Anti-Clone: A Lightweight Approach for RFID Cloning Attacks Detection

Yue Feng[1,2], Weiqing Huang[1,2,3], Siye Wang[1,2,3(✉)], Yanfang Zhang[1,2], Shang Jiang[1,2], and Ziwen Cao[1,2]

[1] Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China
{fengyue,huangweiqing,zhangyanfang,jiangshang,caoziwen,wangsiye}@iie.ac.cn

[2] School of Cyber Security, University of Chinese Academy of Sciences, Beijing, China

[3] School of Computer and Information Technology, Beijing Jiaotong University, Beijing, China

Abstract. Millions of radio frequency identification (RFID) tags are pervasively used all around the globe to identify a wide variety of objects inexpensively. However, the tag cannot use energy-hungry cryptography due to the limit of size and production costs, and it is vulnerable to cloning attacks. A cloning attack fabricates one or more replicas of a genuine tag, which behave the same as the genuine tag and can deceive the reader to obtain legitimate authorization, leading to potential economic loss or reputation damage. Among the existing solutions, the methods based on radio frequency (RF) fingerprints are attractive because they can detect cloning attacks and identify the clone tags. They leverage the unique imperfections in the tag's wireless circuitry to achieve largescale RFID clone detection. However, training a high-precision detection model requires a large amount of data and high-performance hardware devices. And some methods require professional instruments such as oscilloscopes to collect fine-grained RF signals. For these reasons, we propose a lightweight clone detection method Anti-Clone. We combine convolutional neural networks (CNN) with transfer learning to combat data-constrained learning tasks. Extensive experiments on commercial off-the-shelf (COTS) RFID devices demonstrate that Anti-Clone is more lightweight than the existing methods without sacrificing detection accuracy. The detection accuracy reaches 98.4%, and the detection time is less than 5 s.

Keywords: Radio frequency identification (RFID) · Cloning detection · Fingerprint · Transfer learning

1 Introduction

Radio frequency identification (RFID) technology is a non-contact automatic identification technology through spatial coupling or backscattering of radio frequency signals. The advantages of low cost, lightness, and long-distance identification of multiple targets make RFID technology widely used in every corner

H. Gao et al. (Eds.): CollaborateCom 2022, LNICST 461, pp. 75–90, 2022.
https://doi.org/10.1007/978-3-031-24386-8_5

of our life. Such as payment systems, object monitoring, and continuous health monitoring through implantation [14,16–20,26,27,29,30]. However, since RFID can be attached to cash and other valuable objects and implanted into animals and people, their widespread usage has raised severe security and privacy concerns. More importantly, the low cost and small size of tags make some excellent cryptographic algorithms and security mechanisms unable to be applied to existing RFID systems. For these reasons, RFID tags are vulnerable to attack.

This paper considers the tag cloning attack, where the attacker extracts data from the corrupted tag to other tag chips or rogue devices called clone tags. The clone tag saves all the valid data the same as the genuine tag and has the same permissions as the genuine tag. Intuitively, the resilience of RFID tags to cloning attacks is strongly correlated to their applicability in critical applications. For example, by injecting clone tags into the logistics or drug supply chain, the company will lose the tracking of assets [31]. By injecting clone tags into e-passports to ensure national borders' security, terrorists or illegal immigrants will enter a country undetected. By injecting clone tags into the access control system, unauthorized personnel will enter the control area at will. More importantly, clone tags may cause severe damage to human health and safety because RFID technology is used in the medical field.

Approach. To solve the cloning problem of low-cost tags without relying on cryptography, some prior work has proposed approaches based on radio frequency (RF) fingerprints [2,7,11,24,25,32]. RF fingerprints leverage the common individual differences in the RFID tag circuit. By extracting the features of the received signal and associating them with a given tag, the unique identification of the tag can be obtained. These features are generated in the production process and cannot be controlled by human beings. We call them RF fingerprints. Existing methods rely on protocol-specific feature-extraction techniques, such as minimum power response [25], spectral characteristics [32], and dynamic wavelet fingerprints [1], which can only be applied to a specific tag type. And these methods need professional equipment such as oscilloscopes and universal software radio peripheral (USRP) to collect fine-grained fingerprints, which is beyond the capacity of existing commercial off-the-shelf (COTS) readers. In contrast, in this paper, we use machine learning (ML), especially convolutional neural networks (CNNs), to create RF fingerprint classifiers to detect clone tags. Compared with traditional ML, the main advantage of CNN is that it uses many parameters and can distinguish high device populations.

