Analytical and Experimental Validation of Wireless Authentication Through Enhanced RF Fingerprints of Chaotic Antenna Arrays

Thomas Ranstrom, Omar Jebreil, *Member, IEEE*, Fawaz Abdul Razak, Yasin Yilmaz, *Senior Member, IEEE*, and Gokhan Mumcu, *Senior Member, IEEE*

***Abstract*—Chaotic antenna arrays (CAAs) have been shown to produce enhanced and robust RF fingerprints, enabling more reliable device authentication using machine learning (ML) compared to traditional methods based on subtle hardware imperfections. In this paper, we present a novel CAA-specific multipath channel model to accurately capture the CAA's phase errors across all propagation paths providing a basis for processing schemes that remove the channel effect, enabling extraction of the RF signature of the CAA. In addition, we provide a comprehensive experimental validation of CAA-based authentication under practical wireless channel conditions and include full details covering the design, fabrication, and characterization of custom CAA nodes, along with their integration within a software-defined radio (SDR) testbed for over-the-air measurements. This manuscript shows, for the first time, that training of the ML-based authenticator on the CAA RF fingerprints can be conducted under line-of-sight (LOS) conditions and effectively generalized to diverse scenarios, including non-line-of-sight (NLOS) environments, as long as a dominant propagation path exists. High authentication accuracy is consistently achieved when this key spatial channel characteristic is preserved. Accuracy exceeds 90% in LOS and reaches up to 87% in NLOS conditions with a single dominant reflected path. This study provides the first practical validation of spatially varying CAA fingerprints, underscoring their promise for secure and robust physical layer authentication across varied wireless conditions.**

***Index Terms*—Antenna array, deep learning, software-defined radio, authentication, 3D printing, RF fingerprinting, physical layer, security, wireless communications, wireless channel.**

I. Introduction

AUTHENTICATION is a fundamental security measure in wireless systems, ensuring that devices are properly identified and trusted before access to a network can be established. While traditional authentication methods in wireless systems often rely on credential-based techniques, such as cryptographic schemes, these methods are not always secure, especially in environments vulnerable to spoofing or man-in-the-middle attacks [1], [2].

One promising alternative to traditional authentication methods is RF fingerprinting authentication, also referred to as specific emitter identification (SEI). In contrast to traditional authentication, this type of authentication typically employs machine learning (ML) to discriminate between devices based on the unique physical characteristics of the transmitted RF signals, rather than relying on software certificates [3], [4], [5], [6]. The concept of RF fingerprinting is based on the fact that all radio devices have an inherent, subtle "fingerprint" induced by their hardware, including imperfections and variations in components such as power amplifiers (PAs), I/Q modulators, and antennas. On the other hand, RF fingerprinting faces challenges. The RF fingerprints produced by devices are often not very diverse since they are caused by the manufacturing platform tolerances. Since traditional manufacturing aims to replicate devices/components as identically as possible, RF fingerprints inherently become close to each other [2]. Consequently, even state-of-the-art ML models, which are effective in many applications, may struggle to reliably differentiate between devices. This limitation makes it challenging to achieve the desired authentication accuracy, especially in environments with a large number of devices or when the signals are noisy. Nevertheless, RF fingerprint authentication, or SEI, has seen much improvement over the last years, much due to the transition from handcrafted feature extraction towards feature extraction that is ML-driven [7], [8].

Unlike the conventional research directions within the field of RF fingerprinting that focus more on marginal improvements of ML models [8], we have proposed an alternative approach where the hardware is deliberately engineered to produce a more distinctive RF fingerprint [9]. Specifically, these variations are achieved using additively manufactured (i.e., 3D printed) antennas, which can more easily introduce randomized alterations for enhanced fingerprint uniqueness. While similar antenna-based strategies have been explored by others [10], their method focused on stand-alone antennas by varying substrate thickness and incorporating non-plated through holes of different sizes and locations into circularly polarized truncated corner probe-fed patch antennas. In contrast, we examine multiple antennas, namely CAA, which are phased arrays with antenna elements and feed lines randomized in position and length, respectively (see Fig. 1).

