High Accuracy RF-PUF for EM Security through Physical Feature Assistance using Public Wi-Fi Dataset

Md Faizul Bari[#1], Baibhab Chatterjee[#2], Kathiravetpillai Sivanesan[*3], Lily L Yang[*4], Shreyas Sen[#5]
[#]Department of Electrical and Computer Engineering, Purdue University, USA
[*]Intel Corporation, USA
{[1]mbari, [2]bchatte, [5]shreyas}@purdue.edu, [3]kathiravetpillai.sivanesan@intel.com, [4]lily.l.yang@intel.com

***Abstract*— In this work, using physical features extracted from RF nonidealities in communicated EM signals, we show that radio frequency physical unclonable function (RF-PUF) performs much better compared to a solely convolutional neural network (CNN) based secure authentication method, ORACLE. For the static and quasi-static channels, respectively, we achieve 96% and 100% accuracy for RF-PUF compared to 87.13% and 98.6% accuracy for authentication using ORACLE. For the first time, RF-PUF has been applied for Wi-Fi devices to show that $> 95\%$ accuracy can be achieved for a wide range of transmitter and receiver separation from $2ft$ to $62ft$ both for the static and quasi-static channel, showing a peak of $\sim 100\%$ within $38ft$ range for the static case. The design space has been explored in detail. Finally, the concept of RF-PUF has been applied for clustering to detect safe-listed devices.**

***Keywords*— RF-PUF, ORACLE, Wi-Fi, security, clustering**

I. Introduction

A. Background and Motivation

The unprecedented growth in the Internet of Things (IoT) devices has gifted humanity a smart, connected, and comfortable life. But simultaneously, IoT devices pose a new security threat as they are often either mobile or placed in remote areas where unauthorized personnel can have physical access to the device. Due to the wide attacking surface and multiple security threats faced by these devices, they are the weakest point of a large, connected network and define the security of the whole system. The traditional digital signature-based method involves using a symmetric/asymmetric key, Hash-based Message Authentication Codes (HMAC) [1], or OAuth 2.0 [2]. They are vulnerable to various key-hacking attacks and cross-site-recovery forgery (CSRF) [3]. OAuth 2.0 requires manual authentication which is often cumbersome in practice.

To address these issues, various physical signature-based authentication methods have been proposed that use unique device signatures, manifested as nonidealities in the RF signal. Recent developments involve using complex deep neural networks (CNN models, generative adversarial networks, etc.) at the RX to find the pattern variation in unprocessed I-Q samples. One such example is ORACLE [4], which uses an AlexNet-like CNN structure to classify RF devices (Fig. 1(a)). These methods ignore the fact that RF data are contaminated with noise and interference and the absence of any data processing and proper feature extraction cannot exploit the full potential of physical signature variation. An alternative method, called RF-PUF [5], performs *authentication or trust augmentation using RF nonidealities and their statistical parameters as features, analyzed through an onboard neural network (NN)* in an asymmetric network (Fig. 1(b)). In this work, using a publicly available dataset [4] containing data from 16 USRP TX, we show the performance of RF-PUF over ORACLE (the method proposed by the authors of the dataset in use). RF-PUF shows 96% and 100% accuracy for static (fixed TX-RX separation) and quasi-static (a random combination of different TX-RX separation) channels whereas ORACLE shows 87.13% and 98.6% accuracy, respectively. We also show that RF-PUF provides $\sim 100\%$ accuracy for a TX-RX separation of $38ft$, and maintains $> 95\%$ accuracy up to $62ft$. The effect of channel length has been scrutinized and the design space has been explored. In a more realistic scenario of dynamic TX/RX, RF-PUF shows $> 95\%$ accuracy with an optimum model capacity of the employed neural network. Finally, RF-PUF has been applied for clustering the devices in authorized and unauthorized groups.