Existing Issues. A fundamental challenge in training any CNN model comes from the need for large data sets. This challenge is severe in our environment due to the limited public RF fingerprint data sets. A naive solution is to continuously collect the data of each tag for a long time. However, it is difficult to obtain large-scale and high-quality data in actual scenarios due to cost, privacy, environmental constraints, and other issues. Therefore, to reduce the cost of model training and adapt the neural network to the learning task with limited data, this paper introduces transfer learning into CNN and proposes a lightweight method Anti-Clone for detecting clone tags.

Technical Contributions. We summarize the novel contributions of Anti-Clone to the current status of cloning detection:

1. We entirely use the limited processing capacity of passive RFID tags and introduce Anti-Clone, which can detect cloned tags in real-time. Anti-Clone only requires COTS devices and no additional hardware devices.
2. We use the non-replicable physical layer signal to establish the tag RF fingerprint, creatively convert the signal sequence into images, and build the fingerprint database of genuine tags based on CNN. Then combined with transfer learning to reduce the cost of model training and simultaneously make the network adapt to the learning task with limited data.
3. We implemented a prototype and conducted extensive experiments. Our results show that Anti-Clone has high detection accuracy. Extensive experiments show that the detection accuracy reaches up to 98.4%, and the detection time overhead is minimal. The fastest is less than 5 s.

The rest of this paper is organized as follows. Section 2 introduces the related work. Section 3 provides an overview of the cloning attack threat model, the theoretical and experimental basis for Anti-Clone's work, and the challenges and solutions of clone detection. Section 4 describes the Anti-Clone in detail. Section 5 evaluates the performance of Anti-Clone. Section 6 concludes this paper.

2 Related Work

Aiming at the risk of cloning attacks faced by RFID technology, how to quickly and effectively detect clone tags has attracted much attention. Current scholars focus on synchronization keys, collision detection, trajectory analysis, and RF fingerprints.

2.1 Synchronization Keys

Synchronization keys are double authentication for a tag by loading different random numbers into a low-cost tag. Lehtonen [15] investigated a method to pinpoint tags with the same ID. It writes a new random number on the tag's memory every time the tag is scanned. A back-end that issues these numbers detect tag cloning attacks as soon as the genuine and the cloned tag are scanned. Okpara [21] proposed a detection method based on chaos theory used to generate random numbers. These methods increase the communication delay and require tag memory space.

2.2 Collision Detection

The method based on the collision principle to detect clone tags was proposed by Bu et al. [3–5]. The conflict caused by a genuine tag and a cloned tag with the same ID is used for clone tag detection, which is driven by the Aloha communication protocol. However, these methods were later overturned by Burmester et al. [6]. They proved that these methods are impossible in practice by analyzing the protocol.

2.3 Trajectory Analysis

The trajectory-based detection method indicates whether the trajectory to be measured matches the normal trajectory. Normal trajectories can be predefined trajectories or statistical features based on historical trajectories.

Ouafi and Vaudenay [22] proposed Pathchecker. When the final trajectory is not equal to the defined target trajectory, it is regarded as abnormal. This method has high detection accuracy. However, storing the correct trajectory requires a large amount of memory, which is a high requirement for tags.

Feng et al. [10,12] proposed the deClone, which obtained the features of normal trajectories through statistics on many historical trajectories and then found anomalies through matching. Wang et al. [28] also contributed to this field. These methods are highly portable. However, they could only detect the presence of a cloning attack in the system, not identify which one is the cloning tag.

2.4 RF Fingerprints

The method based on RF fingerprint can distinguish individual tags. In detail, it can identify which is the genuine tag and which is the clone tag. The seminal work applies RFP to 50 HF tags, achieving a 2.43% error rate [8]. Among others, the features used are based on the Hilbert transform. Zanetti et al. [32] use the time and spectrum level domain to fingerprint 70 UHF tags, achieving 71% accuracy. To improve detection accuracy, Piva et al. [23] combine CNN and federated learning. However, these methods ignore the difficulty of collecting data. Therefore, for learning tasks with limited data, we combine CNN with transfer learning. Without loss of detection accuracy, our method is more lightweight than other methods.

3 Overview of Anti-Clone

3.1 Threat Model

In RFID systems, a cloning attack is to create one or more copies of genuine tags, which are called clone tags and have the same valid data as genuine tags. The clone tag saves all the valid data the same as the genuine tag and has the same permissions as the genuine tag. Since most RFID applications use the authenticity of tags to verify the authenticity of tagged objects, clone tags may harm the entity. Therefore, this paper aims to identify clone tags with the COTS devices.