Received 27 May 2025; revised 8 January 2026 and 7 March 2026; accepted 9 March 2026. Date of publication 18 March 2026; date of current version 2 April 2026. This work was supported by U.S. National Science Foundation under Award 2233774. The associate editor coordinating the review of this article and approving it for publication was Dr. F. Javier Lopez-Martinez. *(Corresponding author: Thomas Ranstrom.)*

The authors are with the Department of Electrical Engineering, University of South Florida, Tampa, FL 33620 USA (e-mail: jranstrom@usf.edu; omarjebreil@usf.edu; fawaz243@usf.edu; yasiny@usf.edu; mumcu@usf.edu).

Digital Object Identifier 10.1109/TIFS.2026.3675522

1556-6021 © 2026 IEEE. All rights reserved, including rights for text and data mining, and training of artificial intelligence and similar technologies. Personal use is permitted, but republication/redistribution requires IEEE permission.
See https://www.ieee.org/publications/rights/index.html for more information.
Authorized licensed use limited to: University of South Florida. Downloaded on June 18,2026 at 02:32:01 UTC from IEEE Xplore. Restrictions apply.

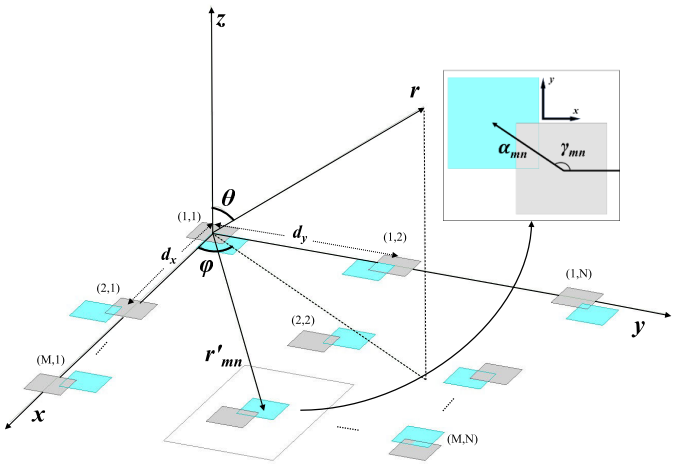


Fig. 1. Positions of antenna elements within a Chaotic Antenna Array (CAA) (cyan rectangles) in comparison to element locations of a traditional array (gray rectangles). Each element of CAA is also excited with a randomized length feed line.

These perturbations create large-scale and direction-dependent phase errors embedded in the transmitted signal, making them significantly more distinguishable than traditional RF fingerprints. Moreover, unlike many conventional high-volume manufacturing techniques, additive manufacturing is mask-free, and the introduced geometry randomizations incur no additional cost. This makes CAA and 3D-printed randomized RF hardware highly suitable for widespread adoption.

Recently, our research group made notable contributions to RF authentication and physical layer security using CAAs. In [11], the potential of ML-based RF fingerprint authentication was demonstrated with CAAs and it was shown that near perfect (approaching 99%) authentication accuracy could be achieved with 300 devices when employing a ResNet-50 model. The RF fingerprints of CAAs in [12] were further utilized during wireless communications as means of physical layer (PHY) security mechanisms. Specifically, [12] demonstrated that eavesdropping can be hindered by adding intentional distortion based on the CAA's phase errors while allowing a legitimate receiver to mitigate the distortion. Against eavesdropping, antenna architectures different than CAAs have also been considered, such as the frequency-diverse movable arrays that jointly optimize antenna positions and frequency shifts to achieve directional secrecy [13]. More recently in [14], we explored a wireless network scenario consisting of distributed receivers and showed that the users of CAAs can employ the CAA fingerprints for digital encoding along with a controlled directional phase distortion to perform PHY security in wireless communications. This latter technique showed strong promise for preventing eavesdropping while offering wireless system performance close to that of conventional communication schemes employing analog beamforming with no PHY layer security mechanism.

