Deep Learning-based RF Fingerprint Authentication with Chaotic Antenna Arrays

1st Justin McMillen
Dept. of Electrical Engineering
University of South Florida
Tampa, United States
jmcmillen@usf.edu

2nd Gokhan Mumcu
Dept. of Electrical Engineering
University of South Florida
Tampa, United States
mumcu@usf.edu

3rd Yasin Yilmaz
Dept. of Electrical Engineering
University of South Florida
Tampa, United States
yasiny@usf.edu

2023 IEEE Wireless and Microwave Technology Conference (WAMICON) | 979-8-3503-9864-9/23/$31.00 ©2023 IEEE | DOI: 10.1109/WAMICON57636.2023.10124899

***Abstract*—Radio frequency (RF) fingerprinting is a tool which allows for authentication by utilizing distinct and random distortions in a received signal based on characteristics of the transmitter. We introduce a deep learning-based authentication method for a novel RF fingerprinting system called Physically Unclonable Wireless Systems (PUWS). An element of PUWS is based on the concept of Chaotic Antenna Arrays (CAAs) that can be cost effectively manufactured by utilizing mask-free laser-enhanced direct print additive manufacturing (LE-DPAM). In our experiments, using simulation data of 300 CAAs each exhibiting 4 antenna elements, we test 5 different convolutional neural network (CNN) architectures under different channel conditions and compare their authentication performance to the current state-of-the-art RF fingerprinting authentication methods.**

***Index Terms*—Physically Unclonable Wireless Systems, RF fingerprinting, Device authentication, Deep learning, Additive manufacturing, 3D printing**

I. Introduction

As the number of Internet of Things (IoT) devices and amount of wireless data communication rapidly increase, so does the threat posed by adversarial parties trying to exploit the vulnerabilities of wireless systems. Hence, it is vital to develop more secure methods of authentication and communication while satisfying the quality and efficiency constraints. With current technology, security at higher levels in the system (software) usually cannot protect lower layers (such as spoofing and jamming of hardware). Therefore, to work towards a more secure system, physical layer security features can and must complement the upper layer defenses, e.g., multi-factor authentication through RF fingerprinting. With ever increasing technology available to attackers and the emergence of much faster computing methods, traditional encryption techniques will not always be as secure as they currently are [1]. With this in mind, it is imperative to find new, harder-to-crack hardware-based methods to allow for secure systems.

RF fingerprinting is a promising authentication technique for physical layer security. The classical RF fingerprinting methods utilize the small amplitude, phase, and frequency variations that are unique to each device due to the inevitable randomness during the fabrication of the RF integrated circuits (ICs) connected to the antenna elements [2], [3]. These signatures, while being detectable by Machine Learning (ML) algorithms [4], are extremely small due to tight IC fabrication tolerances. State-of-the-art deep neural networks can only achieve around 63% accuracy in authenticating 250 devices using these small signatures [5].

We investigate the concept of *Physically Unclonable Wireless Systems* (PUWS) as a new hardware security architecture to augment RF fingerprinting-based authentication. PUWS can effectively be built by additive manufacturing approaches where multiple devices within the structure can be randomized to exhibit enhanced and distinct fingerprints. An important element for PUWS is chaotic antenna arrays (CAAs) where antenna shapes, locations, and feed networks are randomized [6]. The prior work [6] on CAA assumed that the user with CAA has knowledge of the wireless channel, its own phase errors, and with no spatially varying phase errors. Such knowledge by the device is undesired and mostly impractical for real life applications. In this paper, we extend the CAA concept to work *without* the knowledge of wireless channel or its own errors during authentication by resorting to deep learning-based detection algorithms. The mask-free laser-enhanced direct print additive manufacturing (LE-DPAM) technology investigated by our group can play as the key enabler of such antenna arrays[7]–[10]. Introducing randomness will generate RF fingerprints based on phase errors at the antenna elements with spatial (i.e., θ, ϕ) variance, which will be shown to greatly benefit physical layer authentication with RF fingerprint enhancement.