3.2 Basic Idea

The application layer data (such as EPC and ID) stored in the tag memory can be cloned by the attacker. The physical layer RF signal is difficult to clone because the RF signal is affected by many factors, including device diversity, multipath effect, tag position, and direction. Different environments and hardware devices

significantly impact the RF signal, which makes the RF signal unpredictable and is widely used in wireless sensing. The received signal strength (RSS) and phase are two basic physical-layer metrics of RF signals. The received signal strength indication (RSSI) reflects the value of RSS. An RFID reader can directly read RSSI and phase.

In this section, we first model the RF signal and theoretically deduce the influence of different tags on the signal. Then, we prove our derivation through experiments.

RSS/Phase Model. RSS model. Received signal strength (RSS) measures the power present in a received RF signal. Phase reflects the offset degree between the received signal and the sent signal. According to the Friis equation [9], we can quantify the effect of different tags on RSS.

$$RSS = 10\lg\left(\frac{P_{T,\text{ reader}}}{1\,mW}{G_{\text{reader}}}^2{G_{tag}}^2\left(\frac{\lambda}{4\pi d}\right)^4 T_b\right) \tag{1}$$

where $P_{T,reader}$ is the transmission power of the reader antenna, G_{reader} is the gain of the reader antenna, G_{tag} is the gain of the tag antenna, d is the distance from the reader antenna to the tag, λ is the working wavelength of the RFID system, and T_b is a constant representing the backscattering loss.

In the same environment, when the readers are the same and the distance between the readers and tags is the same, RSS depends on the gain of the tag antenna. And the gain varies with different devices.

Phase model. The phase reading ϕ reported by the RFID reader contains three parts.

$$\phi = \phi_{\text{tag}} + \phi_{\text{pro}} + \phi_{\text{cir}} \tag{2}$$

where ϕ_{tag} is the phase shift caused by the tag and is related to the tag antenna impedance Za. ϕ_{pro} is caused by the distance d that the signal travels in the air. ϕ_{cir} is the phase shift introduced by the RFID reader circuit. All three parts are unknown.

When the readers and their distance from the tag are the same, ϕ_{pro} and ϕ_{cir} are fixed. ϕ_{tag} is the phase shift caused by the tag and is related to the tag antenna impedance Za and tag diversity. And many studies have shown that the object material will have an impact on the impedance.

RSS/Phase Changes for Different Tags. We show the impact of different tags on RF signals through a toy experiment. In the same environment, we placed five different tags with the same type at the same location and observed the RSSI and phase. The results are shown in Fig. 1. The abscissa is the phase, and the ordinate is the RSSI. Different colors represent different tags. Although the experimental environment and deployment conditions remain unchanged, the RF signal measurement results of different tags differ. Hardware differences cause this. These results confirm the significant influence of tag diversity on RF signals. We can distinguish tags by RF signal.

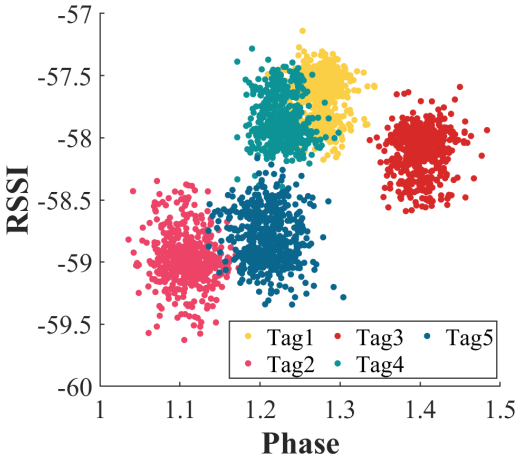

Fig. 1. Tag diversity.

3.3 Observation and Challenges

When the tag reports its ID to the reader, the reader measures RSSI and phase. Therefore, for tags with different IDs, we can easily classify the physical layer signal according to the IDs. However, when a cloning attack occurs, the clone tag has the same valid data as the genuine tag, including ID. The measured RSSI and phases mix even though they come from different tags (a genuine tag and its clone tags). The preliminary studies show that RF signals can distinguish different tags.

However, we still face challenges. First, the difference between tags is minimal, and RF signals are highly couple. A simple classification algorithm makes it difficult to distinguish the tags accurately. Second, collecting a large amount of data requires a lot of human and financial resources, and it needs to design an efficient classifier for the learning task with limited data. Third, tags are usually attached to the surfaces of the objects. The surface material of the object will affect the RF signal.