Our most recent work related to CAA based device authentication [15] considered simulations of time-varying Rician wireless channels and investigated factors that impact the authentication performance such as signal-to-noise ratio (SNR), selection of ML algorithms, sampling rates, and channel coherence times. In addition, [15] presented design and modeling of a potential additively manufactured antenna element and provided an initial experimental verification of CAA-based authentication. This manuscript presents key advancements and novelties with respect to [15] in several aspects, as follows:

- First-time analytical derivation of a CAA-specific multipath wireless channel model that incorporates direction-dependent phase errors across all propagation paths, fully capturing their impact on the receiver's signature extraction accuracy. In contrast, the Rician channel model in [15] considers the CAA phase error in only a single transmission direction, implicitly restricting scattering to occur within the vicinity of the receiver (authenticator) while being absent around the transmitter (CAA).
- A novel processing scheme to extract the RF signatures of CAAs from the received signal. This step is critical for enabling authentication across a diverse set of multipath scenarios exhibiting a dominant propagation path, whereas [15] is limited to scenarios where training and authentication occurs within the same wireless channel environment.
- Full details pertaining to the design and manufacturing of CAAs and the SDR-based testbed implementation with wireless signal processing and extraction, while [15] omits CAA design details and presents experimental training/authentication data limited to cases where CAAs and receiver (authenticator) remain fixed in their physical locations.
- Directional sweeps of CAAs and extraction of the fingerprints provide first-time evidence for the existence and uniqueness of direction-dependent CAA fingerprints.
- A substantially expanded and comprehensive set of real-life experiments over [15] that involves multiple positions, CAA orientations, and reflective environments to validate CAA-based authentication and associated analytical multipath wireless channel models.

These contributions collectively establish a practical and analytically grounded framework for CAA-based authentication. Section II presents an overview of the manuscript by identifying the key concepts, components, models, and software that are employed in the authentication of CAA-equipped devices. Subsequently, Section III presents the hardware details of the CAA test nodes and their manufacturing along with realized gain and $|S_{11}|$ measurements to confirm the operation of the CAA antenna elements within the targeted 5.8 GHz ISM band. Section IV details the theory, design, and implementation of the software-defined radio (SDR)-based testbed that employs the CAA test nodes and is used for capturing wireless data for the ML-based authentication. Section IV investigates the wireless channel impact in ML-based authentication of CAA test nodes with a particular emphasis on the wireless channels exhibiting a dominant propagation path. Section V presents the considered wireless scenarios while Section VI shows that ML-based authentication can utilize the captured data for detecting and identifying the CAA test nodes. Moreover, it is experimentally demonstrated that the ML-based authentication works extremely well in wireless channels exhibiting a dominant propagation path. Finally,

Authorized licensed use limited to: University of South Florida. Downloaded on June 18,2026 at 02:32:01 UTC from IEEE Xplore. Restrictions apply.

Section VII summarizes the key conclusions and outlines potential future research directions.

II. Overview of CAA-Based Authentication

CAA-based authentication consists of five main stages:

1) CAA RF Fingerprint Creation: Intentional randomization is introduced into the antenna element positions and feed line lengths in order to generate unique and direction-dependent phase errors in comparison to the traditional uniformly spaced antenna arrays.
2) Signaling strategy: During each authentication attempt, known pilot signals are transmitted from the antenna elements of a CAA in sequential order. Correlation is used on the receiver side for synchronization.
3) Wireless Channel Interaction: The transmitted signals from the antenna elements of the CAA are superimposed with the direction-dependent phase errors. The transmitted signals also get impacted by the wireless channel such as from multipath reflections, scattering, and noise.
4) Estimation and Signal Processing: The received signal transmitted from each CAA antenna element is detected and the phase is extracted. To improve accuracy, phase extraction is done through estimation across multiple symbols/samples. Signal processing is used for suppressing the wireless channel induced effects and the phase arising from the traditional array-factor components.
5) Machine Learning-Based Authentication: Processed data trains classifiers to authenticate devices based on their unique signatures.

