Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000.

Digital Object Identifier 10.1109/ACCESS.2024.0429000

Hardware and Deep Learning-Based Authentication through Enhanced RF Fingerprints of 3D-Printed Chaotic Antenna Arrays

JUSTIN MCMILLEN[1,*], (Graduate Student Member, IEEE) FAWAZ ABDUL RAZAK[1,*], GOKHAN MUMCU[1], (Senior Member, IEEE), and YASIN YILMAZ[1], (Senior Member, IEEE)

[1]Department of Electrical Engineering , University of South Florida, Tampa, United States (e-mails: {jmcmillen,fawaz243,mumcu,yasiny}@usf.edu)

[*]Equal contribution.

Corresponding author: Yasin Yilmaz (e-mail: yasiny@usf.edu).

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

ABSTRACT Radio frequency (RF) fingerprinting is a hardware-based authentication technique utilizing the distinct distortions in the received signal due to the unique hardware differences in the transmitting device. Existing RF fingerprinting methods only utilize the naturally occurring hardware imperfections during fabrication; hence their authentication accuracy is limited in practical settings even when state-of-the-art deep learning classifiers are used. In this work, we propose a Chaotic Antenna Array (CAA) system for significantly enhanced RF fingerprints and a deep learning-based device authentication method for CAA. We provide a mathematical model for CAA, explain how it can be cost-effectively manufactured by utilizing mask-free laser-enhanced direct print additive manufacturing (LE-DPAM), and comprehensively analyze the authentication performance of several deep learning classifiers for CAA. Our results show that the enhanced RF signatures of CAA enable highly accurate authentication of hundreds of devices under practical settings.

INDEX TERMS 3D printing, additive manufacturing, deep learning, device authentication, RF fingerprinting, physical layer, wireless communications, security.

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 (such as storing a secret key in nonvolatile memory to perform cryptographic primitives) is not sufficient against sophisticated attacks. In addition, invasive and non-invasive attacks have been shown to learn secret keys [1], [2] as the key must exist at all times in digital form. Cryptography can also be prohibitive for certain low-cost, lower-power, and resource-constrained IoT devices. 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 [3]. To this end, hardware-based security methods can complement the upper layer defenses, e.g., multi-factor authentication through radio frequency (RF) fingerprinting.

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 [4], [5]. However, since IC manufacturing is tailored towards cost-effective and high volume manufacturing of identical devices, the fingerprint signatures from ICs are weak. For example, while being detectable by Machine Learning (ML) algorithms [6], state-of-the-art deep neural networks could only achieve around 63% accuracy in authenticating 250 devices when trying to make use of these small signatures [7]. In this work, we build upon our previous findings, [8], to leverage a novel randomized antenna array concept, called Chaotic Antenna Array (CAA), for significantly enhanced RF signatures, and in turn, highly accurate authentication.

In CAAs, shapes of the antenna elements, their locations within the array grid, and their feed networks are intentionally randomized based on a desired probability density function.

Although such geometry randomizations can possibly be realized with several techniques, such as the widely available printed circuit board (PCB) manufacturing, 3D-printing techniques such as laser-enhanced direct print additive manufacturing (LE-DPAM), stand out as strong candidates. Unlike many types of traditional manufacturing, LE-DPAM is mask-free and generates the device structure layer-by-layer, making randomizations available for little to no cost. We have shown capabilities of LE-DPAM in realizing antennas and arrays with embedded control ICs and RF/digital lines - paving the way for introducing randomizations at any level of the device structure [9]–[12].

Our prior theoretical work [13] on device authentication with CAAs assumed that the user with the CAA has knowledge of the wireless channel and most importantly, its own phase signatures. Moreover, the phase signatures were assumed to be transmitted equally in all directions with no spatial variation. However, if phase signatures are known by the device utilizing the CAA (i.e., stored in memory), the device will be prone to secret key based security attacks, as the keys are also stored in memory. Hence, the device with the CAA must be unaware of its own phase errors for the most beneficial, real-world application. In this paper, our goal is to extend the CAA based authentication concept to work without knowledge of the wireless channel or its own signatures by resorting to deep learning-based detection algorithms. Another key novelty is related to the antenna element position randomization. This type of randomization generates an antenna element specific phase error (i.e., RF fingerprint) which is transmitted with spatial (i.e., θ, ϕ) variance with respect to the classical antenna array factor. This type of spatial variation greatly benefits physical layer authentication. When combined with antenna element-specific feed line length randomization (which creates a large scale phase error, but with no spatial variance), the CAA provides an order of magnitude enhanced RF fingerprint, which forms a strong signature for ML-based authentication techniques. Overall contributions reported in this manuscript can be summarized as:

- We comprehensively analyze the authentication performance of CAAs through mathematical modeling, numerical simulations, and preliminary experimental results; and show that highly accurate (nearing 100%) authentication with hundreds of devices is possible through deep learning methods. Neither the CAA device nor the authenticator need to know/store the RF signatures (i.e., phase differences).
- We explain an interesting phenomenon: a performance drop in deep learning-based authentication when the authentication duration matches the channel coherence time.
- Through theoretical array factor, we show that the CAA exhibits a direction-dependent signature due to the randomized antenna location. This can provide extra security against attackers who might try to capture the RF signature. In traditional RF fingerprinting, attackers can simulate the signature by collecting data from any direction and using them to train ML algorithms [14].
- We provide a practical discussion of how the antenna elements of CAAs can be designed and manufactured using LE-DPAM. We also demonstrate that antennas with randomized locations and feed line lengths may perform with good impedance matching while offering phase error variations that are within the entire 2π range.

The remainder of the paper is organized as follows: In Section II, the mathematical model of a CAA is presented. The proposed authentication scheme based on CAAs and deep learning is studied in Section III. Section IV explains cost-effective practical implementation of CAAs. Finally, the paper is concluded in Section V.

II. CHAOTIC ANTENNA ARRAY MATHEMATICAL MODEL

In this section, we consider the mathematical model of the Chaotic Antenna Array (CAA) to study the electric field for a randomized antenna array. We start with the traditional rectangular array consisting of $M \times N$ antennas arranged uniformly on a rectangular grid. Centers of antenna elements in a traditional array are illustrated by the filled green circles in Fig. 1. The center position of antenna element (m, n), $m = 1, 2, ..., M$, $n = 1, 2, ..., N$ without any perturbation is denoted by the position vector $\boldsymbol{r}_{mn}$, which can be written as:

$$\boldsymbol{r}_{mn} = (m-1)d_x\hat{\boldsymbol{x}} + (n-1)d_y\hat{\boldsymbol{y}}, \tag{1}$$

where $\hat{\boldsymbol{x}}$ and $\hat{\boldsymbol{y}}$ are unit vectors, d_x and d_y are the distances between the two antenna elements in the direction of x-axis and y-axis, respectively. Throughout the manuscript, bold text is used for vectors. Each antenna element, by itself, at the center of the coordinate system radiates the electric field

$$\mathbf{E}_{mn} = \mathbf{e}_{mn}(\theta, \phi)\frac{e^{-jkr}}{r} \tag{2}$$

where $\mathbf{e}_{mn}$ represents the field pattern in spherical coordinate system as a function of θ and ϕ, r is the distance to observation point, k is the wavenumber given by $2\pi f/c$, where f denotes frequency and c is the speed of light. Ignoring the mutual couplings, and assuming identical antenna elements for the array, we can express $\mathbf{e}_{mn}(\theta, \phi) = \mathbf{e}(\theta, \phi)\ \forall mn$. Although randomization of antenna shapes is also possible, we do not investigate such randomizations in this work.

We proceed by perturbing the location of each antenna element within the uniformly spaced antenna array. The locations of the antenna elements are denoted by the unfilled red circles in Fig. 1 and can be expressed as

$$\boldsymbol{r}'_{mn} = (m-1)d_x\hat{\boldsymbol{x}} + (n-1)d_y\hat{\boldsymbol{y}} + \alpha_{mn}(\hat{\boldsymbol{x}}\cos\gamma_{mn} + \hat{\boldsymbol{y}}\sin\gamma_{mn}) \tag{3}$$

where $\alpha_{mn} \in U(0, \alpha_{max})$ and $\gamma_{mn} \in U(0, 2\pi)$ are uniformly distributed perturbation magnitude and angle. α_{max} denotes the maximum radius of perturbation. In a practical CAA realization, α_{max} will be restricted by the amount of mutual coupling that can be tolerated by the wireless communication

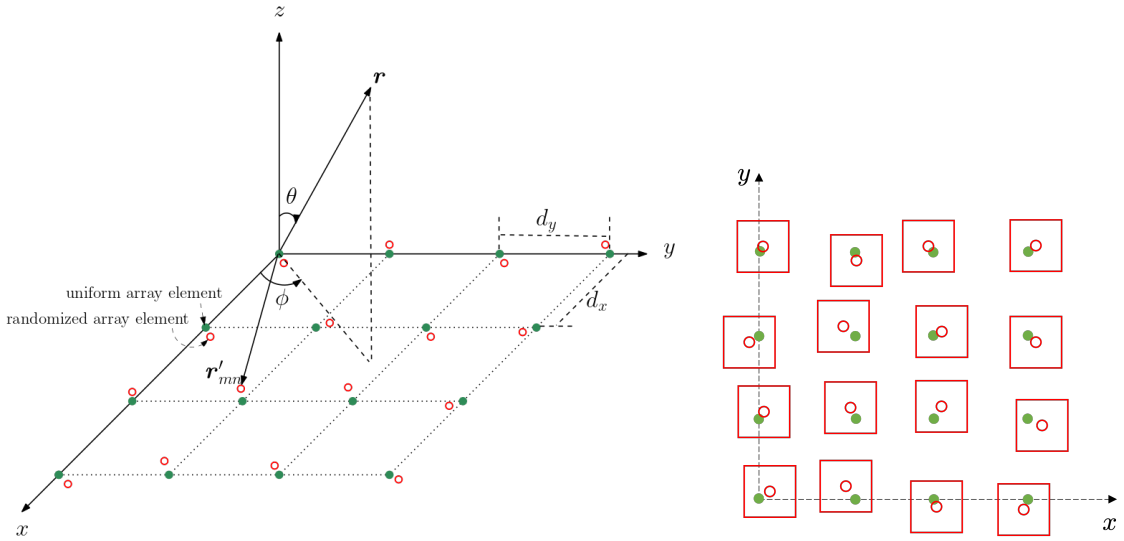

FIGURE 1. **Traditional uniform rectangular array antenna center locations are shown with green filled circles. Left: Randomized antenna center locations in the CAA are shown with red unfilled circles. 3D array geometry to study electric field radiation. Right: 2D sketch of the CAA with randomized antenna elements shown as red squares.**

system. For a regular antenna array with antenna elements spaced in half-wavelength increments, α_{max} therefore will be limited to fractions of a wavelength, generating phase errors not reaching up to the full 2π range. To address this, we also introduce a random perturbation in the feed line length of each antenna element, which will generate an additional phase term of $e^{-jL_{mn}}$ in the electric field equation, where $L_{mn} \in U(0, 2\pi)$.