To overcome these challenges, we combined two physical layer indicators. We convert the sequence data into two-dimensional images classified through CNN. We combine CNN with transfer learning to adapt to the learning task with limited data and design a lightweight clone detection method, Anti-Clone. In the experimental evaluation stage, we considered the impact of different material types of attachments on the experimental results.

4 Anti-Clone Design

To achieve our goal of detecting the clone tag, we propose Anti-Clone, which operates as shown in Fig. 2.

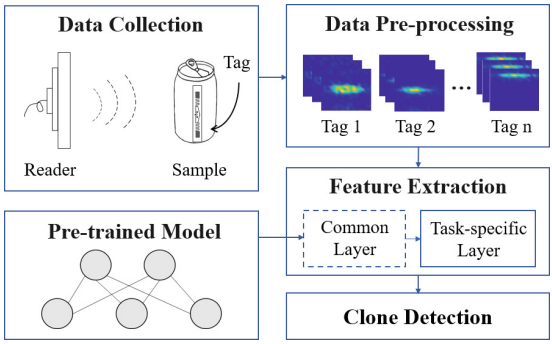

Fig. 2. Overview of Anti-Clone.

4.1 Data Pre-processing

In this section, we will pre-process the data. We transform the sequence into the form of images to better distinguish the tags.

We divide the data sequence of a tag into multiple data blocks and then form multiple images containing the same amount of data. However, due to the different sampling rates of devices and the interference of the environment, it is impossible to ensure that the amount of data collected is the same in the same collection time. In addition, for the network, the larger the amount of data, the higher the accuracy of the model. Therefore, we use the sliding window to divide the data sequence into blocks with the same amount of data as much as possible. In order to make the images contain more effective information and ensure that the same class has the same reference, we take the maximum and minimum values of all the data by a tag as the boundary of this class of heat map. Figure 3 shows the heat map generated by four different tags.

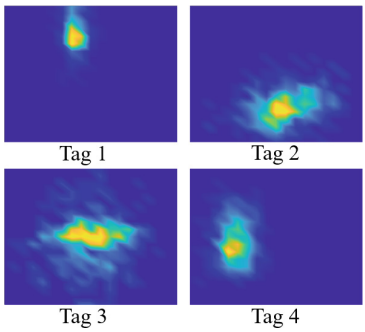

Fig. 3. Heatmap of different tags.

4.2 Feature Extraction

The feature extraction stage mainly extracts the features of each tag to realize the establishment of a fingerprint database. We do this by extracting features from images. First, we describe the neural networks. Then, we describe how to effectively transfer the network to solve the small sample problem and reduce the training time.

Neural Network Description. We extract tag features through CNN. Currently, CNN has reached industrial application in multiple classification problems. However, the general network has a complex structure and a large amount of computation, which is incompatible with a large amount of data and reasonable real-time. This paper decides to use the lightweight network SqueezeNet for image classification.

SqueezeNet was proposed by Forrest et al. in 2017 [13]. It has fewer parameters while ensuring the same recognition accuracy, which means that the architecture requires less communication with the server in distributed training. SqueezeNet is more suitable for deployment on devices with limited performance.

The fire module is the basic building module in SqueezeNet, which is composed of a squeeze module and expand module. The squeeze module comprises a set of 1×1 continuous convolution. The expand module contains a set of 1×1 continuous convolution and 3×3 convolutions in the spatial ascending superposition. The schematic diagram is shown in Fig. 4.

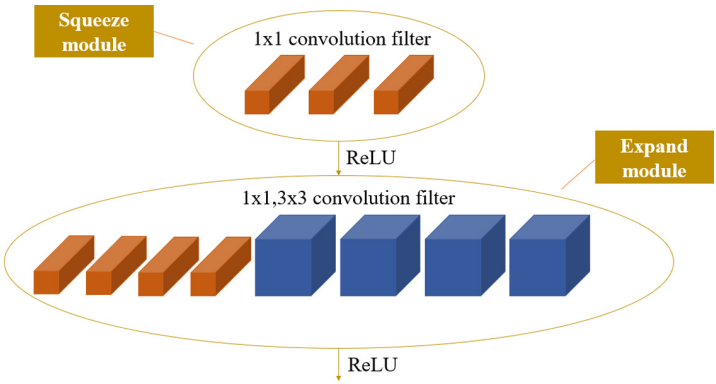

Fig. 4. Fire module schematic diagram.

SqueezeNet starts with the convolution layer (conv1), then uses 8 fire modules (fire2-9), and ends with the convolution layer (conv10). Figure 5 depicts the structure of SqueezeNet.