Although the CAA fingerprints are static after CAA manufacturing, their directional dependency introduces significant variability based on the transmitter's orientation relative to the authenticator. Assuming directional knowledge is used, an adversary would need to capture the pilot signals from all possible orientations with respect to a CAA to successfully mimic a legitimate user. Additionally, subtle hardware imperfections giving rise to the traditional RF fingerprints continue to exist in the system, implying that the CAA signatures are also combined with the conventional RF fingerprints that can be potentially harnessed for added security.

III. CAA Test Nodes

A. Configuration

Our recent work in [15] presented the theoretical array factor for an $M \times N$ element 2D CAA positioned over the $x-y$ plane as depicted in Fig. 1, using spherical coordinates, which are standard in antenna theory for describing radiation patterns. In contrast to a traditional uniform 2D antenna array, each antenna element of the CAA is displaced from its default position based on the parameters of $\alpha_{mn} \in \mathcal{U}(0, \alpha_{max})$ and $\gamma_{mn} \in \mathcal{U}(0, 2\pi)$, where α_{mn} represents the magnitude of the displacement vector, γ_{mn} stands for the angle that the displacement vector makes with the $x-$axis, and $\mathcal{U}$ represents a uniform distribution. The magnitude of the displacement vector is restricted by α_{max} to prevent excessive mutual couplings among the adjacent antenna elements of the array. Since antenna element spacing in CAA is maintained to be half-wavelength on average (i.e. 0.5λ) for prevention of grating lobes, α_{max} is confined to a small fraction of the wavelength, resulting in small-scale phase errors with respect to the antenna elements of a traditional array. Therefore, the electrical length L_{mn} of each antenna feed line is also randomized based on $L_{mn} \in \mathcal{U}(0, 2\pi)$ to introduce large-scale phase errors.

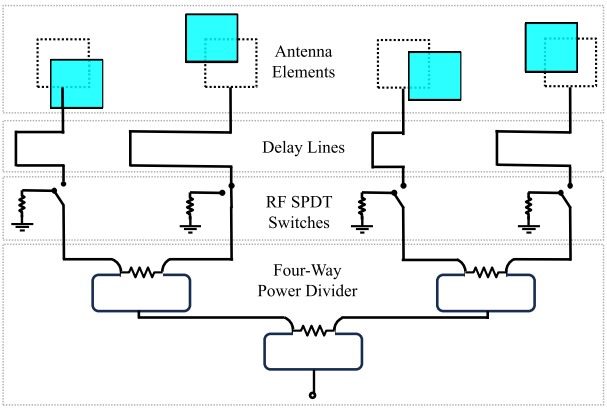


Fig. 2. Test node schematic.

The test nodes presented in this work are designed based on the array configuration in Fig. 1 with the selection of $M = 4$ and $N = 1$. Consequently, the test node CAAs are 4 element linear arrays along $x-$axis randomized in positions and feed line lengths. Dropping the subscript n, the position vector $\boldsymbol{r}'_m$ of each antenna element can be expressed as

$$\boldsymbol{r}'_m = \hat{x}[(m-1)d_x + \alpha_m \cos\gamma_m] + \hat{y}\alpha_m \sin\gamma_m \tag{1}$$

where $m = 1, 2, \ldots, M$. Following the formulation in [15], the far-field electric field $\boldsymbol{E}_m$ radiated from an antenna element can be written as

$$\begin{aligned}\boldsymbol{E}_m &= \boldsymbol{e}(\theta,\phi)\frac{e^{-jk(r-\hat{\boldsymbol{r}}\cdot\boldsymbol{r}'_m)}}{r}e^{-jL_m} \rightarrow \\ \boldsymbol{E}_m &= \boldsymbol{e}(\theta,\phi)\frac{e^{-jkr}}{r}e^{jk(m-1)d_x \sin\theta\cos\phi} \\ &\quad \times e^{jk\alpha_m \cos\gamma_m \sin\theta\cos\phi}e^{jk\alpha_m \sin\gamma_m \sin\theta\sin\phi}e^{-jL_m},\end{aligned} \tag{2}$$