Based on the well-known far-field approximations in antenna theory [15], the electric field radiated by an antenna element located at $\boldsymbol{r}'_{mn}$ can be written as

$$\mathbf{E}_{mn} = \mathbf{e}(\theta, \phi) \frac{e^{-jk(r - \hat{\boldsymbol{r}} \cdot \boldsymbol{r}'_{mn})}}{r} e^{-jL_{mn}}, \tag{4}$$

where

$$\hat{\boldsymbol{r}} = \hat{\boldsymbol{x}} \sin\theta \cos\phi + \hat{\boldsymbol{y}} \sin\theta \sin\phi + \hat{\boldsymbol{z}} \cos\theta \tag{5}$$

is the unit vector along the direction of observation. Rearranging and carrying out the vector dot product in (4) leads to the expression

$$\begin{aligned} \mathbf{E}_{mn} = \mathbf{e}(\theta, \phi) & \frac{e^{-jkr}}{r} \\ & \times e^{jk(m-1)d_x \sin\theta \cos\phi} e^{jk(n-1)d_y \sin\theta \sin\phi} \\ & \times e^{jk\alpha_{mn} \cos\gamma_{mn} \sin\theta \cos\phi} e^{jk\alpha_{mn} \sin\gamma_{mn} \sin\theta \sin\phi} \\ & \times e^{-jL_{mn}}. \end{aligned} \tag{6}$$

The second line in equation (6) is well recognized as the terms of the array factor belonging to a traditional uniformly spaced antenna array structure. The terms in the third and fourth lines are generated by the randomizations introduced to create the CAA. Therefore, the phase delays implied by these terms can also be considered as ‘‘phase errors" or ‘‘phase signatures" that are unique to the CAA. More specifically, the terms in the third line stem from the antenna location randomizations α_{mn} and γ_{mn}. These terms are dependent on

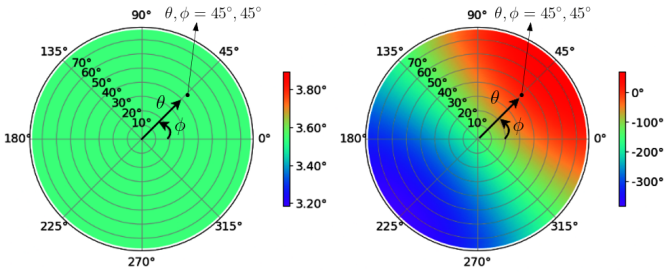

FIGURE 2. **Phase signature w.r.t. a reference antenna in spherical coordinates. The circular angle represents ϕ and the radius (i.e., concentric circles) represents the θ variation. The colormap illustrates the phase difference. Left: Feed line randomization generates a constant signature in all transmission directions. Right: Antenna geometry randomization creates θ, ϕ dependent signature.**

(θ, ϕ), implying a spatial variance in 3D space. The fourth line is the phase delay due to the feed line randomization L_{mn}. This term has no (θ, ϕ), hence the phase delay is transmitted identically to entire 3D space. Fig. 2 presents an example to illustrate the phase signature and spatial variance properties of an antenna element of a CAA with respect to its own unperturbed location and reference line. Feed line length randomization alone creates a signature transmitted equally in all directions, similar to a traditional RF fingerprint, but significantly enhanced. Likewise, when antenna position randomization is incorporated alongside feedline randomization, a phase variation that depends on the direction of radiation is generated, as evidenced by the colored phase distribution in Fig.2. It is important to note that since the equations are based on the far-field approximations, they are not applicable in the near-field region. The scenario in which the authenticator is placed within the near-field of the CAA must be investigated separately and is beyond the scope of this manuscript.

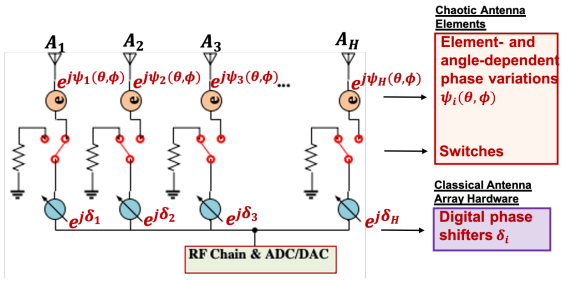

FIGURE 3. Circuit diagram of a CAA. Each chaotic antenna element is sequentially turned on using switches and has a random and direction-dependent phase signature due to its unique geometry.

III. AUTHENTICATION

Early RF fingerprint authentication schemes used statistical detectors [16], and wavelet transforms [17]–[19]. More recently, traditional machine learning methods have been applied to this problem, such as k-Nearest Neighbors (kNN) or Support Vector Machines (SVM), among others [20], [21]. Present state-of-the-art relies on deep neural networks [7], [22], [23], where 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 [22], [23]. However, [7] recently showed in a sizable study that naturally occurring RF fingerprints are insufficient even for cutting-edge deep CNNs (63% accuracy) under realistic circumstances with a large number of devices. They go on to show that under differing training and test environment conditions, accuracy can drop as low as 35%. This section presents the proposed authentication scheme based on CAA and shows that the enhanced RF fingerprints of CAA enable close-to-perfect (99%) authentication accuracy in scenarios similar to the ones considered in [7]. Fig. 3 depicts the circuit diagram of the CAA used within the proposed scheme. The terms which follow the switches and digital phase shifters represent spatially dependent phase signatures of each antenna element, denoted by $e^{j\psi_i(\theta,\phi)}$, $i = 1, 2, \ldots, H$, where $H = MN$. The digital phase shifters are an essential part of the system for analog beamforming during the wireless communication stage. In addition to phase shifters, switches are included to provide access to individual antennas during the proposed CAA-based authentication scheme.

A. AUTHENTICATION WITH CAA AND THREAT MODEL

Consider a physical layer (PHY) authentication system employing CAAs, in which a set $\mathcal{L}$ of K legitimate users need to first authenticate their identity before receiving service (Fig. 4). During authentication, user k transmits a complex pilot signal by sequentially turning on its H antennas using the switches as shown in the block diagram of CAA in Fig. 3. This provides the authenticator with an H-dimensional complex fingerprint $x_k \in \mathbb{C}^H$, which includes the random phase response of each antenna element. A distorted fingerprint $y_{k,t} \in \mathbb{C}^H$ is received by the authenticator during

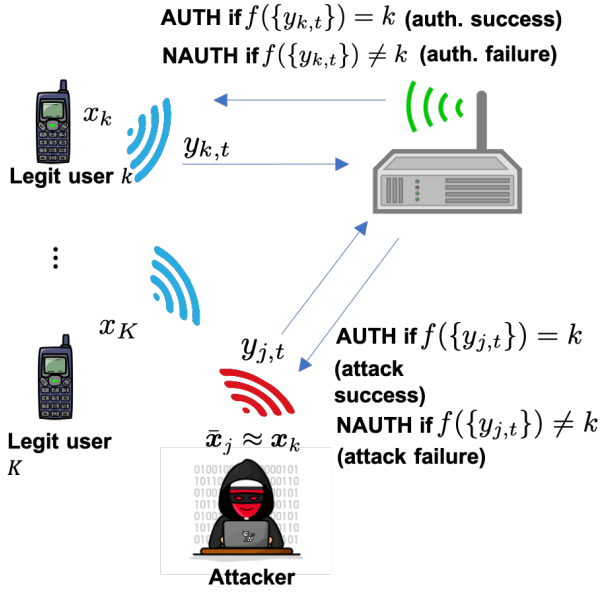

FIGURE 4. Threat model for authentication. Targeted: attacker knows the login credentials of a legitimate user and tries to spoof its RF fingerprint. Untargeted: login credentials are not used in upper layers and authenticator checks only the RF fingerprint: AUTH if $f(y_{k,i}) \in \{1, \ldots, K\}$, NAUTH if $f(y_{k,i}) = 0$.

the authentication session because of wireless channel uncertainties such as multiplicative and additive noise, multipath fading, Doppler shift, etc. To deal with such uncertainties, the authenticator builds a function $f(\{y_{k,t}\}_t) \in \{0, 1, \ldots, K\}$ in a secure training session using several training data instances received from all legitimate users. Success in authentication is defined as $f(\{y_{k,t}\}) = k$ for $k \in \mathcal{L}$ or $f(\{y_{j,t}\}) = 0$ for an illegitimate user $j \notin \mathcal{L}$.

An impersonation attack [24] is defined as an illegitimate user $j \notin \mathcal{L}$ trying to authenticate as a legitimate user. If there is also an upper-layer authentication system, such as passwords or MAC addresses, in addition to PHY authentication, then the attacker must target a specific legitimate user. In such targeted attacks, as shown in Fig. 4, the attacker aims to design an RF fingerprint $\bar{x}_j \approx x_k$, different from its own fingerprint x_j through software, so that $f(\{y_{j,t}\}) = k$, where $\{y_{j,t}\}$ is the received signal as a result of transmitted $\bar{x}_j$. When there is no additional authentication system, the attacker may also perform an untargeted attack by simply trying to get authenticated as any of the legitimate users, i.e., $f(\{y_{j,t}\}) \neq 0$.

B. SIMULATION SETUP

For a study on the feasibility of CAA-based RF fingerprint authentication, we generated data using the mathematical framework described in Section II. From this framework, 1200 antennas were simulated, which were grouped into $K = 300$ CAAs, each with $H = 4$ antenna elements configured in a square grid as $M = 2$ and $N = 2$. α_{max} was set at 4 mm, d_x and d_y were both set at 26 mm, and the radial distance r to the observation point was set at 5 m. The azimuth angle ϕ and the polar angle θ from the transmitting CAA to the receiver are randomly selected within $[-180°, 180°]$ and

TABLE 1. Dataset Parameters

Var \ Set	1	2	3	4	5	6	7
F_s (kHz)	10	10	10	10	10	100	1000
V_{move} (m/s)	1	5	10	0.5	0.1	1	1
f_d (Hz)	16.7	83.3	166.7	8.3	1.7	16.7	16.7
T_c (sec)	0.025	0.005	0.003	0.051	0.25	0.025	0.025

$[0°, 75°]$, respectively. We simulated an $f = 5$ GHz WiFi environment with Rician multipath fading, in which people may be moving between the device and the receiver. Considering a movement speed V_{move} ranging from 0.1 m/sec to 10 m/sec, the maximum Doppler shift f_d is between 16.67 Hz and 166.7 Hz following the formula $f_d = (V_{move}/c)f$. The channel coherence time under Clarke's model, $T_c = 0.423/f_d$, ranges from approximately 0.0254 to 0.00254 sec. Also, the sampling rate F_s is varied between 10 KHz and 1 MHz to test the robustness to different test environments. By varying V_{move} and F_s, 7 different datasets were created to allow testing under different scenarios. Table 1 summarizes the different datasets and their properties. The rationale behind selecting these values is explained in Sec. III-D.