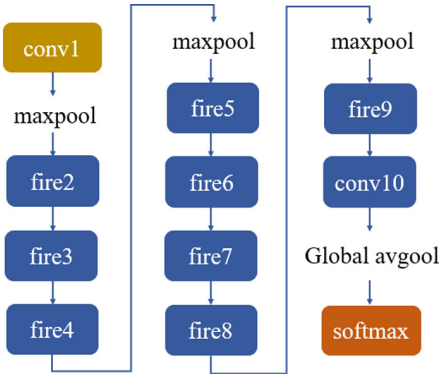

Fig. 5. SqueezeNet model flow diagram.

Extending to New Tasks. We hope to expand the network to new classification tasks efficiently to reduce the training network's consumption. For example, after training the classifier with a large data set, we want to extend it to the learning task with limited data to detect clone tags. Therefore, we adopt transfer learning to transfer training knowledge from a well-trained source domain to a new target domain.

The networks described in the previous section are composed of multiple layers. Some of them are used for feature extraction or coding. At the same time, others are used for classification. The feature extraction layer can be further divided into a common layer and a task-specific layer. The common layer can be directly transferred from the trained classifier to the target domain as a freezing layer. This dramatically reduces the number of parameters that the new task needs to learn, thus reducing the size of the data set required to achieve high accuracy. We freeze the previous layer and replace the last two-dimensional convolution layer "conv10" and classification layer "softmax". And then retrain the network.

4.3 Clone Detection

We have introduced the classification model based on transfer learning in detail. This model realizes the feature extraction of genuine tags and can establish the legal fingerprint database of genuine tags. When the tag to be tested is read, we will match the fingerprint of the tag to be tested with the fingerprint database to complete the cloning detection. In this section, we will introduce this process in detail.

During the cloning attack, the attacker clones the valid application data, including the ID used for identification. The fingerprint signal used for data transmission in the communication process depends on the device itself and cannot be predicted and cloned. Therefore, when the clone tag appears, although

the ID is the same as the ID of the genuine tag, we can still distinguish the genuine tag and the clone tag by fingerprints.

In detail, based on the fingerprint database established by the genuine tag, we carry out clone tag detection. When the reader collects the tag information to be tested, the detection model matches the fingerprint to be tested with the genuine fingerprint in the fingerprint database. When the matched category is the same as the ID by the tag to be tested, we consider the tag to be tested to be a genuine tag. On the contrary, when the matched category is different from the ID by the tag to be tested, we consider the tag is a clone tag. See Algorithm 1 for the detailed detection process.

Algorithm 1. Cloning tag detection algorithm

Input:
The ID of the tag, which means the category: ID
RSSI of the tag to be detected: R
Phase of the tag to be detected: P
Output:
The status of the tag to be detected: clone or genuine
image: An image transformed from a sequence of the tag to be detected
pred: The prediction category of the model on the image
$image =$ toImage(R, P)
$pred =$ classify$(image)$
if $pred \neq ID$ **then**
  The tag is cloned.
else
  The tag is genuine.
end if

5 Implementation and Evaluation

In this section, we present the implementation and evaluation of our system.

5.1 Experimental Setup

We implemented Anti-Clone in the indoor environment of a typical office building. We use COTS RFID devices to build a system prototype. As shown in Fig. 6. An Impinj Speedway R420 reader connects to a larid S9028 antenna to collect the physical layer signal of each tag. The reader continuously broadcasts signals. When the tag responds to ID, the reader simultaneously records the RSSI and phase information of the tag.

We collected data with three types of tags to evaluate the impact of tag types on Anti-Clone performance. Tags were pasted on objects with four types of materials. We collected them to evaluate the effects of different material types on detection performance. We used 500 tags for the experiment and carried out a cloning attack on each tag in turn.

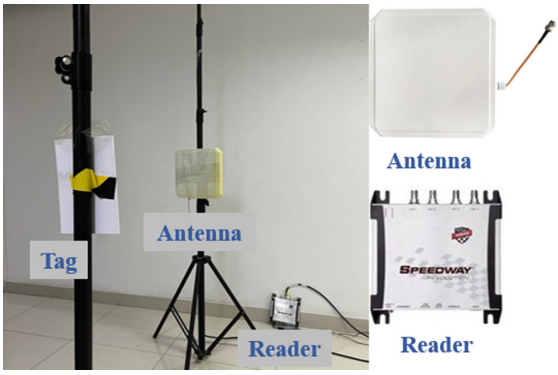

Fig. 6. System deployment.