where $\boldsymbol{e}(\theta,\phi)$ is the antenna elements' stand-alone electric field distribution in spherical coordinates as a function of θ and ϕ, $k = 2\pi/\lambda$ is the wave number, r stands for the length of the observation vector $\boldsymbol{r}$, and $\hat{\boldsymbol{r}}$ is the unit vector of $\boldsymbol{r}$. It is seen that the first line of (2) represents the terms that will contribute to the array factor of a traditional uniform antenna array. The second line of the equation represents the terms that will enter into the array factor due to the unique CAA configuration, implying phase errors with respect to the traditional antenna array factor. It is clearly observed that antenna position randomization results in phase errors with spatial variance (i.e. θ and ϕ dependence), whereas the feed line length randomization results in a spatially invariant phase error. Since α_m is restricted due to mutual coupling, feed line length randomization provides a large-scale phase error variation across the antenna elements of the CAA while the position randomization generates the spatial variation.

B. Design

Figure 2 depicts the schematic of the test node consisting of four design blocks. The first block is a four-way

Authorized licensed use limited to: University of South Florida. Downloaded on June 18,2026 at 02:32:01 UTC from IEEE Xplore. Restrictions apply.

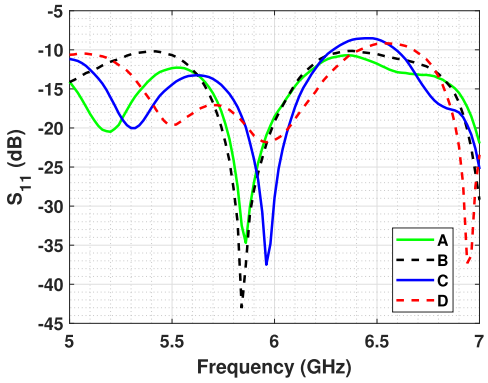


Fig. 3. Measured $|S_{11}|$ of the CAA elements A, B, C, and D.

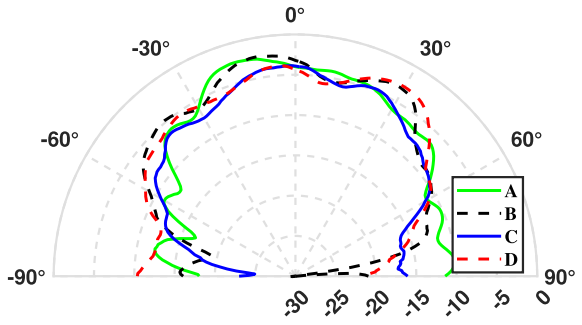


Fig. 4. Measured realized gain (dBi) of the CAA elements, A, B, C and D.

power divider formed by cascading two-way Wilkinson power dividers (WPDs) designed by following the well-established techniques [16].

The second block is the switch network to transmit individually from the antenna elements of the CAA. This block can be expanded to include phase shifters to perform beamforming in wireless communication scenarios with array radiation patterns closely approximating the traditional uniform antenna arrays [14]. The third and fourth blocks represent the randomized feed line lengths and the randomized positions of the antenna elements. To realize the randomized components with additive manufacturing, the microstrip feed lines are flipped to the backside of the RF substrate by employing vertical interconnects and slots. The antenna elements are designed as aperture coupled patch antennas on a relatively thick 3D printed ABS substrate. The antennas are also covered from the top with a thin ABS superstrate to prevent visual observation. The substrate stack-up of the test node, its fabrication details, and the operation of the test node with microcontroller are detailed in the Appendix.

C. Test Node RF Performance

Our work in [15] reported the simulated RF performance of the aperture-coupled patch antenna with a bandwidth of 9.4% while exhibiting a realized gain of 6.7 dBi (decibels relative to an isotropic radiator) at 5.8 GHz assuming a relatively short 6.5 mm long randomized feed line section. Additionally, 1200 randomized antennas were simulated with $\alpha_{\max} = 4$ mm restriction to investigate the effects of patch displacement over its coupling slot demonstrating slight frequency shifts, yet providing well impedance match across a bandwidth that includes