In each authentication sequence, the 4 antennas in a CAA are turned on sequentially to transmit a complex pilot signal. The authenticator receives the in-phase and quadrature (I/Q) samples through multipath fading channels in addition to additive white Gaussian noise:

$$y_{i,t} = h_{i,t} * x_i + w_{i,t} \tag{7}$$

where $x_i = e^{j\psi_i(\theta,\phi)}$ is the transmitted pilot signal from antenna i of CAA k with constant amplitude and the corresponding phase signature $\psi_i(\theta, \phi)$ (array index k is dropped for notational simplicity), $h_{i,t}$ is the multipath fading channel impulse response, $*$ denotes the convolution operation, and $w_{i,t} \sim \mathcal{N}_c(0, \sigma_w^2)$ is the additive white complex Gaussian noise. The impulse response of multipath fading channel can be represented as [25]:

$$h_{i,t} = \sum_{n=0}^{N-1} a_{i,n} e^{j\theta_{i,n}} \delta(t - \tau_{i,n}) \tag{8}$$

where N is number of multipath components, $a_{i,n}e^{j\theta_{i,n}}$ is the complex amplitude of the n-th multipath component for antenna i, which in our channel model follows a Rician distribution, $\tau_{i,n}$ is the propagation delay for the n-th multipath component, and δ is the Dirac delta function.

The I and Q samples are the real and imaginary parts of the received signal $y_{i,t}$. With 4 antenna elements in each array and collecting I and Q samples of the received signal from each antenna, the data used to authenticate a CAA has a size of $N_a \times 8$, where N_a and is the number of instances within an authentication session. In our experiments, we used $N_a = 1,000$. The CAA phase signatures and the received signals through multipath fading channels were simulated using MATLAB's Communications Toolbox. In this simulation, a strong direct path exists between the transmitting antenna and the authenticating receiver, accompanied by scattering in the vicinity of the receiver's position. Given that the distance between the transmitting antenna and the authenticating receiver is significantly larger compared to the scattering area, the angular spread of the departing rays is minimal [26]. Consequently, all propagation paths are assumed to experience approximately the same phase error induced by the CAA. This corresponds to a line-of-sight (LOS) scenario, where the user and authenticator maintain direct visibility, while objects in the vicinity of the receiver introduce additional reflections.

However, in the initial field experiments described in Section III-E we show that the proposed CAA-based authentication system is not restricted to the assumed channel conditions in the simulations with scatterers focused around receiver. In the field experiments, the transmitter and receiver were positioned closer to each other, resulting in stronger scattering effects on the transmitter side and all along the channel. A horn antenna was used at the receiver, where no objects were present in its immediate vicinity. This experimental setup closely resembles the deployments of practical communication systems, where receivers are often installed in environments with minimal surrounding scatterers. As shown in Sections III-D and III-E, our authentication system achieves high performance under different channel conditions with different scatter and fading settings.

We include the naturally occurring signatures, used in traditional RF fingerprinting, by modeling the power amplifier non-linearities [27]–[29]. In the literature, models with or without memory are used. A model with memory using Volterra series is described in [29]. Power amplifier models without memory typically use a Taylor Series model,considering odd or even powers of the signals. A model using odd powers is discussed in [28]. More recently, in [27], the authors used a Taylor series model with even powers, which is the model we incorporate in our experiments:

$$f_{PA}(x_t) = x_t(1 + \psi_0|x_t|^2 + \psi_1|x_t|^4), \tag{9}$$

where x_t is the most recent I/Q sample, and ψ_0, ψ_1 are coefficients unique to each power amplifier. We randomly generate the values of ψ_0 for each antenna array from a Gaussian distribution with mean 0.2 and standard deviation 0.01. Similarly for ψ_1, the mean and standard deviation are 0.15 and 0.01, respectively. The mean and standard deviation values are obtained from [27] and [29], respectively.

Fig. 5 visualizes simulated data from four CAAs. For each CAA, each row shows data received by the authenticator through multipath fading channels in four different sample authentication sessions. The original $1,000 \times 8$ input data is trimmed to an 8×8 image in the figure for better visualization. The eight columns in each authentication session (i.e., image) are the I and Q samples from four antenna elements in the array, as explained earlier in this section. The phase signature $\psi_i(\theta, \phi)$ of each antenna i in an array is clearly seen in the vertical colored pattern within a column in each image. The signatures of all antenna elements in an array (i.e., colorful

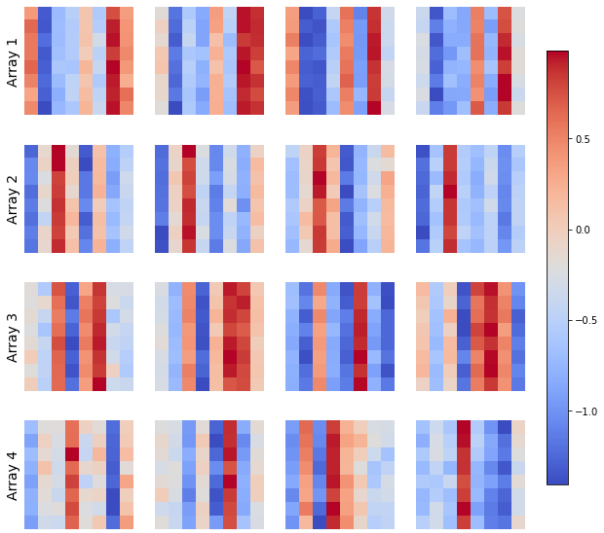

FIGURE 5. Input data to the authentication algorithm visualized as a color map. Each row corresponds to a CAA, and each image represents data received in an authentication session under different channel conditions. The first 8 of the 1,000 instances in an authentication session are shown for clarity. The 8 columns in each image correspond to the I and Q samples from 4 antenna elements in each array. A consistent pattern is observed for each array.

columns in an image) together form the signature of the array within each image. Despite the significant randomness across the four authentication sessions performed at different times due to multipath fading channel noise, one can still observe a signature pattern for each array thanks to the enhanced RF fingerprints of CAAs. For instance, while the second and third columns of Array 1 typically have lower values (represented by blue),its last columns typically have higher values (represented by red). We see such distinct but significantly noisy patterns in each array, which makes deep learning classifiers, in particular Convolutional Neural Networks (CNNs), promising for learning those patterns to accurately authenticate hundreds of CAAs.

Remark 1: As shown in the literature [7], as well as our results in Figs. 6 and 7, even with deep learning classifiers, the naturally occurring phase signatures in traditional RF fingerprinting are not distinct enough to survive the noise of multipath fading channels in realistic scenarios.

Remark 2: Although there is an underlying pattern across the images in each row, it is subject to challenging levels of randomness in different authentication sessions due to multipath fading channels. Such a complex pattern recognition task neccesitates the use of sophisticated deep learning classifiers, which is the topic of next section, instead of simpler statistical detectors.

C. DEEP LEARNING CLASSIFIERS

CNNs are particularly well-suited for capturing the subtle phase differences and distortions in I/Q samples due to their inductive bias towards local spatial structure, which aids in modeling the phase relationships between the signals. The convolutional filters in CNNs can learn spatially correlated patterns within the data, allowing the network to discern the consistent phase shifts that come from the CAAs. Furthermore, CNNs are robust to noise, allowing them to isolate device-specific distortions in signal characteristics, even in the presence of multipath fading channel noise, enhancing the model's capacity to generalize across diverse channel conditions.

To study the effectiveness of ML algorithms for authenticating CAAs, we test a spectrum of CNN based classification models. The baseline model is a simple CNN, consisting of two convolution-max pooling-ReLU layers, followed by a single dense layer (CNN-3). The four other models are described below. The model receives equalized 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.

First, we consider VGG-16 [30], a neural network architecture with 16 layers. This model contains the most parameters out of any model tested ($138M$). We trained VGG-16 from scratch on our data.

Our next model, ResNet-50 [31], introduces residual connections, which effectively mitigates the vanishing gradient problem. This in turn facilitates the training of deeper networks with enhanced accuracy. We selected ResNet-50 for our tests, and considered two different approaches for training. In addition to fully training a randomly initialized version on our data, we also fine-tuned a version that was pretrained on the popular ImageNet-1K dataset.

Following ResNet-50 is InceptionV3 [32], characterized by its "network within a network" architecture, which enables deeper and more efficient feature learning without significantly increasing computational demand. Our InceptionV3 was pretrained on ImageNet-1K before being fine-tuned on our data.

The final model chosen is Xception [33], which incorporates separable convolutional layers alongside residual connections. Xception represents the most cutting-edge model for off-the-shelf CNN-based classification methods. Like ResNet-50, we use both fully trained and fine-tuned (pretrained on ImageNet-1K) versions of Xception.

For all models, except the simple CNN-3 network, we slightly modify the first layer in the model to accept the I/Q samples as input.

Through MATLAB simulations, 110 authentication sequences for 300 CAAs were formed. The data is partitioned using a 100-10 split for training and testing, respectively. We train each model with Adam [34] optimizer, a learning rate of 10^{-5}, decay of 10^{-6}, for 200/500 epochs, depending on the model. Batch size depends on model architecture, and was selected for each model to fill the GPU VRAM. During offline training, the 5 classifiers described above are trained to map the input x_k, $k \in \mathcal{L}$, to probabilities $\{p_i\}$ for each user $i \in \mathcal{L}$, where $\sum p_i = 1$, indicating the probability of the input sequence x_k belonging to user i. The output probability vector

is used to compute the cross-entropy loss:

$$L_{CE} = -\sum_{i=1}^{\mathcal{L}} z_i \log p_i \tag{10}$$

where z_i represents the one-hot-encoded ground truth, taking the value 0 for every user in $\mathcal{L}$ except the user which transmitted the data. The resulting loss is back-propagated using Adam to optimize the network parameters over the training process. For inference, we declare the transmitting device to be $\hat{i}$ for which p_i is maximized:

$$\hat{i} = \arg\max_i p_i \tag{11}$$

The overall accuracy over the test set is defined as the sum of correct classifications divided by the number of test instances.

