RF Fingerprint Using Machine Learning Against NFC/ HF RFID Cloning Attacks

Shu He Yang(1), Ching-Hsiang Kung(1), Yu-Chen Huang(1), Helio Augusto Muzamane(1), and Hsin-Chin Liu*(1)
(1) National Taiwan University of Science and Technology, Taipei, Taiwan; 106335; e-mail:
m10907602@mail.ntust.edu.tw; m10907611@mail.ntust.edu.tw; m10907612@mail.ntust.edu.tw;
d10607804@mail.ntust.edu.tw; hcliu@mail.ntust.edu.tw

Near field communication (NFC) tags and proximity integrated circuit cards (PICC) sharing the exact air interface specification of high frequency radio frequency identification (HF RFID), like ISO 14443 A/B, have been widely used for payment or access control applications. These passive devices are threatened by cloning attacks, which cannot be protected by the security system using cryptographic authentication methods. Radio frequency fingerprint (RFF) technology that extracts unique features from the electromagnetic signal emitted by a radio device, is one promising countermeasure against cloning attacks [1] [2] [3].

In [2], the authors use an oscilloscope to record the PICC signals and to extract the RFF features from the recorded signal. These features are obtained using frequency sweep operation, which is non-compliant with standards. In [1] the authors compare the accuracy of various machine learning models, such as convolutional neural network (CNN) and deep neural network (DNN), for the PICC RFF classifier. However, the classifier is limited to legitimate PICCs whose RFF have been registered a priori. Hence these classifier models are not suitable for combating PICC cloning attacks since the RFF of cloned PICC is not in the classifiers training data.

In order to combat the cloning attack, a classifier should have the ability of anomaly (cloned PICC) detection. To achieve this objective, we adopt a CNN-based Support Vector Data Description (CSVDD) classifier similar to [4]. We use statistical features extracted from the "answer to request, Type A (ATQA)" message emitted from PICC cards for classifier training and testing.

In this work, we use 24 legitimate PICCs and six cloned PICCs to perform 10000 tests for each card. The confusion matrices associated with both CNN-based and CSVDD classifiers are shown in Figure 1 (a). For the RFF classifier of legitimate PICC test, both classifiers have high accuracy rates (98.1% and 99.5%) as shown in Figure 1 (a). However, for the RFF classifier of cloned PICC test, the CNN-based classifier only has 50.2% detection accuracy; contradictorily, the detection accuracy of CSVDD classifier is 96.4% as shown in Figure 1 (b). Clearly, RFF classifier using CSVDD is an excellent choice for PICC authentication applications.

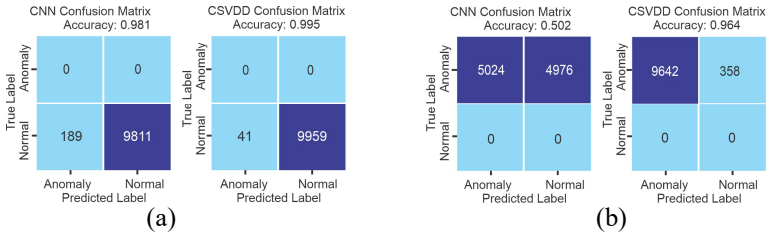

Figure 1. Confusion matrix for the CNN-based and the proposed CSVDD classifiers. The legitimate card classifiers are in (a) and the cloned card classifiers are in (b).

References

[1] W. Lee, S. Y. Baek and S. H. Kim, "Deep-Learning-Aided RF Fingerprinting for NFC Security," *IEEE Communications Magazine,* May 2021.

[2] B. Danev, T. S. Heydt-Benjamin and S. Capkun, "Physical-layer Identification of RFID Devices," *18th USENIX Security Symposium,* pp. 199-214, 2009.

[3] H. P. Romero, K. A. Remley, D. F. Williams and C.-M. Wang, "Electromagnetic Measurements for Counterfeit Detection of Radio Frequency Identification Cards," *IEEE Transaction on Microwave Theory and Techniques,* vol. 5, pp. 1383-1387, May 2009.

[4] C. Liu and K. Gryllias, "A Deep Support Vector Data Description Method for Anomaly Detection in Helicopters," *Proceedings of the 6th European Conference of the Prognostics and Health Management Society ,* pp. 234-242, 2021.