II. Chaotic Antenna Array Model

For the model, we consider aperture coupled rectangular patch antennas and introduce randomness into the geometry of the patch and the length of a meandered feed line section inserted between the coupling aperture and feed point. The superstrate, substrate, and coupling aperture thicknesses are kept constant. The unperturbed patch is 14.4 x 12 mm^2 and resonates at 5.8 GHz with 12% matching bandwidth, well above ISM bandwidth, allowing resonance shifts by these randomizations to be tolerable. Corner points (x_i, y_i), $i \in \{1, 2, 3, 4\}$ are randomized according to:

$$(x_i, y_i) = (x_i = r\cos\psi + c_i\cos\tau_i, y_i + r\sin\psi + c_i\sin\tau_i) \quad (1)$$

This work was funded by U.S. National Science Foundation (NSF) under grant 2233774.

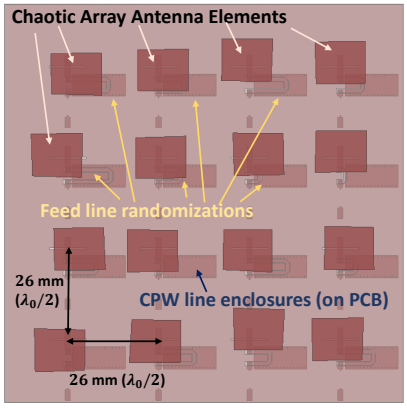

Fig. 1. Ansys model of a 4×4 5.8 GHz ISM band CAA with randomized antenna positions, shapes, and feed line lengths.

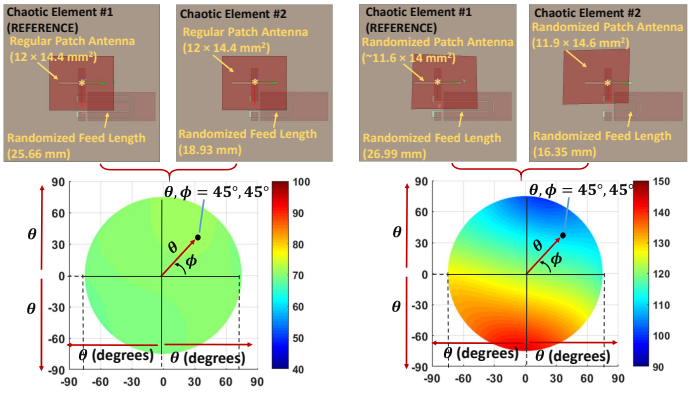

Fig. 2. Phase error w.r.t. a reference antenna in polar coordinates. (Left) Feed line randomization generates a constant error in all transmission directions; (Right) Antenna geometry randomization creates θ, ϕ dependent error.

where $r \in U[0, R]$ and $\psi \in U[0, 2\pi]$, denoting a randomized shift in the center point of the rectangle with respect to the coupling aperture. $c_i \in U[0, C]$ and $\tau_i \in U[0, 2\pi]$ are used to perturb the corners of the shifted rectangle to change its shape into a trapezoid. U represents a uniform distribution while R and C set maximum limits for the randomizations, set to 4mm and 0.5mm, respectively. Figure 1 shows a 16 element CAA that can be formed from the randomized antennas. The CAA technique is suitable for any frequency band and 5.8 GHz ISM is selected for popularity and availability of components to form a test bed in near future. Antenna spacing is half-wavelengths as in traditional practice.

Randomizing the antenna shape provides the spatial variance property depicted in Fig. 2. While feed line length randomization alone creates an enhanced signature transmitted equally in all directions, like the traditional RF fingerprint, antenna shape randomization causes the phase error to depend on the direction of radiation as evidenced by the colorful phase distribution in Fig.2. Histogram data obtained from 1200 antennas shows that phase error is uniformly distributed across a $[0, \sim 2\pi]$ range.