All models mentioned are implemented using PyTorch. The experiments were conducted using an RTX 4090 GPU with 24GB of VRAM. The training time for each network depends on the architecture, number of trainable parameters, batch size, and processing power.

The selection of classifiers was informed by each model's differing structural advantages, to provide a wide range of comparisons on the unique challenges presented by I/Q signal data classification. VGG-16 has a straightforward, densely connected structure, providing a baseline to determine if more complex architectures are necessary for acceptable performance on this data type. ResNet-50, InceptionV3, and Xception, in contrast, have advanced architectures, each designed to mitigate the vanishing gradient issue in different ways. These models thus facilitate deeper learning of features which we hope to see improve authentication performance under unideal channel conditions.

D. RESULTS

Table 2 shows the test classification accuracy for each of the networks trained and tested on each dataset mentioned in Section III-B. For 5 out of the 7 datasets, all models, including the baseline CNN-3, score significantly above the 63% state-of-the-art accuracy in the literature achieved by ResNet-50 using the traditional (non-CAA) RF fingerprints [7] in a similar setup. The performance drop in sets 5 and 6 are analyzed in detail in the following paragraphs. Comparing the performance between the fully trained and fine-tuned versions of the models, we notice no significant difference in accuracy. This indicates that pretraining on large image datasets is not necessary for RF fingerprinting. Thorough training on the I/Q data itself is sufficient to provide optimal performance under these circumstances.

It is seen in Table 2 that the classification accuracy depends heavily on the ratio between the channel coherence time T_c and authentication duration $T_a = N_a/F_s$, reported as a subscript in the column headings, where $N_a = 1,000$ is the number of samples in an authentication sequence and F_s is the sampling frequency. In sets 1, 2, 3, we initially increase $V_{move} \in \{1, 5, 10\}$ m/s while keeping the sampling frequency fixed at $F_s = 10$ kHz to study faster

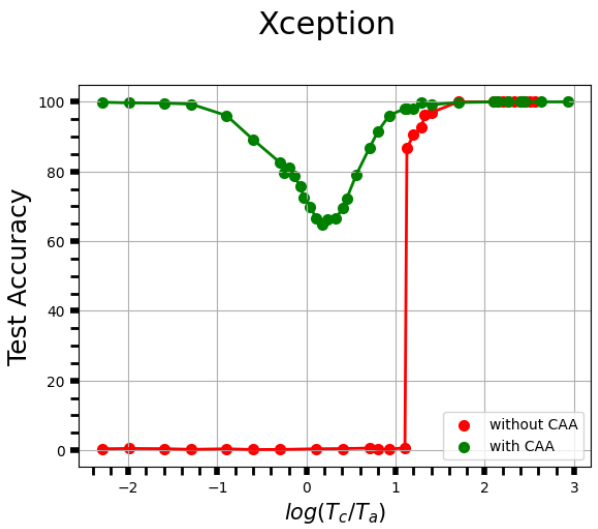

FIGURE 6. Test set classification accuracy of pretrained Xception when sweeping T_c/T_a at $SNR = 20dB$. Smaller/larger T_c/T_a values correspond to faster/slower fading channels. While the traditional RF signatures without CAA only work in scenarios where the channel varies slowly with respect to the authentication frequency, the proposed enhanced RF signatures with CAA enable accurate authentication in both fast and slow-fading channels with a caveat of performance drop in a mid-range band where the channel's fading pattern overlaps and causes interference with the authentication pattern ($T_c/T_a \approx 1$).

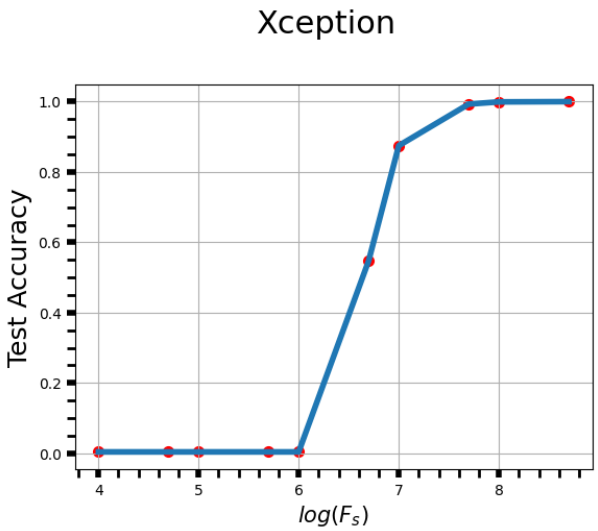

FIGURE 7. Authentication accuracy of pretrained Xception on traditional RF signatures without CAA generated by the power amplifier model in equation (9). Movement speed in the channel is set at $V_{move} = 20$ m/s. Successful authentication is observed at sampling rates close to 100 MHz.

TABLE 2. Test accuracy on data generated with CAA for SNR = 20 dB. Sets are represented with $(F_s, V_{move})_{T_c/T_a}$, where T_c and T_a denote the channel coherence time and authentication duration.

Model \ Set	$(10K,1)_{0.25}$	$(10K,5)_{0.05}$	$(10K,10)_{0.025}$	$(10K,0.5)_{0.50}$	$(10K,0.1)_{2.53}$	$(100K,1)_{2.53}$	$(1M,1)_{25.36}$
CNN-3	82.09	96.51	98.69	72.06	47.27	44.24	91.66
VGG-16	83.30	95.87	97.03	81.78	59.36	56.45	98.36
ResNet-50	89.87	99.00	98.87	74.06	57.42	55.81	98.57
Xception	**90.78**	99.00	**100.00**	85.24	58.06	53.33	97.90
ResNet-50 (Pretrained)	90.03	**99.42**	99.90	**86.42**	**68.57**	**72.42**	**99.96**
InceptionV3 (Pretrained)	90.00	99.15	99.96	84.78	51.18	50.09	97.03
Xception (Pretrained)	88.18	99.24	99.81	81.96	66.33	70.66	99.90

TABLE 3. Test accuracy on data generated with CAA for different SNR values for ResNet-50 model. Sets are represented with $(F_s, V_{move})_{T_c/T_a}$, where T_c and T_a denote the channel coherence time and authentication duration.

SNR \ Set	$(10K,1)_{0.25}$	$(10K,5)_{0.05}$	$(10K,10)_{0.025}$	$(10K,0.5)_{0.50}$	$(10K,0.1)_{2.53}$	$(100K,1)_{2.53}$	$(1M,1)_{25.36}$
-30 dB	68.75	85.30	90.57	61.33	45.27	45.48	70.42
-25 dB	64.93	86.57	89.66	62.63	46.84	46.09	72.06
-20 dB	71.06	82.21	90.45	63.33	45.63	47.15	69.42
-15 dB	77.09	84.36	87.78	62.30	49.24	44.60	69.78
-10 dB	86.75	95.15	95.21	72.15	53.96	54.48	88.45
-5 dB	85.45	96.66	97.93	76.42	58.72	57.18	97.39
0 dB	89.84	97.96	99.60	81.96	62.81	56.63	99.09
5 dB	88.18	98.09	98.81	80.72	65.27	63.57	98.60
10 dB	90.30	98.21	98.78	85.39	67.09	62.90	99.72
15 dB	89.93	98.96	99.48	83.96	65.60	62.48	99.24
20 dB	90.03	**99.42**	**99.90**	**86.42**	**68.57**	**64.96**	**99.96**
25 dB	**90.66**	98.33	99.18	85.45	66.66	64.33	99.12
30 dB	90.33	98.72	99.33	85.51	62.96	63.36	99.33

TABLE 4. Test accuracy on data generated without CAA (regular antenna arrays with only power amplifier signatures) for SNR = 20 dB. Sets are represented with $(F_s, V_{move})_{T_c/T_a}$, where T_c and T_a denote the channel coherence time and authentication duration.

Model \ Set	$(10K,1)_{0.25}$	$(10K,5)_{0.05}$	$(10K,10)_{0.025}$	$(10K,0.5)_{0.50}$	$(10K,0.1)_{2.53}$	$(100K,1)_{2.53}$	$(1M,1)_{25.36}$
CNN-3	0.27	0.27	0.33	0.27	0.48	0.69	35.33
VGG-16	0.21	0.18	0.24	**0.42**	0.09	0.30	62.45
ResNet-50	0.18	0.30	0.21	0.27	**1.45**	**1.72**	95.12
ResNet-50 (Pretrained)	**0.39**	0.21	**0.36**	0.39	0.90	**1.72**	**95.80**
Xception (Pretrained)	0.12	**0.24**	0.21	0.24	0.18	0.18	84.06

fading channels. In those scenarios, the channel coherence time $T_c \in \{0.025, 0.005, 0.003\}$ sec and the $T_c/T_a \in \{0.25, 0.05, 0.025\}$ ratio both decrease, i.e., more random channel realizations are observed during an authentication sequence. Although counterintuitive, the performance of all five methods increase as the wireless channel becomes more challenging. To complete the picture, we also investigate slower fading channels by decreasing $V_{move} \in \{0.5, 0.1\}$ m/s in sets 4 and 5 compared to set 1. In these scenarios, the channel coherence time $T_c \in \{0.05, 0.25\}$ and the $T_c/T_a \in \{0.5, 2.53\}$ ratio both increase. Interestingly, the performance drops across all algorithms while the channel becomes less challenging (elaborated in Remark 3). We also increase the sampling frequency $F_s \in \{100K, 1M\}$ Hz in sets 6 and 7 while keeping V_{move} constant to further study the increasing T_c/T_a ratio (even less channel randomness in an authentication sequence). As T_c/T_a increases to 25.36, the performance of all algorithms again climb above 90% accuracy, reaching up to 99.9%.

Remark 3: It is observed that the performance drop, demonstrated by the green curve in Fig. 6 for Xception, happens in a band of scenarios in which the T_c/T_a ratio is around unity. In those cases, the authentication duration and channel coherence time are comparable, meaning that during each authentication sequence the channel is renewed. Coherence time denotes the duration in which the channel's effect on the transmitted signal becomes uncorrelated. When the channel coherence time and authentication duration coincide, there is another pattern, the channel's fading cycle, that is overlaid on top of the authentication signature. As the channel's fading pattern collides with the authentication pattern, destructive interference occurs between the two, causing a performance drop for classification algorithms.