5.2 Efficiency of Anti-Clone

Overall Performance. We study the effectiveness of Anti-Clone against cloning attacks, which helps remind users and avoid potential economic losses. We use the accuracy rate, false positive rate (FPR), and false negative rate (FNR) to display the results. FPR means a false alarm rate. FNR means miss alarm rate. The detection results show that the detection accuracy of Anti-Clone for cloning attack is 98.4%.

We evaluated the classification model separately. This model realizes the feature extraction of tag individuals and is the primary determinant of the detection effect of Anti-Clone. We use the traditional machine learning classifier quadratic discriminant analysis (QDA), K-nearest neighbor (KNN) clustering algorithm, and SqueezeNet for comparison. The results are shown in the following table. The results show that the classification model is superior to other methods in terms of classification effect (Table 1).

Table 1. Comparison of the results of different classifiers

Approach	QDA	KNN	SqueezeNet
Accuracy	58.23%	69.63%	**99.4%**

Performance with Different Types of Tags. In the RFID application system, different tags are designed according to the protected objects' types, shapes and materials, and planned costs. We evaluated the impact of different tag types on the effectiveness of Anti-Clone and selected three commonly used typical tags in the experiment, including NXP U8, Impinj R6, and imping M4E. We compared the performance in Fig. 7. The results show that different types of tags

have different degrees of influence on the experimental results, but the effect is negligible. Therefore, Anti-Clone has robustness in clone tag detection and can adapt to different types of tags.

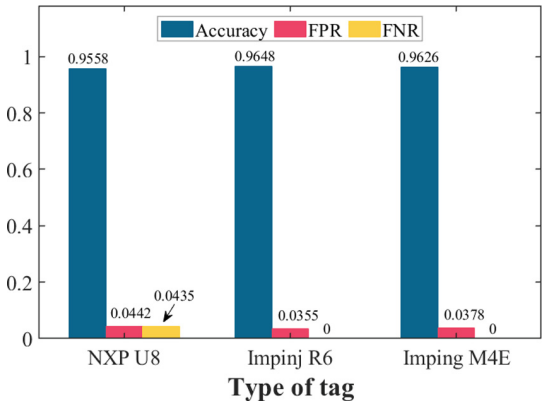

Fig. 7. Accuracy v.s. type of tags.

Performance with Different Material Types of Objects. In the RFID application system, the effect of the surface material of the protected object on the tag signal has been proved by experiments. In this section, we evaluate the effects of objects with different materials on the clone detection effect. We selected four typical materials commonly used in the system, including paper, plastic and rubber. Figure 8 shows the experimental results. The abscissa indicates different types of attached objects, and the ordinate indicates the accuracy rate, FPR, and FNR. We can see that the detection accuracy is over 96% for different types of attached objects. Therefore, the different materials of the tag protection object have no impact on the Anti-Clone, which has good robustness in the clone tag detection.

5.3 Time Overhead

Model Training Time. At the stage of establishing a fingerprint database, we combine CNN with transfer learning to combat small sample learning, make the network lightweight, and reduce the dependence on hardware resources. In this section, the lightweight is demonstrated by using the training time of the network before and after the transfer learning. We used the same data to train the network. The results show that 23 min can be saved by using transfer learning with a 1.8% loss of detection accuracy.

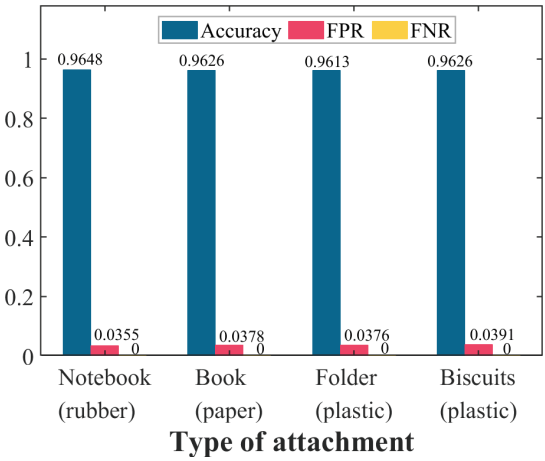

Fig. 8. Accuracy v.s. type of attachment.

Clone Detection Time. Cloning attacks detection system usually needs high real-time performance and requires administrators to respond quickly to clone tags. Therefore, the shorter the detection time and the loss can be reduced as much as possible.