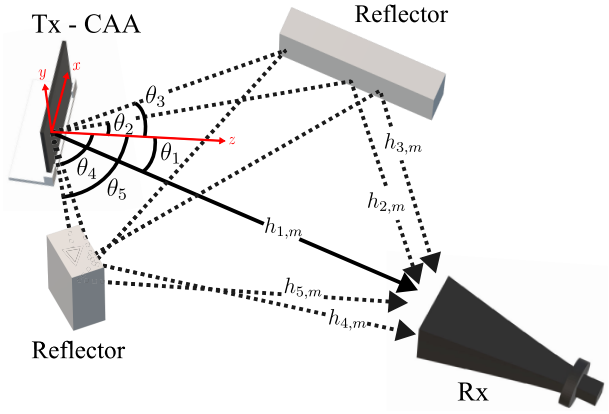


Fig. 5. Conceptual illustration of a CAA test node in a multipath wireless channel with LOS path.

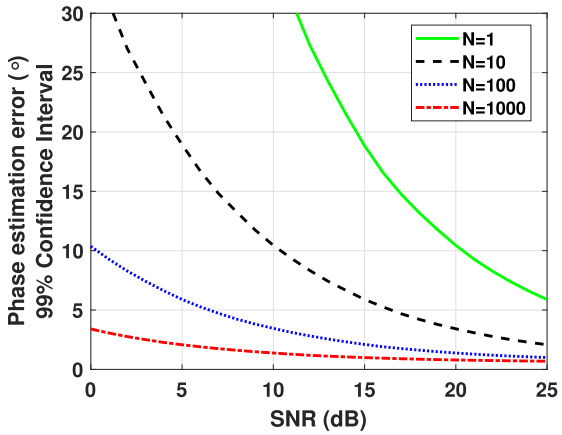


Fig. 6. Phase estimation error ϵ at 99% confidence interval when there is only a single dominant path with noise.

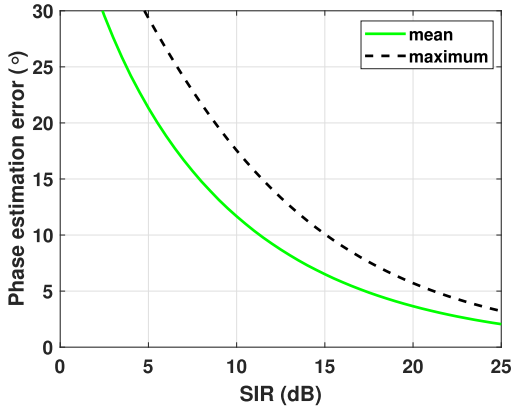


Fig. 7. Phase estimation error ϵ_{wR} in a scenario when the signals from residual paths interfere with the signal from dominant path.

and exceeds the 5.8 GHz ISM band. To experimentally verify the simulated RF performance, in this subsection, we report the measured RF performance of one of the fabricated test nodes with the design layout and manufactured parts shown in the Appendix in figures 19 and 20, respectively. The four antenna elements (labeled as A, B, C, and D in Fig. 20) were sequentially activated by reconfiguring the single-pole double-throw (SP2T) switches using the microcontroller to

Authorized licensed use limited to: University of South Florida. Downloaded on June 18,2026 at 02:32:01 UTC from IEEE Xplore. Restrictions apply.

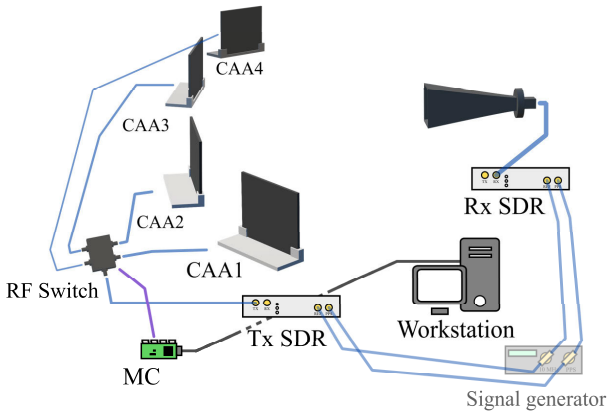


Fig. 8. Testbed setup for validation test with four CAAs. An RF switch, controlled by a Teensy 4.0 microcontroller (MC) selects the active user. Time and frequency synchronization is achieved by supplying a 10 MHz reference signal and 1 PPS signal to each of the radios.