To measure the robustness of CAA-based authentication to

noise, we tested the performance of pretrained ResNet-50 for various values of Signal-to-Noise Ratio (SNR) ranging from -30 dB to 30 dB. The results are summarized in Table 3. We see that the phase-based signatures introduced by CAA are very resilient to high levels of noise.

CAA vs. Traditional RF Fingerprinting: Next, to evaluate the contribution of CAA signatures, we generated additional datasets for regular non-CAA antenna arrays using only the power amplifier model in Eq. (9) under the same 7 scenarios of (F_s, V_{move}) values as in the previous experiment for CAAs. The results in Table 4 show that without CAAs, the models perform extremely poorly on all datasets, except dataset 7, in which the channel is almost static within the authentication sequence. To analyze this trend in detail, we generated more scenarios for regular antenna arrays with different combinations of moving speed and sampling frequency. As the results in Table 5 show, highly accurate authentication with regular antenna arrays is only possible under idealistic scenarios where the channel does not change significantly during the authentication process, i.e., channel coherence time is much longer than the authentication duration. This fact is demonstrated by the red-colored curve in Fig. 6. It is seen in Fig. 6 that under fading channels ($\log(T_c/T_a) < 1$), traditional RF fingerprinting signatures without CAAs are not sufficient to be reliable, while the enhanced RF signatures of CAAs enable high accuracy across fast and slow-fading channels, with a caveat of some performance drop in a mid-range band where the channel's fading pattern overlaps and causes interference with the authentication pattern ($T_c/T_a \approx 1$). Even in that case, the performance of CAAs does not drop below 65% accuracy. Note that such a potential performance drop can be easily avoided with rough knowledge of the channel condition by selecting the sampling frequency (e.g., downsampling in software) small enough to ensure a relatively fast-fading channel (lower T_c/T_a values in Fig. 6). This is a remarkable feature of CAA, as non-CAA RF signatures do not yield acceptable results under fast-fading channels.

Since it is shown that the authentication performance depends on the ratio between channel coherence time and authentication duration, it seems possible to deal with the fast-fading even with traditional antenna arrays without CAAs by increasing the sampling frequency. To verify, we conduct further experiments on traditional RF fingerprints by keeping V_{move} constant at 20m/s (typical vehicle speed) and varying sampling frequency. From the results shown in Table 6 and Fig. 7, it is observed that highly accurate authentication is possible when the sampling frequency approaches 100 MHz. At sufficiently high sampling rates for a given fast-fading channel, the channel is practically static, allowing the weak signatures introduced by the amplifiers to be picked up by the classifier. In contrast, at lower sampling frequency values, the channel is varying, and thus the signatures introduced by the power the amplifier alone are not enough for reliable authentication. However, in practice, implementing a receiver with such high sampling rates is more costly and complex compared to a receiver with a lower sampling rate.

In general, power consumption and circuit complexity in ADCs increase with increasing sampling frequency. This means the cost of ADCs increases with higher sampling frequency, as observed for the figure of merit P vs Cost graph in [35]. The theoretical lower bound for sampling power is discussed in [36]. This bound is known to be directly proportional to the sampling frequency. Extrapolating the power consumption graph shown in [37], it can be seen that for 10 KHz sampling frequency the power consumption is in the μW range, while for 100 MHz is in the mW range. The actual power consumption depends on the ADC type and other design factors, but in general increases with increasing sampling frequency, as observed from experimental data collected in [38]. Another consideration when designing ADCs is the complexity of the ADC circuit as sampling frequency increases. In [35], in a design of Sigma-Delta ADC, the increase in filter order is discussed as sampling frequency increases. Specifically, for 10 MHz sampling frequency, the filter order could be as high as 5,000. In [39], the authors discuss the increased difficulty in implementing high sampling rate ADCs due to mismatches in sampling speeds of different sampling circuits, leading to the need of larger sized devices which in turn lead to parasitic capacitances.

The CAA-enabled authentication system thus gives a considerable advantage over traditional RF-based fingerprinting in terms of power consumption and circuit complexity, resulting in cost savings in a practically feasible implementation, which is elaborated in Section IV.

Wireless Channel Impact: To analyze the impact of the Rician channel on the phase of the transmitted signal, we plot and compare the phase of the input signal and the output signal after passing through the Rician channel. The analysis is conducted for the first antennas of four CAAs, with a fixed position chosen for each array, consistent with the simulation setup. The phase plot of the input signal is depicted in Fig. 8, while the phase plot of the output signals for various walking speeds are shown in shown in Figs. 9, 10, and 11. The input data sequence consists of all ones, and the memoryless nonlinearity effects of the amplifier are incorporated into the input data phase. Additionally, the phase contributions from the CAA position and feed line randomization are included. Since the array position remains fixed, the phase contribution from the CAA remains constant throughout the transmission for a single array. Consequently, distinct but constant phase values for each array are observed in Fig. 8. The signal is then transmitted through a Rician channel, with the Doppler shift determined by walking speed. Higher walking speeds correspond to more dynamic channels, resulting in faster fading. Two walking speeds, 1 m/s and 10 m/s, are considered to demonstrate the effects of slow and fast-fading channels, respectively. At a walking speed of 0 m/s, zero Doppler spread is observed, and the phase variations are solely due to AWGN, as illustrated in Fig. 9. In the case of a slow-fading channel with additive white Gaussian noise (AWGN), as shown in Fig. 10, a walking speed of 1 m/s and a sampling rate of 10 kHz result in the received signal phase remaining approximately

TABLE 5. Test accuracy on data generated without CAA (regular antenna arrays with only power amplifier signatures) for SNR = 20 dB increases as the channel becomes static. Sets are represented with $(F_s, V_{move})_{T_c/T_a}$, where T_c and T_a denote the channel coherence time and authentication duration.

Model \ Set	$(200K,1)_{5.07}$	$(400K,1)_{10.14}$	$(10K,0.01)_{25.36}$	$(1.4M,1)_{35.50}$	$(1.8M,1)_{45.65}$	$(10K,0.001)_{253.62}$	$(100K,0.001)_{2536.24}$
CNN-3	2.6	6.48	32.72	53.66	63.89	**100**	**100**
VGG-16	0.21	0.24	39.72	70.42	91.18	84.75	99.78
ResNet-50	14.96	64.27	93.6	97.9	98.63	**100**	**100**
ResNet-50 (Pretrained)	**44.81**	**82.3**	**99.42**	98.36	**98.84**	**100**	**100**
Xception (Pretrained)	36.51	66.24	98.57	**99.33**	98.81	**100**	**100**

TABLE 6. Test accuracy on data generated without CAA (regular antenna arrays with only power amplifier signatures) for SNR = 20 dB increases with higher sampling rates. Sets are represented with $(F_s, V_{move})_{T_c/T_a}$, where T_c and T_a denote the channel coherence time and authentication duration.

Model \ Set	$(10K,20)_{0.0126}$	$(100K,20)_{0.1268}$	$(1M,20)_{1.268}$	$(10M,20)_{12.68}$	$(100M,20)_{126.81}$
CNN-3	0.18	0.33	0.21	10.03	99.73
VGG-16	0.21	0.18	0.21	0.30	98.81
ResNet-50	**0.39**	**0.45**	**0.36**	83.00	99.24
ResNet-50 (Pretrained)	**0.39**	**0.45**	0.30	**90.87**	**100**
Xception (Pretrained)	**0.39**	0.18	0.21	86.39	**100**

TABLE 7. Model parameters, computational complexity, and inference speed (Authentications per Second - APS) for each model.

Model	Params (M)	GFLOPs	APS
CNN-3	2.4	0.0012	2430.4
VGG-16	139.0	15.5	437.5
ResNet-50	26.2	1.25	109.5
Xception	23.5	1.24	116.3
InceptionV3	27.8	0.35	60.7

constant over longer time intervals before changing. For the fast-fading channel scenario, the walking speed is increased to 10 m/s while maintaining the 10 kHz sampling rate. In this fast-fading scenario, the channel becomes highly dynamic, with phase values fluctuating significantly over short time intervals, as shown in Fig. 11. This corresponds to a much shorter channel coherence time compared to the slow-fading case. Phase plots effectively illustrate the behavior of the received signal under realistic slow and fast-fading conditions, consistent with theoretical expectations. Presented work shows that these challenging phase signatures under realistic channel conditions can be detected by ML algorithms with high accuracy.

Computational Complexity: *Table* 7 compares the model paramters, computational complexity, and inference speed (measured as Authentications per Second - APS) for the deep learning models used in this study. All models were tested on an Nvidia RTX 4090 GPU. The baseline CNN-3 model is the most lightweight by far, with 2.4 million parameters and 0.0012 GFLOPs, resulting in 2430 APS. This makes it extremely efficient for scenarios with many devices, but as shown in this section, lacks the accuracy of other methods. VGG-16, ResNet-50, Xception, and InceptionV3 each offer different trade-offs between complexity, size, and speed. ResNet-50 and Xception have similar GFLOPs values (1.25 and 1.24, respectively), yet Xception outperforms ResNet-50 in terms of APS, with 116 vs 109, likely due to Xception's factorized convolutions which optimize computation. InceptionV3, with 27.8 million parameters, has much lower GFLOPs complexity than other other advanced methods yet barely passes 60 APS, indicating that some other bottleneck

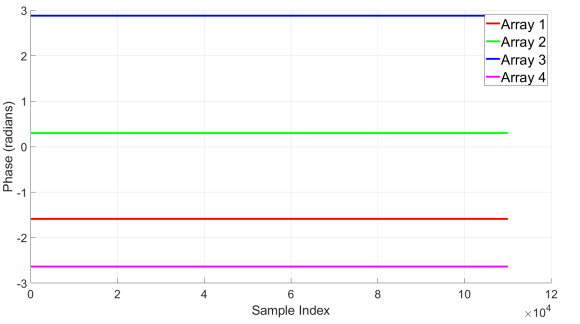

FIGURE 8. Phase of an input signal plotted after adding phase terms due to memoryless non-linearities in addition to CAA at a fixed position for each of the first antenna of the first four arrays.

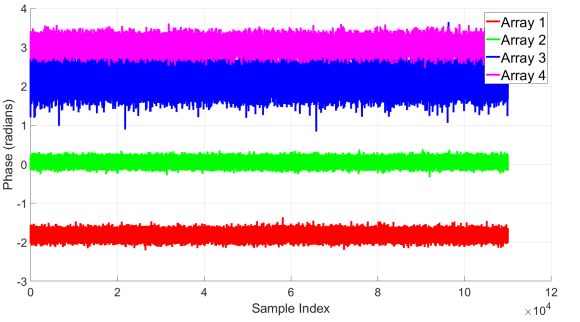

FIGURE 9. Phase of a received signal for a walking speed of 0 m/s and sampling frequency of 10 KHz, corresponding to static channel with only AWGN added.