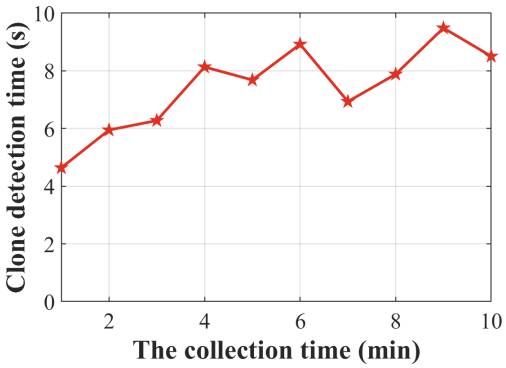

Fig. 9. Clone detection time overhead.

In this paper, the construction of the fingerprint database is offline, and the modeling time will not affect the detection time. Therefore, in this section, we only consider the time cost in the online detection stage. We built a system prototype on a laptop with common performance. The following figure shows the impact of different data volumes on the detection time. The abscissa represents the data collection time. The ordinate represents the clone detection time. When

the data to be measured is collected for one minute, the time required for detection is less than 5 s. This means we can know whether a tag is a cloned tag within 5 s after it is read, which can timely prevent the harm caused by cloning attacks. In Fig. 9, the clone detection time is proportional to the data collection time, but it is not fully proportional. This is because due to the environment's influence, the reader's reading rate to the tag is different, which makes the amount of data collected simultaneously have apparent differences.

Through experiments, we verify that the Anti-Clone has a slight detection delay and real-time performance.

6 Conclusion

This paper proposes a lightweight clone tag detection method, Anti-Clone. Its basic idea is to use the unpredictable and unclonable physical layer signal to describe each tag with COTS RFID devices. We combined CNN with transfer learning to overcome the challenges of limited data and high signal coupling. A large number of experimental results show that the detection accuracy of Anti-Clone can reach 98.4% without any software or hardware modifications needed.

Our future work will be conducted on the extension of Anti-Clone to arbitrary environments. We try to design a detection method with environment robustness.

Acknowledgment. This work was supported by the Strategic Priority Research Program of Chinese Academy of Sciences, Grant No. XDC02040300

References

1. Bertoncini, C., Rudd, K., Nousain, B., Hinders, M.: Wavelet fingerprinting of radio-frequency identification (rfid) tags. IEEE Trans. Industr. Electron. **59**(12), 4843–4850 (2012)
2. Bu, K., Weng, M., Zheng, Y., Xiao, B., Liu, X.: You can clone but you cannot hide: a survey of clone prevention and detection for RFID. IEEE Commun. Surv. Tutor. **19**(3), 1682–1700 (2017)
3. Bu, K., Liu, X., Luo, J., Xiao, B., Wei, G.: Unreconciled collisions uncover cloning attacks in anonymous RFID systems. IEEE Trans. Inf. Forensics Secur. **8**(3), 429–439 (2013)
4. Bu, K., Liu, X., Xiao, B.: Approaching the time lower bound on cloned-tag identification for large RFID systems. Ad Hoc Netw. **13**, 271–281 (2014)
5. Bu, K., Xu, M., Liu, X., Luo, J., Zhang, S., Weng, M.: Deterministic detection of cloning attacks for anonymous RFID systems. IEEE Trans. Industr. Inf. **11**(6), 1255–1266 (2015)
6. Burmester, M., Munilla, J., Ortiz, A.: Comments on "unreconciled collisions uncover cloning attacks in anonymous RFID systems". IEEE Trans. Inf. Forensics Secur. **13**(11), 2929–2931 (2018)
7. Chen, X., Liu, J., Wang, X., Zhang, X., Wang, Y., Chen, L.: Combating tag cloning with cots rfid devices. In: 2018 15th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON), pp. 1–9. IEEE (2018)