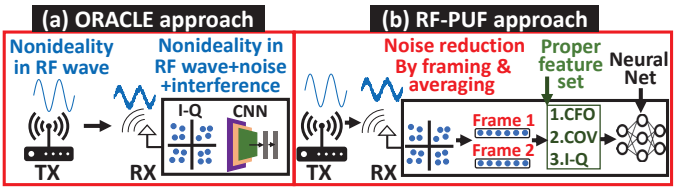

Fig. 1. (a) Noise/interference may overwhelm RF nonidealities in a practical channel. Raw samples with CNN (ORACLE) cannot use the full potential of physical signatures. (b) RF-PUF groups the samples in frames to extract proper features per frame to feed a NN, utilizing the physical signatures better.

B. Related Work

Different temporal and spectral properties of individual transmitters have been used for RF fingerprinting in the past [6], [7]. These methods have various limitations including high oversampling ratio, transient detection, and the use of fixed preamble. MAC-layer protocols have also been used for device authentication. However, device identifiers in upper layers like IMEI number, IP address, MAC address, etc. can be easily attacked and spoofed [8]. Context-aware operation enabled by self learning [9] for IoT communication focuses on achieving minimum energy efficiency, but doesn't address the security issue. Recent work proposes to use dynamic irregular clustering for augmenting trust [10]. Recently, a growing number of works are using deep learning-based methods where raw or slightly processed data are fed into a deep neural

2021 IEEE/MTT-S International Microwave Symposium - IMS 2021 | 978-1-6654-0307-8/21/$31.00 ©2021 IEEE | DOI: 10.1109/IMS19712.2021.9574917

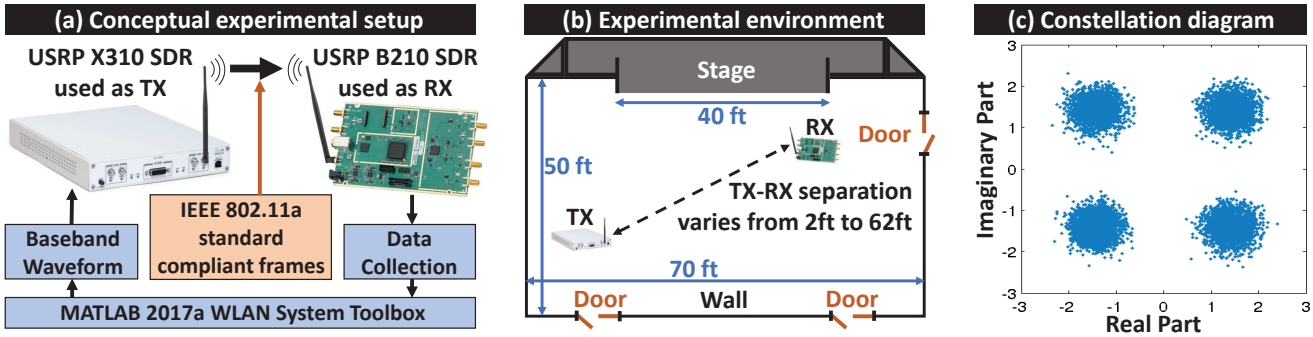

Fig. 2. (a) USRP X310 TX transmits IEEE 802.11a standard-compliant frames (generated in MATLAB) to a USRP B210 RX. (b) The experiment was performed in a $70ft \times 50ft$ room, where the distance between TX and RX is varied from $2ft$ to $62ft$ [4]. (c) Constellation diagram of the raw samples.

network [4], [11], [12], [13]. As wireless data are contaminated with noise and interference, any use of the RF data without processing always posits a risk of huge performance drop in scenarios where environmental nonidealities can go beyond the estimation that was used while designing the network. Also, this approach doesn't provide insight into design parameters.

C. Our Contribution

1) In this work, with the assistance of physical features extracted from RF nonidealities, we have shown **the superiority of RF-PUF with much higher accuracy (100% vs 98.6% for the static and 96% vs 87.13% for the quasi-static channel)** over ORACLE on a publicly available dataset of 16 USRP X310 transmitters.

2) With a comprehensive analysis of TX-RX separation, we have shown that **RF-PUF provides $\sim 100\%$ accuracy for a TX-RX separation of $38ft$, maintaining $> 95\%$ accuracy all the way up to a large TX-RX separation of $62ft$.**

3) The design space has been explored in detail and the effect of the model capacity of the neural network and the amount of train-validation-test data has been analyzed. Also, RF-PUF has been used on the same dataset for clustering.