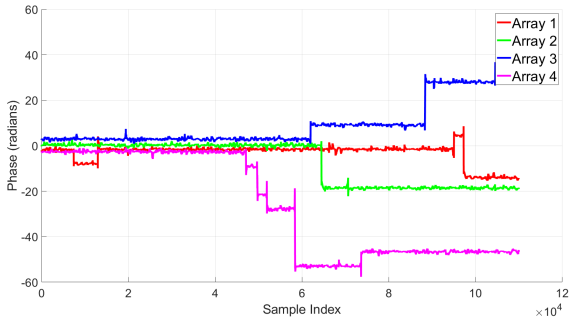

FIGURE 10. Phase of a received signal for a walking speed of 1 m/s and sampling frequency of 10 KHz, corresponding to slow-fading scenario.

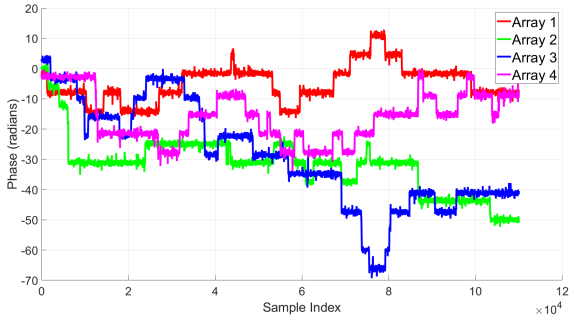

FIGURE 11. Phase of a received signal for a walking speed of 10 m/s and sampling frequency of 10 KHz, corresponding to fast-fading scenario.

exists for this model, likely memory speed and number of sequential operations. VGG16, on the other hand, has vastly more parameters and GFLOPs compared to the other models selected (139 million parameters and 15.5 GFLOPs), but at the same time, vastly outperforms them on APS, with 437.5. This is due to VGG16's highly parallelizable design, allowing the GPU to very quickly infer from the input data.

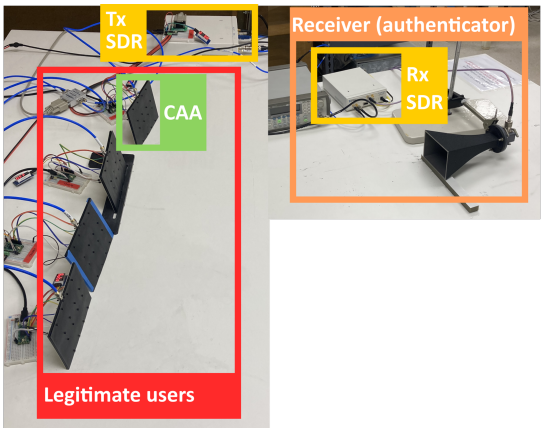

FIGURE 12. Testbed setup with the CAAs shown on the left and Authenticating Receiver shown on right.

E. EXPERIMENTAL VERIFICATION

To evaluate the performance of the CAA-based authentication system using real-world data rather than synthetically generated data, we are developing a testbed in our laboratory. As shown in Fig. 12, the testbed includes software defined radios (SDRs), CAAs manufactured in our laboratory, necessary control electronics to turn on/off antenna elements of the CAAs, software for controlling the testbed and data collection. Full verification of the CAA based authentication technique presented in this manuscript, particularly the training/authentication demonstrations involving spatially variant fingerprints of the CAAs, involve many sets of systematic data collections that are currently being investigated. In addition, systematic data collection under different wireless channel conditions is planned using the testbed. Consequently, the details of the testbed (hardware design and manufacturing, hardware characterization, SDR programming, wireless channel scenarios, description of data sets and their collection conditions such as the CAA positions) and comprehensive experimental verifications of CAA based authentication will be reported in a future work.

The first set of experiments performed with this testbed have the CAAs at fixed positions during the data collection. The testbed utilizes four CAAs, each comprising four antenna elements arranged linearly with randomized positions and feed line lengths. Although our simulations modeled a square array in this manuscript, this difference is negligible since the angle-dependent signature exists both in square or linear array arrangements. A horn antenna is connected to an Ettus USRP X440 SDR, which serves as the receiver. Data was gathered by sequentially activating each antenna element in a cyclic manner. The data format matched that of the synthetic data, allowing seamless input into our model without modification. A total of 110 samples, each containing 1000 sequences were collected, to match the simulations in number. To ensure consistency with the Rician channel model used in the simulations, a direct line-of-sight path was maintained between the CAAs and the receiver. However, the scattering objects in the environment are spread around the room, including the vicinity of transmitters, as opposed to the channel environment in the simulations in the previous section. This experimental setup let us show that the proposed authentication system is not restricted to the considered simulation environment with focused scatterers around the receiver using the MATLAB Communications Toolbox.

The performance results of the real-world data, processed using the same models as for synthetic data, are presented in Table 8. The table demonstrates that the CAA system performs exceptionally well in field experiments, achieving 100% accuracy in three out of the four tested models. The experiments were conducted in a dynamic lab environment, with people walking in the background and nearby reflective surfaces to account for multipath effects and the presence of external interference sources, such as Wi-Fi signals.

Initial datasets collected with each CAA transmitting in multiple different positions are also showing strong per-

TABLE 8. Test accuracy on field experiment data with linear CAA and fixed array positions.

Model	Test Accuracy (%)
CNN-3	98.86
ResNet-50	100
Xception	100
Inception(Pretrained)	100

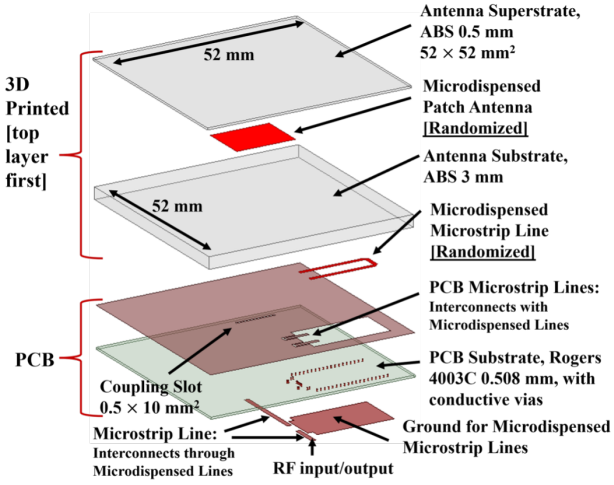

FIGURE 13. Substrate stack-up of the aperture-coupled patch antenna designed for the practical realization of CAAs.

formance with accuracy approaching 98% with ResNet-50. However, as stated, we must significantly expand the data sets by performing many systematic characterizations. Hence, we plan to report the details of the testbed and a comprehensive set of experiments conducted with it in a future work to better assess the performance of CAA-based authentication in increasingly realistic scenarios.

IV. PRACTICAL REALIZATION OF CAA ELEMENTS USING ADDITIVE MANUFACTURING

Randomization in antenna positions and feed line lengths can be carried out with traditional manufacturing technologies; however, this is expected to be costly since low-cost is only achieved by replication of identical circuits. To enable cost effectiveness, we investigate practical realization of the CAAs using additive manufacturing (AM). AM is mask-free and can form a 3D structure layer by layer. Hence, randomization of geometry can be carried out with no additional cost by randomizing the printing files and/or the motions and materials of the manufacturing heads. Recent research work has already demonstrated that laser enhanced direct print additive manufacturing (LE-DPAM) can be employed to realize multilayered patch antennas [40], [41], structurally embedded ICs [42], and packaging of ICs with antennas [43] up to mm-wave frequencies, with performances comparable to those attainable from conventional manufacturing.

Fig. 13 presents the 3D structure of the antenna element proposed for practical CAA realizations. Although LE-DPAM can manufacture the entirety of the shown structure, a hybrid assembly is proposed to combine the best of two manufacturing techniques (i.e., low-cost and rapid production of detailed but identical geometries with PCB vs. low-cost manufacturing of randomized geometries with LE-DPAM). To minimize the area of conductive traces manufactured with LE-DPAM (for faster manufacturing speed), an aperture-coupled patch antenna is considered. The LE-DPAM (i.e. 3D-printed) part consists of four material layers. Two of these are dielectric acrylonitrile butadiene styrene (ABS) layers ($\epsilon_r = 2.6$, $\tan\delta = 0.0085$) that are manufactured by the Fused Deposition Modeling (FDM) capability of LE-DPAM. The remaining two layers are formed from CB028 conductive paste ($\sigma = 1 \times 10^6$ S/m) by using the microdispensing capability of LE-DPAM. Laser processing or micro-milling the edges of the conductive traces are likely not needed for the shown conductive layers (i.e., antenna and microstrip line) due to the larger dimensions for operation at the 5.8 GHz ISM band. The 3D-printed part is designed to be manufactured on the LE-DPAM platform in an upside-down manner (as in [40]). First, the 0.5 mm ABS is printed using FDM to form the material base. This layer also acts as a cover to hide the antenna element from visual inspection. The process follows with microdispensing of conductive paste to form the patch. Subsequently, the 3 mm thick ABS material is printed using FDM. This layer acts as the antenna substrate and mainly controls the antenna bandwidth. Finally, the microstrip line is microdispensed to complete the production of the 3D-printed structure. Antenna position (relative to the coupling slot) and microstrip line lengths are randomized geometry parameters.

The 3D-printed structure will be screwed (or glued/bonded) on to the PCB as illustrated with the substrate stack-up shown in Fig. 13. The PCB is a 0.508 mm thick Rogers 4003C substrate layer ($\epsilon_r = 3.55$, $\tan\delta = 0.0027$) with two layers of conductive traces. One layer carries the RF and antenna ground plane with the antenna coupling slot and a larger cutout area for preventing the overlap with the microdispensed microstrip lines. Inside the cutout area, two very short microstrip lines are included as pads to overlap with the tips of the microdispensed microstrip line when the entire structure is assembled. The second layer carries the RF microstrip feed line that enters the PCB and extends over the coupling slot to feed the antenna element. In addition, this layer carries a rectangular-shaped trace to act as the ground plane of the microdispensed microstrip line. This trace is connected to the main ground using a set of 0.3 mm diameter conductive vias to prevent undesired radiation. Two 0.6 mm diameter conductive vias are used to connect the RF microstrip line with the microstrip line pads on the opposite side of the board. After entering the board from the first conductive layer (i.e., the bottom layer in Fig. 13), the RF signal travels to the second conductive layer, passes over a randomized microdispensed microstrip line, and travels back to the first conductive layer to feed the antenna element through a coupling slot.