8. Danev, B., Heydt-Benjamin, T.S., Capkun, S.: Physical-layer identification of RFID devices. In: USENIX Security Symposium, pp. 199–214 (2009)
9. Dobkin, D.: The RF in RFID: uhf RFID in practice. Newnes (2012)
10. Feng, Y., Huang, W., Wang, S., Zhang, Y., Jiang, S.: Detection of RFID cloning attacks: a spatiotemporal trajectory data stream-based practical approach. Comput. Netw. **189**, 107922 (2021)
11. Han, J., et al.: Geneprint: generic and accurate physical-layer identification for UHF RFID tags. IEEE/ACM Trans. Networking **24**(2), 846–858 (2016)
12. Huang, W., Zhang, Y., Feng, Y.: Acd: an adaptable approach for RFID cloning attack detection. Sensors **20**(8), 2378 (2020)
13. Iandola, F.N., Han, S., Moskewicz, M.W., Ashraf, K., Dally, W.J., Keutzer, K.: Squeezenet: Alexnet-level accuracy with 50x fewer parameters and $<$ 0.5 mb model size. arXiv preprint arXiv:1602.07360 (2016)
14. Ilie-Zudor, E., Kemény, Z., Blommestein, F.V., Monostori, L., Meulen, A.: A survey of applications and requirements of unique identification systems and RFID techniques. Comput. Ind. **62**(3), 227–252 (2011)
15. Lehtonen, M., Ostojic, D., Ilic, A., Michahelles, F.: Securing RFID systems by detecting tag cloning. In: Tokuda, H., Beigl, M., Friday, A., Brush, A.J.B., Tobe, Y. (eds.) Pervasive 2009. LNCS, vol. 5538, pp. 291–308. Springer, Heidelberg (2009). https://doi.org/10.1007/978-3-642-01516-8_20
16. Liu, J., Chen, M., Chen, S., Pan, Q., Chen, L.: Tag-compass: determining the spatial direction of an object with small dimensions. In: IEEE INFOCOM 2017-IEEE Conference on Computer Communications, pp. 1–9. IEEE (2017)
17. Liu, J., Zhu, F., Wang, Y., Wang, X., Pan, Q., Chen, L.: RF-scanner: shelf scanning with robot-assisted RFID systems. In: IEEE INFOCOM 2017-IEEE Conference on Computer Communications, pp. 1–9. IEEE (2017)
18. Liu, X., et al.: Multi-category RFID estimation. IEEE/ACM Trans. Networking **25**(1), 264–277 (2016)
19. Liu, X., et al.: RFID estimation with blocker tags. IEEE/ACM Trans. Networking **25**(1), 224–237 (2016)
20. Liu, X., Xiao, B., Zhu, F., Zhang, S.: Let's work together: fast tag identification by interference elimination for multiple RFID readers. In: 2016 IEEE 24th International Conference on Network Protocols (ICNP), pp. 1–10. IEEE (2016)
21. Okpara, S.: Detecting cloning attack in low-cost passive RFID tags. In: An Analytic Comparison between KILL Passwords and Synchronized Secrets Obinna (2015)
22. Ouafi, K., Vaudenay, S.: Pathchecker: an RFID application for tracing products in supply-chains. Technical report (2009)
23. Piva, M., Maselli, G., Restuccia, F.: The tags are alright: Robust large-scale RFID clone detection through federated data-augmented radio fingerprinting. In: Proceedings of the Twenty-second International Symposium on Theory, Algorithmic Foundations, and Protocol Design for Mobile Networks and Mobile Computing, pp. 41–50 (2021)
24. Romero, H.P., Remley, K.A., Williams, D.F., Wang, C.M.: Electromagnetic measurements for counterfeit detection of radio frequency identification cards. IEEE Trans. Microwave Theory Techniques **57**(5), 1383–1387 (2009)
25. Senthilkumar, C., Thompson, D.R., Di, J.: Fingerprinting RFID tags. IEEE Trans. Depend. Secure Comput. **8**(6), 938–943 (2011)
26. Shahzad, M., Liu, A.X.: Fast and reliable detection and identification of missing RFID tags in the wild. IEEE/ACM Trans. Networking **24**(6), 3770–3784 (2016)

27. Wang, C., Xie, L., Wang, W., Xue, T., Lu, S.: Moving tag detection via physical layer analysis for large-scale RFID systems. In: IEEE INFOCOM 2016-The 35th Annual IEEE International Conference on Computer Communications, pp. 1–9. IEEE (2016)
28. Wang, P., Zhou, Y., Zhu, C., Huang, J., Zhang, W.: Analysis on abnormal behavior of insider threats based on accesslog mining. CAAI Trans. Intell. Syst **12**, 781–789 (2017)
29. Xie, L., Sun, J., Cai, Q., Wang, C., Wu, J., Lu, S.: Tell me what i see: recognize RFID tagged objects in augmented reality systems. In: Proceedings of the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing, pp. 916–927 (2016)
30. Xie, L., Wang, C., Liu, A.X., Sun, J., Lu, S.: Multi-touch in the air: concurrent micromovement recognition using rf signals. IEEE/ACM Trans. Networking **26**(1), 231–244 (2017)
31. Zanetti, D., Fellmann, L., Capkun, S.: Privacy-preserving clone detection for RFID-enabled supply chains. In: 2010 IEEE International Conference on RFID (2010)
32. Zanetti, D., Danev, B., apkun, S.: Physical-layer identification of uhf RFID tags. In: Proceedings of the Sixteenth Annual International Conference on Mobile Computing and Networking, pp. 353–364 (2010)