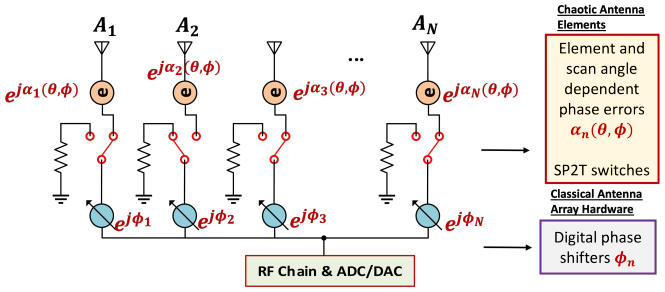

Fig. 3. Circuit diagram of CAA. Each chaotic antenna element is sequentially turned on using switches and has a random and direction-dependent phase error due to its unique geometry.

III. Authentication

The present state-of-the-art in RF fingerprinting-based authentication relies on deep neural networks [5], [11], [12], as opposed to earlier schemes that used traditional ML techniques (e.g., SVM, kNN, etc.) [13], [14], statistical detectors [15], and wavelet transforms. Modern deep convolutional neural networks (CNNs) can successfully authenticate naturally occurring signatures in the RF chain in idealized setups with a small number of devices, according to recent literature [11], [12]. However, [5] recently showed in a sizable study that even for cutting-edge deep CNNs, *naturally occurring RF fingerprints are insufficient under realistic circumstances with a large number of devices and changing channel conditions between training and testing*.

A. Simulation Setup

For a study on the feasibility of RF fingerprint authentication on PUWS, we used simulation data describing the phase variation of 1200 antenna elements and formed 300 CAAs each with 4 antenna elements. The elevation angle θ and the azimuth angle ϕ from the transmitting CAA to the receiver is randomly selected within [0°, 75°] and [-180°, 180°], respectively. We simulated a $f = 5$ GHz WiFi environment with Rayleigh multipath fading, in which people may be walking between the device and the router. Considering a walking speed V_{walk} of 1 m/sec, the maximum Doppler shift f_d is calculated as 16.67 Hz using the formula $f_d = (V_{walk}/c)f$, with the channel coherence time under the Clarke's model, $T_c = \sqrt{9/16\pi f_d^2} = 0.0254$ sec. With a sampling rate of 1 MHz, $N = 1000$ samples are collected within an authentication sequence of 1 msec.

In each authentication sequence, the 4 antennas in a CAA are turned on sequentially to transmit a complex pilot signal, as illustrated in Fig. 3. The circuit diagram in Fig. 3 also shows the chaotic antenna elements with random and direction-dependent phase errors together with the classical digital phase shifters. The authenticator receives the in-phase and quadrature (I/Q) samples through Rayleigh multipath fading channels in addition to additive white Gaussian noise:

$$y_n = h_n x_n + w_n, \tag{2}$$

where $x_n = e^{j\alpha_n}$ is the transmitted pilot signal with constant amplitude and the corresponding phase error α_n,

TABLE I
TEST ACCURACY

Model	Accuracy %
CNN-3	93.3
VGG-16	93.5
ResNet-50	99.2
Inception	**99.9**
Xception	**99.9**

$h_n \sim \mathcal{N}_c(0, \sigma_h^2)$ is the zero-mean complex Gaussian channel coefficient, and $w_n \sim \mathcal{N}_c(0, \sigma_w^2)$ is the additive white complex Gaussian noise. The I and Q samples are the real and imaginary parts of the received signal. With 4 antenna elements in each array and collecting I and Q samples of the received signal from each antenna, the dataset used to authenticate a CAA has a size of $N \times 8$, where $N = 1000$ is the number of samples within an authentication session. The CAA phase errors and the received signals through Rayleigh fading channels were simulated in Matlab. The signal-to-noise ratio (SNR) is set to 20 dB in the simulations, i.e., $\sigma_w^2 = 0.01$. The CAA data is separated using a (80-10-10)% split for training, validation, and testing, respectively.

