocols (ICNP), pp. 267–278. IEEE (2015)
9. Shahzad, M., Liu, A.X.: Fast and accurate estimation of RFID tags. IEEE/ACM Trans. Networking **23**(1), 241–254 (2015)

10. Liu, J., Xiao, B., Chen, S., Zhu, F.: Fast RFID grouping protocols. In: 2015 IEEE Conference on Computer Communications (INFOCOM), pp. 1948–1956. IEEE (2015)
11. Zheng, Y., Li, M.: ZOE: fast cardinality estimation for large-scale RFID systems. In: 2013 Proceedings IEEE, INFOCOM, pp. 908–916. IEEE (2013)
12. Gong, W., Liu, K., Miao, X., Liu, H.: Arbitrarily accurate approximation scheme for large-scale RFID cardinality estimation. In: 2014 Proceedings IEEE, INFOCOM, pp. 477–485. IEEE (2014)
13. Yu, J., Chen, L., Zhang, R., et al.: On missing tag detection in multiple-group multiple-region RFID systems. IEEE Trans. Mob. Comput. **16**(5), 1371–1381 (2017)
14. Liu, X., Li, K., Min, G., Shen, Y., Liu, A.X., Qu, W.: Completely pinpointing the missing RFID tags in a time-efficient way. IEEE Trans. Comput. **64**(1), 87–96 (2015)
15. Liu, X., Li, K., Min, G., Shen, Y., Liu, A.X., Qu, W.: A multiple hashing approach to complete identification of missing RFID tags. IEEE Trans. Commun. **62**(3), 1046–1057 (2014)
16. Shahzad, M., Liu, A.X.: Expecting the unexpected: fast and reliable detection of missing RFID tags in the wild. In: 2015 IEEE Conference on Computer Communications (INFOCOM), pp. 1939–1947. IEEE (2015)
17. Yang, L., Han, J., Qi, Y., Liu, Y.: Identification-free batch authentication for RFID tags. In: 2010 18th IEEE International Conference on Network Protocols (ICNP), pp. 154–163. IEEE (2010)
18. Bianchi, G.: Revisiting an RFID identification-free batch authentication approach. IEEE Commun. Lett. **15**(6), 632–634 (2011)
19. Liu, X., Xiao, B., Zhang, S., Bu, K.: Unknown tag identification in large RFID systems: An efficient and complete solution. IEEE Trans. Parallel Distrib. Syst. **26**(6), 1775–1788 (2015)
20. Guo, D., Wu, J., Chen, H., et al.: Theory and network applications of dynamic bloom filters. In: Proceedings of 25th IEEE International Conference on Computer Communications, pp. 1–12. IEEE (2006)
21. Bloom, B.: Space/time trade-offs in hash coding with allowable errors. Commun. ACM **13**(7), 422–426 (1970)
22. Philips Semiconductors. Your Supplier Guide to ICODE Smart Label Solutions (2008)