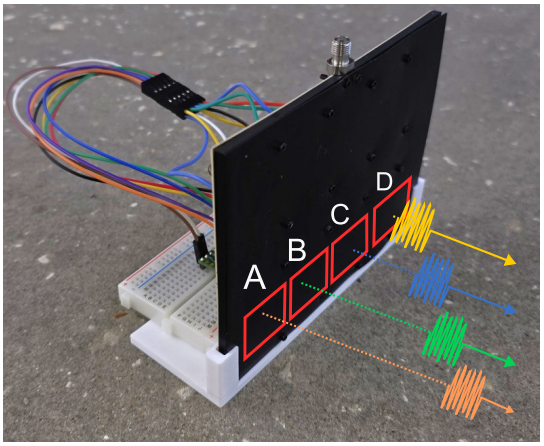


Fig. 9. Manufactured CAA test node with illustration of the sequential transmission of the authentication sequence from elements A, B, C and D.

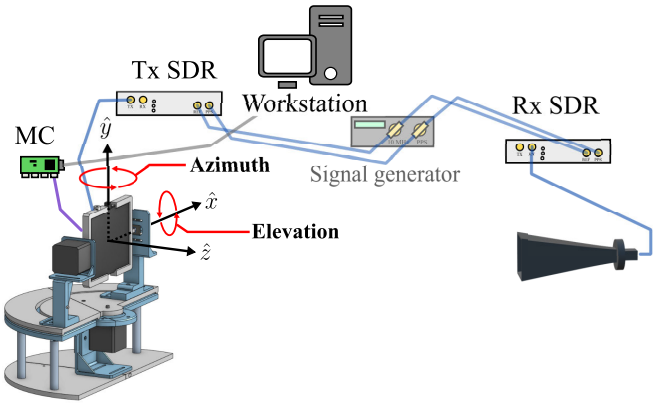


Fig. 10. SDR testbed configuration for training. The CAA test node is scanned in 3D to capture the directional dependency of its RF fingerprints.

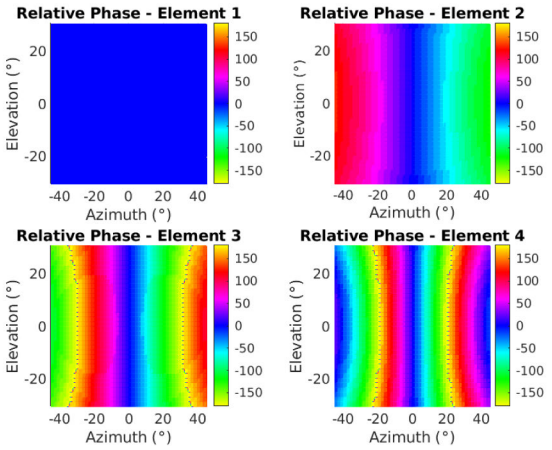


Fig. 11. Simulated phase differences (relative to element 1) perceived at authenticator (receiver) for a traditional array.

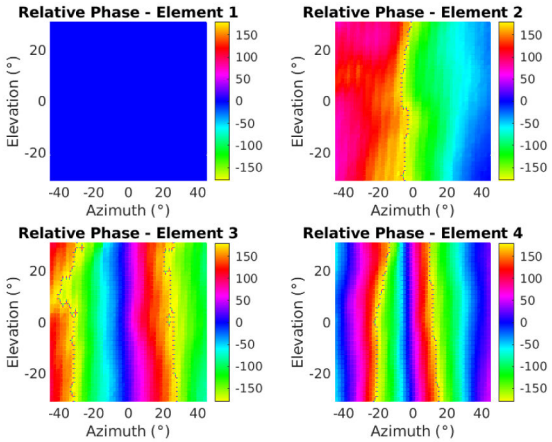


Fig. 12. Captured phase differences (relative element 1), at Rx SDR, for CAA test node #2 at a distance of 2 m.