To better understand how CAA affects RF fingerprint authentication, 5 different CNN architectures were selected. A basic CNN consisting of two convolutional layers each with 64 neurons followed by a single dense layer forms the baseline performance comparison for the following models. The other models include VGG-16, a 16 layer neural network [16]; ResNet-50, a 50 layer network which introduces the concept of residual connections between layers [17]; Inceptionv3, a deep CNN which utilizes a 'network within a network' strategy to learn features more deeply [18]; and Exception, an Inception based model which utilizes residual connections and separable convolutional layers to improve accuracy [19]. These models were originally intended for image classification, usually taking $244 \times 244 \times 3$ size inputs, hence modifications to the top layers were necessary to work with the received I/Q samples of size $1000 \times 8 \times 1$, where the 8 columns correspond to the I and Q signal samples from the 4 antenna elements.

B. Results

Table I shows the test classification accuracy for each of the networks trained and tested in Python using TensorFlow. Even the baseline CNN-3 scores significantly above the 63% accuracy, which is the existing state-of-the-art performance in the literature achieved by ResNet-50 using the traditional (non-CAA) RF fingerprints [5]. The more advanced networks, VGG-16 and ResNet-50, Inception, and Xception, all achieve much higher accuracies. Comparing the performances of ResNet-50 using the CAA fingerprints ($> 99\%$) to the traditional RF fingerprints (63%) [5] in similar setups, we see that the CAA fingerprints enable significantly enhanced authentication capacity with the help of deep neural networks.

IV. CONCLUSION

As dishonest actors develop more advanced security cracking technologies, it is vital that security keep in-step, lest vital systems become vulnerable to attack. More than ever there is a need for fast, cheap, secure authentication methods. In this vein, we investigated a novel authentication concept and implementation of RF fingerprinting through chaotic antenna arrays (CAAs). By testing 5 popular convolutional neural network (CNN) architectures, we showed that deep learning-based authentication utilizing CAA fingerprints significantly outperforms the existing state-of-the-art results using traditional RF fingerprints found in all communication devices. Compared to the 63% accuracy [5] achieved by ResNet-50, a popular CNN architecture, using the traditional RF fingerprints, the CAA fingerprints enable over 99% accuracy by ResNet-50 in the task of authenticating 300 devices under Rayleigh fading channels.

REFERENCES

[1] P. Shor, "Algorithms for quantum computation: Discrete logarithms and factoring," in *Proceedings 35th Annual Symposium on Foundations of Computer Science*, 1994, pp. 124–134. DOI: 10.1109/SFCS.1994.365700.

[2] G. E. Suh and S. Devadas, "Physical unclonable functions for device authentication and secret key generation," pp. 9–14, 2007.

[3] K. Zeng, K. Govindan, and P. Mohapatra, "Non-cryptographic authentication and identification in wireless networks [security and privacy in emerging wireless networks]," *IEEE Wireless Communications*, vol. 17, no. 5, pp. 56–62, 2010. DOI: 10.1109/MWC.2010.5601959.

[4] A. Jagannath, J. Jagannath, and P. S. P. V. Kumar, "A comprehensive survey on radio frequency (rf) fingerprinting: Traditional approaches, deep learning, and open challenges," 2022. DOI: 10.48550/ARXIV.2201.00680. [Online]. Available: https://arxiv.org/abs/2201.00680.

[5] T. Jian, B. C. Rendon, E. Ojuba, *et al.*, "Deep learning for rf fingerprinting: A massive experimental study," *IEEE Internet of Things Magazine*, vol. 3, no. 1, pp. 50–57, 2020. DOI: 10.1109/IOTM.0001.1900065.

[6] M. Karabacak, B. Peköz, G. Mumcu, and H. Arslan, "Arraymetrics: Authentication through chaotic antenna array geometries," *IEEE Communications Letters*, vol. 25, no. 6, pp. 1801–1804, 2021.