II. Dataset used for Analysis

A. Experimental Setup and Collected Data

For this work, the "ORACLE RF Fingerprinting Dataset" [4] by Northeastern University has been used which is available publicly. This dataset contains data from 16 USRP X310 radios, transmitting IEEE 802.11a standard-compliant frames generated in MATLAB WLAN System Toolbox to a USRP B210 radio (RX) as shown in Fig. 2(a). The TX-RX separation was varied from $2ft$ to $62ft$ in $6ft$ steps in a large $70ft \times 50ft$ room (Fig. 2(b)). The center carrier frequency was $2.45\,\text{GHz}$ and the sampling rate was $5\,\text{MS}\,\text{s}^{-1}$.

B. Data Processing and Feature Extraction

Fig. 2(c) shows the I-Q representation of the received samples. They were grouped in frames (2560 samples per frame) and 1000 such frames were taken from each TX. Features were extracted from each frame. The coarse carrier frequency offset (CFO) and the ratio of the standard deviation (σ) and mean (μ) of CFO, named coefficient of frequency offset variation (COV), were used as two features. The real and imaginary components of raw samples were taken as 8 other features (10 features in total). From 16 devices, 1000 frames from each, a feature set of size 10×16000 was derived. The whole set was distributed as 70%, 15%, and 15% for training, validation, and test purposes respectively.

III. Results

A. Static vs Quasi-static Channel

We have considered two specific scenarios. Firstly, detection accuracy is calculated for one specific TX-RX separation at a time, labeled as "static channel". Later, a more realistic approach is considered where the data for different TX-RX separations have been randomly combined to form a large dataset. This mimics a dynamic channel where the TX-RX separation varies. We call this "Quasi-static channel".

B. Comparison of RF-PUF with ORACLE framework

Sankhe et al. proposed the ORACLE method [4] using raw I-Q samples directly with an AlexNet-like one-dimensional CNN structure at the RX. RF data in general are contaminated with noise, interference, and other unwanted emissions. Contaminated data can render faulty predictions, especially if the contrast between training and test environment is large. On the other hand, using only statistical parameters as features can force the NN to overfit, as it tends to converge around those constant parameter values. RF-PUF follows a middle ground, taking CFO (RF nonideality) and COV (statistical parameter) along with raw samples. As a result, RF-PUF performs better in similar conditions as shown in Table 1.

Table 1. Performance comparison of RF-PUF [5] and ORACLE [4] on the same dataset shows that RF-PUF performs better in similar conditions.

Condition	**RF-PUF**	**ORACLE**
Fixed TX-RX separation	100%	98.6%
Mixed TX-RX separation	96%	87.13%

C. Device Detection in Static Channel

Fig. 3(a) shows detection accuracy with respect to TX-RX separation. Using a lightweight NN (single layer with 20