Fig. 14 presents the layout of the aperture-coupled patch

IEEE Access

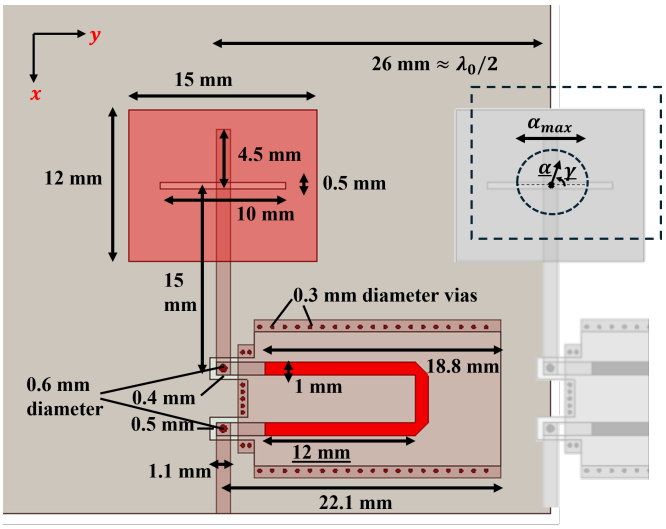

FIGURE 14. Layout details of the CAA element in Fig. 13. Dimensions that are randomized (feed line length, and antenna location) are underlined.

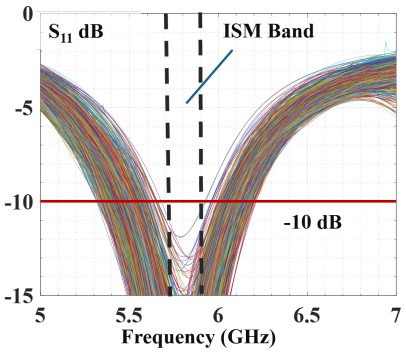

FIGURE 15. $|S_{11}|$ performance of 1200 antenna elements as their geometry is randomized.

antenna. Although patch dimensions can be randomized to create differences in cross polarization and phase delay, they are left constant in this study. An important aspect of the design is the choice of a relatively thick 3 mm antenna substrate. Since impedance matching aperture-coupled patch antennas is sensitive to the coupling slot position and its dimensions, the thick antenna substrate is utilized to obtain a wideband operation when the antenna element is centered over the coupling slot as shown in Fig. 14. The relative position of the patch with respect to the coupling slot is randomized as described in Section II ($\alpha_{max} = 4$ mm). This results in a frequency shift in the antenna element, but the antenna remains impedance matched due to its wideband characteristics. The microdispensed feed line is bent to fit more line length within the half-wavelength space of an antenna array, as shown in Fig. 14. Each bent section can assume a length between 2.5 mm and 16.5 mm. Considering the 2.5 mm length as the reference state, the total microdispensed line length can be randomly enlarged from 0 mm to 28 mm, where the latter corresponds to a $\approx 360^\circ$ phase shift within the shown substrate stack-up. 2.5 mm is the length allocated for the overlap with the pads of the feed line on the PCB. This contact-based electrical connection can be further strengthened with the application of silver epoxy. It is also important to note that the feed line width is 1.1 mm for the bottom conductive trace of the PCB since the trace is modeled to be open to air whereas the microdispensed line is an embedded line.

The Ansys Electronics Desktop (EDT) HFSS simulation of the antenna element (with the shown 52×52 mm^2 cross section, but with a short 6.5 mm feed line) shows that the unperturbed antenna operates with 9.4% $|S_{11}| < -10$ dB at the center frequency of 5.75 GHz. The realized gain is 6.7 dBi at 5.8 GHz, corresponding to a radiation efficiency of 93%. A MATLAB m-file was written to create a script that automates Ansys EDT HFSS to simulate antenna elements with randomized locations and feed line lengths. The script is also capable of exporting the parameters of interest and repeating the process over the desired number of antenna realizations. Both geometry randomizations are based on a uniform distribution, as discussed in Section II. Fig. 15 shows the $|S_{11}|$ (dB) (i.e., port reflection coefficient) performance of the 1200 antenna elements automatically simulated with the MATLAB – Ansys EDT HFSS framework. Resonance frequency shifts are notably visible due to displacement of the antenna element over the coupling slot.

However, it is important to note that the CAA concept is not limited to the aperture-coupled patch antenna design presented in this study. Alternative antenna configurations, such as probe-fed patch antennas, could minimize or eliminate frequency shifts. For example, prior work [9], [11], [44] has demonstrated the feasibility of implementing vertical interconnects in 3D-printed substrates using conductive ink-filled vias, which could support such designs. While these approaches are effective, they involve additional manufacturing steps that may extend the production time and we prefer to avoid in our initial prototypes. The aperture-coupled patch antennas are specifically designed with a much broader bandwidth than the intended communication band, ensuring that the expected resonance frequency shifts not change the fact that the antennas remain well-matched with $|S_{11}| < 10$ dB, allowing for over 90% power acceptance. The presented study validates this fact with all 1200 antenna instances maintaining a lower than -10 dB $|S_{11}|$ across the 5.8 GHz ISM band. Comprehensive manufacturing details, their usage within test nodes and testbeds employing software defined radios will be the subject of a future study. Additionally, future work will explore alternative antenna designs to further mitigate resonance frequency shifts and enhance compatibility with specific wireless standards.

Wireless Communications with CAAs: The randomized antenna positions in the CAA share similarities with non-uniform antenna arrays, such as thinned or sparse arrays that have been explored extensively in the literature. For a system that can be designed to make CAAs perform beamforming by relying on analog phase shifters behind each antenna element, we restricted the average spacing among the antenna elements

to half-wavelengths and avoided the issues of grating lobes. Moreover, the magnitude of the vector used to randomize the positions of the antennas were restricted to keep mutual coupling among the antennas low. Under scenarios when the randomizations are not known by the user of the CAA, pilot signal training sequences can be employed to perform analog beamforming as demonstrated in our recent work [45]. While pilot signal adds an extra step for point-to-point communications, the process aligns well with the training requirements when the analog beamforming arrays are operated within scattering or non-line-of-sight environments. It is important to note that the CAA concept can also be employed within systems that will perform fully digital beamforming, where the digital system can optimize the transmission coefficients from the CAAs to achieve the best data rates. Consequently, CAA concept can support both authentication and communication functionalities, most likely without compromising wireless communication system performance. Future work will also focus on the utilization of CAAs during wireless communications, while investigating their data rates along with their potential for hindering eavesdropper success capabilities.

V. CONCLUSION

A novel machine learning (ML) based wireless device authentication concept based on enhanced RF fingerprinting through the utilization of chaotic antenna arrays (CAAs) was investigated. A range of neural network architectures were trained on several wireless channel scenarios with varying fast- and slow-fading conditions. The authentication performances of these trained models were shown to be promising for advancement of the state-of-the-art in RF fingerprinting-based authentication, with even simpler neural networks performing extremely well. It is also seen that more advanced networks achieve perfect accuracy under a variety of scenarios. Relative performance degradation under scenarios where channel coherence time nears sample duration suggests that the sampling rate of the authenticator should be set according to the channel statistics to avoid possible interference from channel patterns. The results as they stand, however, indicate that enhanced fingerprints offered by CAAs nevertheless allow for highly accurate RF fingerprint authentication. More specifically, the results of deep learning-based authentication utilizing CAA-based RF fingerprints were shown to be significantly outperforming the existing state-of-the-art results based on traditional RF fingerprints found in all wireless communication devices. While the weak signatures used in traditional RF fingerprinting are only useful under idealistic conditions where the channel is static during authentication, the enhanced RF signatures of CAAs enable highly accurate authentication under realistic fast-fading wireless channel scenarios. Moreover, we showed that the randomized antenna locations in CAAs result in a direction-dependent signature, which can provide extra security against RF signature capturing attacks, which are known to threaten traditional RF fingerprinting. We also presented a mathematical model of the CAA's electric field and explained how CAAs can be realized using practical manufacturing techniques. The authenticator is assumed to be in the far-field of the transmitters. Although the antenna shapes could also be randomized, we considered only location randomization in this work for mathematical tractability. A future research direction is to expand the preliminary experimental study with the testbed for a comprehensive empirical analysis of the proposed CAA-based authentication system.

ACKNOWLEDGMENT

The authors express their sincere gratitude to Thomas Ranstrom and Omar Jebreil from the Department of Electrical Engineering at the University of South Florida for their collaboration in conducting the initial set of field experiment reported in this manuscript through the development of a testbed and manufacturing of the CAAs. The authors also acknowledge Thomas Ranstrom for his insightful guidance on key system design considerations related to the wireless communication channel which significantly contributed to enhancing the quality and robustness of this work.

REFERENCES

[1] A. Barenghi, L. Breveglieri, I. Koren, and D. Naccache, "Fault Injection Attacks on Cryptographic Devices: Theory, Practice, and Countermeasures," *Proceedings of the IEEE*, vol. 100, pp. 3056–3076, 2012.
[2] K. Ardis, "How Physically Unclonable Function (PUF) Technology Protects Embedded Systems," https://www.maximintegrated.com/en/design/technical-documents/white-papers/7/7218.html, Jul. 2020.
[3] P. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," in *Proceedings 35th Annual Symposium on Foundations of Computer Science*, 1994, pp. 124–134.
[4] G. E. Suh and S. Devadas, "Physical unclonable functions for device authentication and secret key generation," in *2007 44th ACM/IEEE Design Automation Conference*, 2007, pp. 9–14.
[5] 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.
[6] 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. [Online]. Available: https://arxiv.org/abs/2201.00680
[7] T. Jian, B. C. Rendon, E. Ojuba, N. Soltani, Z. Wang, K. Sankhe, A. Gritsenko, J. Dy, K. Chowdhury, and S. Ioannidis, "Deep learning for rf fingerprinting: A massive experimental study," *IEEE Internet of Things Magazine*, vol. 3, no. 1, pp. 50–57, 2020.
[8] J. McMillen, G. Mumcu, and Y. Yilmaz, "Deep learning-based rf fingerprint authentication with chaotic antenna arrays," in *2023 IEEE Wireless and Microwave Technology Conference (WAMICON)*, 2023, pp. 121–124.
[9] M. Kacar, J. Wang, G. Mumcu, C. Perkowski, K. Church, B.-I. Wu, and T. Weller, "Phased array antenna element with embedded cavity and mmic using direct digital manufacturing," in *2019 IEEE International Symposium on Antennas and Propagation and USNC-URSI Radio Science Meeting*, 2019, pp. 81–82.
[10] 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.
[11] 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.
[12] 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.