[7] M. Kacar, J. Wang, G. Mumcu, *et al.*, "Phased array antenna element with embedded cavity and mmic using direct digital manufacturing," in *2019 IEEE International Symposium on Antennas and Propagation & USNC-URSI Radio Science Meeting*, 2019, pp. 81–82. DOI: 10.1109/APUSNCURSINRSM.2019.8888323.

[8] M. Kacar, C. Perkowski, P. Deffenbaugh, J. Booth, G. Mumcu, and T. Weller, "Wideband ku-band antennas using multi-layer direct digital manufacturing," in *2017 IEEE International Symposium on Antennas and Propagation & USNC/URSI National Radio Science Meeting*, 2017, pp. 1243–1244. DOI: 10.1109/APUSNCURSINRSM.2017.8072664.

[9] M. Kacar, T. M. Weller, and G. Mumcu, "3d printed wideband multilayered dual-polarized stacked patch antenna with integrated mmic switch," *IEEE Open Journal of Antennas and Propagation*, vol. 2, pp. 38–48, 2021. DOI: 10.1109/OJAP.2020.3041959.

[10] R. A. Ramirez, E. A. Rojas-Nastrucci, and T. M. Weller, "Laser-assisted additive manufacturing of mm-wave lumped passive elements," *IEEE Transactions on Microwave Theory and Techniques*, vol. 66, no. 12, pp. 5462–5471, 2018. DOI: 10.1109/TMTT.2018.2873294.

[11] K. Sankhe, M. Belgiovine, F. Zhou, S. Riyaz, S. Ioannidis, and K. Chowdhury, "Oracle: Optimized radio classification through convolutional neural networks," in *IEEE INFOCOM 2019 - IEEE Conference on Computer Communications*, 2019, pp. 370–378. DOI: 10.1109/INFOCOM.2019.8737463.

[12] N. Soltani, G. Reus-Muns, B. Salehi, J. Dy, S. Ioannidis, and K. Chowdhury, "Rf fingerprinting unmanned aerial vehicles with non-standard transmitter waveforms," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 12, pp. 15 518–15 531, 2020. DOI: 10.1109/TVT.2020.3042128.

[13] B. Danev, T. S. Heydt-Benjamin, and S. Capkun, "Physical-layer identification of rfid devices.," in *USENIX security symposium*, 2009, pp. 199–214.

[14] F. zhuo, Y. Huang, and J. chen, "Radio frequency fingerprint extraction of radio emitter based on i/q imbalance," *Procedia Computer Science*, vol. 107, pp. 472–477, 2017, Advances in Information and Communication Technology: Proceedings of 7th International Congress of Information and Communication Technology (ICICT2017), ISSN: 1877-0509. DOI: https://doi.org/10.1016/j.procs.2017.03.092. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1877050917303678.

[15] H. Patel, "Non-parametric feature generation for rf-fingerprinting on zigbee devices," in *2015 IEEE Symposium on Computational Intelligence for Security and Defense Applications (CISDA)*, 2015, pp. 1–5. DOI: 10.1109/CISDA.2015.7208645.

[16] K. Simonyan and A. Zisserman, *Very deep convolutional networks for large-scale image recognition*, 2014. DOI: 10.48550/ARXIV.1409.1556. [Online]. Available: https://arxiv.org/abs/1409.1556.

[17] K. He, X. Zhang, S. Ren, and J. Sun, *Deep residual learning for image recognition*, 2015. DOI: 10.48550/ARXIV.1512.03385. [Online]. Available: https://arxiv.org/abs/1512.03385.

[18] C. Szegedy, V. Vanhoucke, S. Ioffe, J. Shlens, and Z. Wojna, *Rethinking the inception architecture for computer vision*, 2015. DOI: 10.48550/ARXIV.1512.00567. [Online]. Available: https://arxiv.org/abs/1512.00567.

[19] F. Chollet, *Xception: Deep learning with depthwise separable convolutions*, 2016. DOI: 10.48550/ARXIV.1610.02357. [Online]. Available: https://arxiv.org/abs/1610.02357.