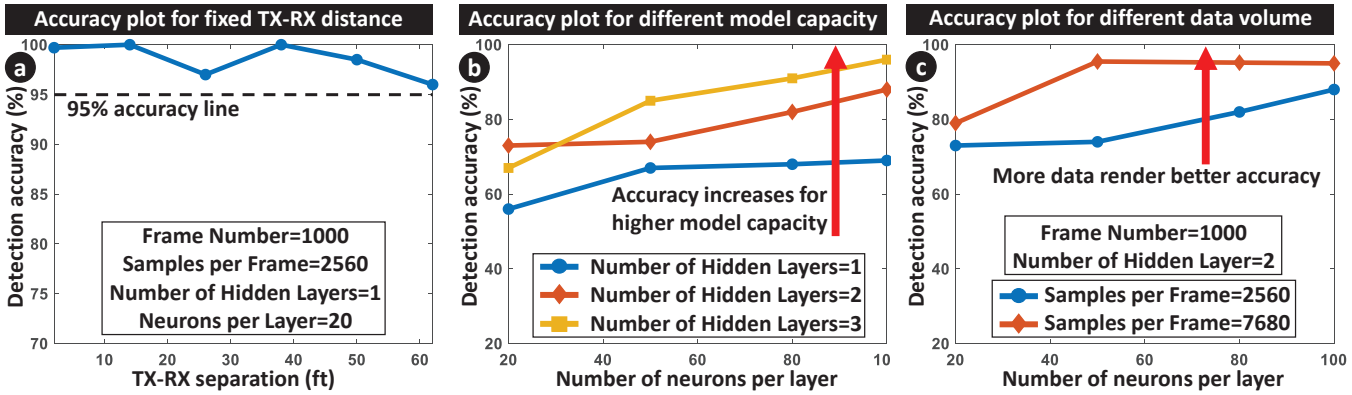

Fig. 3. (a) Accuracy plot for static channel shows $> 95\%$ accuracy even at $62ft$. (b) Accuracy plot for quasi-static channel shows that increasing the number of hidden layers and/or neurons per layer increases accuracy. (c) Increasing train-validation-test data also increases accuracy.

neurons), it has been shown that for up to $38ft$, the accuracy remains 100% (with an outlier at $26ft$). Accuracy drops for higher separation but remains $> 95\%$ up to $62ft$.

D. Device Detection in Quasi-static Channel

The performance for the quasi-static channel is shown below in terms of two important design parameters, the model capacity of the neural network and the data volume.

1) Effect of the Model Capacity of the Network

Fig. 3(b) shows that accuracy increases with the increase in both network width (the number of neurons per layer) and depth (number of hidden layers). So higher model capacity of the NN renders better performance.

2) Effect of Data Volume

Fig. 3(c) shows the effect of data volume on detection accuracy. More sample per frame provides more information. As a result, finding a pattern in the data becomes easier for the NN, and hence accuracy also increases.

E. Clustering

At this point, the initial problem is redefined. Instead of detecting each device individually, they are divided randomly into two groups: authorized (10 devices) and unauthorized (6 devices), and the group or cluster is detected. This is particularly important in applications where specific device detection is not required, rather the identification of safe-listed or authorized devices is important. Here, the same set of features and data distribution (70%, 15%, and 15% for training, validation, and test purpose) have been used. Fig. 4(a) shows that, except for one outlier at $26ft$, the accuracy is $> 95\%$ for the whole TX-RX separation range ($2ft$ to $62ft$) for a static channel. Based on the application in hand, false positive (FP) or false negative (FN) counts might be important. The plot also shows that false positive (FP) or false negative (FN) count curves overlap and except for one outlier, always remains $< 2.5\%$. Fig. 4(b) shows that the accuracy is a bit lower for the quasi-static channel ($> 90\%$), which can be improved with more data or higher width and/or depth of the NN.

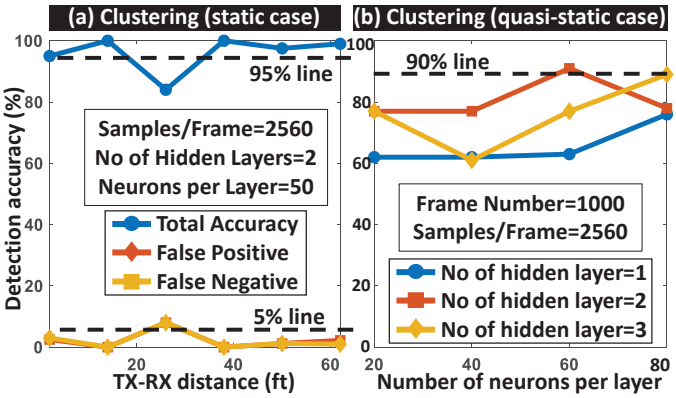

Fig. 4. (a) Accuracy plot for clustering with the static channel. Accuracy is $> 95\%$ in general with similar false positive and false negative count (both $< 2.5\%$ in most cases). (b) Clustering for quasi-static channel shows $> 90\%$ accuracy. Further improvement can be achieved with more data and higher model capacity of the NN as discussed in subsection III-D.