[13] 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.
[14] O. Gungor and C. E. Koksal, "On the basic limits of rf-fingerprint-based authentication," *IEEE transactions on information theory*, vol. 62, no. 8, pp. 4523–4543, 2016.
[15] C. A. Balanis, *Antenna theory: analysis and design*. Wiley-Interscience, 2005.
[16] 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.
[17] R. W. Klein, M. A. Temple, and M. J. Mendenhall, "Application of wavelet-based rf fingerprinting to enhance wireless network security," *Journal of Communications and Networks*, vol. 11, no. 6, pp. 544–555, 2009.
[18] C. Bertoncini, K. Rudd, B. Nousain, and M. Hinders, "Wavelet fingerprinting of radio-frequency identification (rfid) tags," *IEEE Transactions on Industrial Electronics*, vol. 59, no. 12, pp. 4843–4850, 2011.
[19] M. Ezuma, F. Erden, C. K. Anjinappa, O. Ozdemir, and I. Guvenc, "Micro-uav detection and classification from rf fingerprints using machine learning techniques," in *2019 IEEE Aerospace Conference*. IEEE, 2019, pp. 1–13.
[20] B. Danev, T. S. Heydt-Benjamin, and S. Capkun, "Physical-layer identification of rfid devices." in *USENIX security symposium*, 2009, pp. 199–214.
[21] 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). [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1877050917303678
[22] 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.
[23] 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.
[24] NIST Computer Security Resource Center, "Verifier impersonation attack," https://csrc.nist.gov/glossary/term/verifier_impersonation_attack, accessed: 2022-05-25.
[25] A. Tkac, V. Wieser, and S. Pollak, "Calculation of impulse response in rician and rayleigh channel," in *2012 ELEKTRO*, 2012, pp. 99–102.
[26] D. Tse and V. Pramod, *Fundamentals of wireless communication*. United Kingdom: Cambridge University Press, Jan. 2005, vol. 9780521845274, publisher Copyright: © Cambridge University Press 2005.
[27] S. Karunaratne, E. Krijestorac, and D. Cabric, "Penetrating rf fingerprinting-based authentication with a generative adversarial attack," in *ICC 2021-IEEE International Conference on Communications*. IEEE, 2021, pp. 1–6.
[28] C. Liu, H. Xiao, Q. Wu, F. Li, and K. Tam, "Nonlinear distortion analysis of rf power amplifiers for wireless signals," in *6th International Conference on Signal Processing, 2002.*, vol. 2, 2002, pp. 1282–1285 vol.2.
[29] A. C. Polak, S. Dolatshahi, and D. L. Goeckel, "Identifying wireless users via transmitter imperfections," *IEEE Journal on Selected Areas in Communications*, vol. 29, no. 7, pp. 1469–1479, 2011.
[30] K. Simonyan and A. Zisserman, "Very deep convolutional networks for large-scale image recognition," 2014. [Online]. Available: https://arxiv.org/abs/1409.1556
[31] K. He, X. Zhang, S. Ren, and J. Sun, "Deep residual learning for image recognition," 2015. [Online]. Available: https://arxiv.org/abs/1512.03385
[32] C. Szegedy, V. Vanhoucke, S. Ioffe, J. Shlens, and Z. Wojna, "Rethinking the inception architecture for computer vision," 2015. [Online]. Available: https://arxiv.org/abs/1512.00567
[33] F. Chollet, "Xception: Deep learning with depthwise separable convolutions," 2016. [Online]. Available: https://arxiv.org/abs/1610.02357
[34] D. P. Kingma and J. Ba, "Adam: A method for stochastic optimization," 2017. [Online]. Available: https://arxiv.org/abs/1412.6980
[35] S. K. Mankani, S. Sajjanar, Mohana, and H. Ravish Aradhya, "Power and area optimization of decimation filter for application in sigma delta adc," in *2016 International Conference on Circuits, Controls, Communications and Computing (I4C)*, 2016, pp. 1–5.
[36] T. Sundstrom, B. Murmann, and C. Svensson, "Power dissipation bounds for high-speed nyquist analog-to-digital converters," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 56, no. 3, pp. 509–518, 2009.
[37] F. Rivet, Y. Deval, J.-B. Begueret, D. Dallet, P. Cathelin, and D. Belot, "The experimental demonstration of a sasp-based full software radio receiver," *IEEE Journal of Solid-State Circuits*, vol. 45, no. 5, pp. 979–988, 2010.
[38] B. Le, T. Rondeau, J. Reed, and C. Bostian, "Analog-to-digital converters," *IEEE Signal Processing Magazine*, vol. 22, no. 6, pp. 69–77, 2005.
[39] L. Zhao and Y. Cheng, "Design challenges of high speed adc in cmos technology for next generation optical communication applications," in *2014 12th IEEE International Conference on Solid-State and Integrated Circuit Technology (ICSICT)*, 2014, pp. 1–4.
[40] 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*. IEEE, 2017, pp. 1243–1244.
[41] J. O'Brien, M. F. Córdoba-Erazo, E. Rojas, J. Castro, M. Abdin, G. Mumcu, J. Wang, K. Church, P. Deffenbaugh, and T. Weller, "Miniaturization of microwave components and antennas using 3d manufacturing," in *2015 9th European Conference on Antennas and Propagation (EuCAP)*. IEEE, 2015, pp. 1–4.
[42] M. Kacar, J. Wang, G. Mumcu, C. Perkowski, K. Church, B.-I. Wu, and T. Weller, "Phased array antenna element with embedded cavity and mmic using direct digital manufacturing," in *2019 IEEE International Symposium on Antennas and Propagation and USNC-URSI Radio Science Meeting*. IEEE, 2019, pp. 81–82.
[43] M. Kacar, T. Weller, and G. Mumcu, "Conductivity improvement of microdispensed microstrip lines and grounded coplanar waveguides using laser micromachining," *IEEE Transactions on Components, Packaging and Manufacturing Technology*, vol. 10, no. 12, pp. 2129–2132, 2020.
[44] R. Liu, G. Mumcu, and J. Wang, "Towards additive manufacturing based packaging of mm-wave antenna arrays and beamformer ics," in *2024 IEEE Wireless and Microwave Technology Conference (WAMICON)*, 2024, pp. 1–3.
[45] T. Ranstrom, H. Arslan, and G. Mumcu, "Physical layer security using chaotic antenna arrays in point-to-point wireless communications," in *2024 IEEE Wireless and Microwave Technology Conference (WAMICON)*, 2024, pp. 1–4.

JUSTIN O. MCMILLEN received the Bachelor of Science degree in electrical engineering from the University of South Florida in 2022. During this time, he worked as a distribution control room engineer at The Tampa Electric Company. His research interests include multimodal data fusion, computer vision, and deep learning-based authentication. Starting in 2022, he is pursuing a Ph.D. degree in Electrical Engineering from the University of South Florida. He is currently a funded member of the University of South Florida's NSF NRT program, investigating applications of machine learning on semiconductor manufacturing, design, and security.

FAWAZ ABDUL RAZAK received the Master of Technology degree in Communication Engineering from The University of Calicut in 2016. He worked as a senior research fellow at the Indian Institute of Technology, Palakkad. His research interests include adversarial machine learning, radio frequency-ased authentication, information theory, and communication engineering. He is currently pursuing a Ph.D. degree in electrical engineering from the University of South Florida.

GOKHAN MUMCU (Senior Member, IEEE) received the B.S. degree in electrical engineering from Bilkent University, Ankara, Turkey, in 2003, and the M.S. and Ph.D. degrees in electrical and computer engineering from The Ohio State University, Columbus, OH, USA, in 2005 and 2008, respectively. He is currently a Professor in the Electrical Engineering Department at the University of South Florida, Tampa, FL, USA. His research interests include reconfigurable antennas and RF circuits with their mm-Wave applications, additive manufacturing of structural antennas and phased array antennas with integrated RF electronics, microfluidics for highly reconfigurable RF devices, and new concepts (e.g., metamaterials, volumetric 3-D reactive loading, polymers) for designing conformal, miniature, and multifunctional antennas.

Dr. Mumcu was the recipient of the 2014 CAREER Award from the U.S. National Science Foundation, the 2014 and 2024 Faculty Outstanding Research Awards from the University of South Florida, and the 2008 Outstanding Dissertation Award of The Ohio State University, ElectroScience Laboratory. He was the recipient of the 1999 International Education Fellowship of the Turkish Ministry of Education. He ranked first in the national university entrance exam taken annually by over 1.5 million Turkish students in 1999. He served as the Technical Program Committee Chair in the 2013 IEEE International Symposium on Antennas and Propagation and USNC/URSI National Radio Science Meeting, 2016 and 2025 International Workshop on Antenna Technology, and 2022 IEEE Wireless and Microwave Technology Conference (WAMICON). In addition, he served as the Vice and General Chairs of IEEE WAMICON in 2023 and 2024, respectively.

YASIN YILMAZ (S'11-M'14-SM'20) received the B.S. degree in electrical and electronics engineering from Middle East Technical University, Ankara, Turkey, in 2008, the M.S. degree in electrical and computer engineering from Koc University, Istanbul, Turkey, in 2010, and the Ph.D. degree in electrical engineering from Columbia University, New York, NY, USA, in 2014.

He is currently an Associate Professor in the Department of Electrical Engineering at the University of South Florida, Tampa, FL, USA. His research interest includes machine learning, statistical signal processing, and their applications in computer vision, cybersecurity, biomedical, energy, transportation, communication, environmental, and socioeconomic systems.

Dr. Yilmaz's awards and honors include the Highly Ranked Scholar by ScholarGPS, Top 2% most cited scientist globally by Stanford University, Best Paper Award at the 2023 IEEE Conference on Dependable and Secure Computing, and 2023 Outstanding Research Achievement Award from University of South Florida. He has been serving as a Topic Editor for Frontiers in Robotics and AI and as a Editorial Board Member for Discover Data, Springer-Nature. He was the Technical Chair of Signal Processing and Machine Learning for Social Good Symposium at IEEE GlobalSIP 2019 and Vice Chair of the Special Interest Group on AI Embedded Cognitive Networks, Technical Committee on Cognitive Networks, IEEE Communications Society.