IV. Conclusion

In this work, we show the inherent advantage of RF-PUF, an authentication method for EM security using RF nonidealities and their statistical parameters as features, by showing its better performance over ORACLE, an authentication method that depends solely on AlexNet-like CNN structure. Using a publicly available Wi-Fi dataset of 16 USRP radios used as transmitters, it has been shown that $> 95\%$ accuracy can be achieved for a TX-RX separation range of $2ft$ to $62ft$ with $\sim 100\%$ accuracy even at $38ft$. Detailed analysis of the design space reveals that increasing data volume and/or model capacity of the NN (either by increasing the number of neurons per layer and/or the number of layers) improves detection accuracy. Finally, RF-PUF has been applied to the clustering problem where devices are divided into two groups, showing $> 95\%$ accuracy for the static channel and $> 90\%$ accuracy for the quasi-static scenario. This work proves the efficacy and advantage of RF-PUF in EM security which uses RF nonideality-based physical features without any assistive preamble or modifications to the existing transmitter devices whatsoever.

REFERENCES

[1] H. Krawczyk, M. Bellare, and R. Canetti, "HMAC: Keyed-hashing for Message Authentication," 1997.

[2] D. Hardt *et al.*, "The OAuth 2.0 Authorization Framework," 2012.

[3] E. Shernan, H. Carter, D. Tian, P. Traynor, and K. Butler, "More Guidelines than Rules: CSRF Vulnerabilities from Noncompliant OAuth 2.0 Implementations," in *International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment*. Springer, 2015, pp. 239–260.

[4] K. Sankhe, M. Belgiovine, F. Zhou, L. Angioloni, F. Restuccia, S. D'Oro, T. Melodia, S. Ioannidis, and K. Chowdhury, "No Radio Left Behind: Radio Fingerprinting through Deep Learning of Physical-layer Hardware Impairments," *IEEE Transactions on Cognitive Communications and Networking*, vol. 6, no. 1, pp. 165–178, 2019.

[5] B. Chatterjee, D. Das, S. Maity, and S. Sen, "RF-PUF: Enhancing IoT Security through Authentication of Wireless Nodes using In-Situ Machine Learning," *IEEE Internet of Things Journal*, vol. 6, no. 1, pp. 388–398, 2018.

[6] M. Barbeau, J. Hall, and E. Kranakis, "Detection of Rogue Devices in Bluetooth Networks using Radio Frequency Fingerprinting," in *proceedings of the 3rd IASTED International Conference on Communications and Computer Networks, CCN*. Citeseer, 2006, pp. 4–6.

[7] T. D. Vo-Huu, T. D. Vo-Huu, and G. Noubir, "Fingerprinting Wi-Fi Devices using Software Defined Radios," in *Proceedings of the 9th ACM Conference on Security & Privacy in Wireless and Mobile Networks*, 2016, pp. 3–14.

[8] Q. Xu, R. Zheng, W. Saad, and Z. Han, "Device Fingerprinting in Wireless Networks: Challenges and Opportunities," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 1, pp. 94–104, 2015.

[9] S. Sen, "Invited: Context-aware Energy-efficient Communication for IoT Sensor Nodes," in *2016 53nd ACM/EDAC/IEEE Design Automation Conference (DAC)*, 2016, pp. 1–6.

[10] M. F. Bari, B. Chatterjee, and S. Sen, "DIRAC: Dynamic-IRregulAr Clustering Algorithm with Incremental Learning for RF-based Trust Augmentation in IoT Device Authentication," in *IEEE International Symposium on Circuits and Systems (to be published)*. IEEE, 2021.

[11] T. O'Shea and J. Hoydis, "An Introduction to Deep Learning for the Physical Layer," *IEEE Transactions on Cognitive Communications and Networking*, vol. 3, no. 4, pp. 563–575, 2017.

[12] T. Wang, C.-K. Wen, H. Wang, F. Gao, T. Jiang, and S. Jin, "Deep Learning for Wireless Physical Layer: Opportunities and Challenges," *China Comm.*, vol. 14, no. 11, pp. 92–111, 2017.

[13] C. Zhang, P. Patras, and H. Haddadi, "Deep Learning in Mobile and Wireless Networking: A Survey," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 3, pp. 2224–2287, 2019.