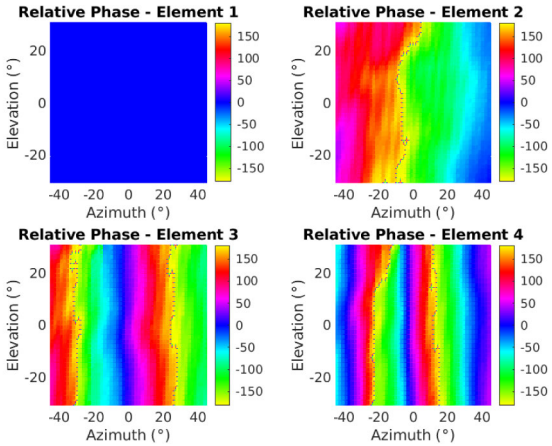


Fig. 13. Captured phase differences (relative element 1), at Rx SDR, for CAA test node #2 at a distance of 1.5 m.

measure their $|S_{11}|$ (implies well impedance matching for antenna radiation if a small quantity) and realized gain patterns. Figure 3 depicts the $|S_{11}|$ as a function of frequency and confirms that the node is well matched at 5.8 GHz with slight resonance shifts near 5.8 GHz as expected. It is also observed that $|S_{11}|$ is well matched (< -10 dB) across a much larger bandwidth than the antenna bandwidth due to the isolation and impedance matching nature of the WPDs. Figure 4 presents the measured realized gain of the antenna elements in the $H-$ (i.e. $x-z$) plane with peak values averaging at -3 dBi

Authorized licensed use limited to: University of South Florida. Downloaded on June 18,2026 at 02:32:01 UTC from IEEE Xplore. Restrictions apply.

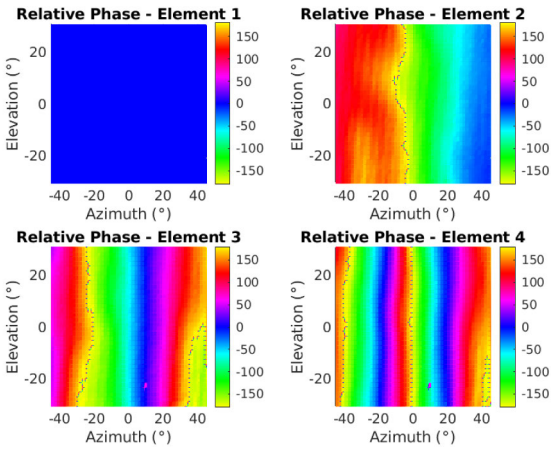


Fig. 14. Captured phase differences (relative element 1), at Rx SDR, for CAA test node #3 at a distance of 1.5 m.

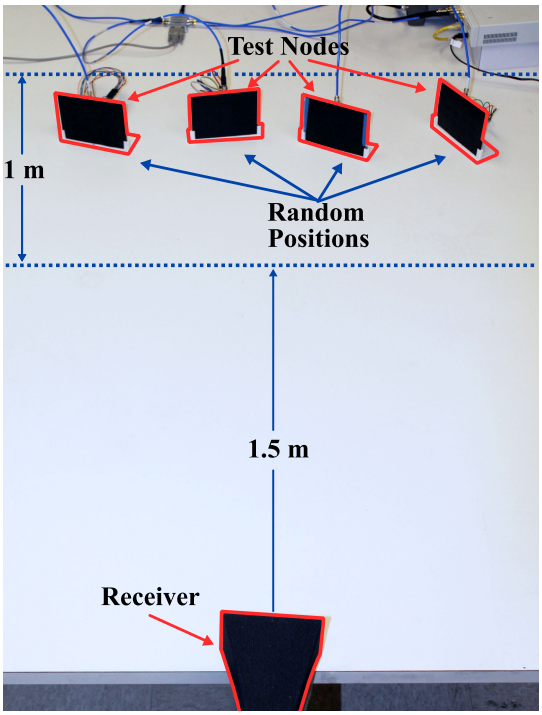
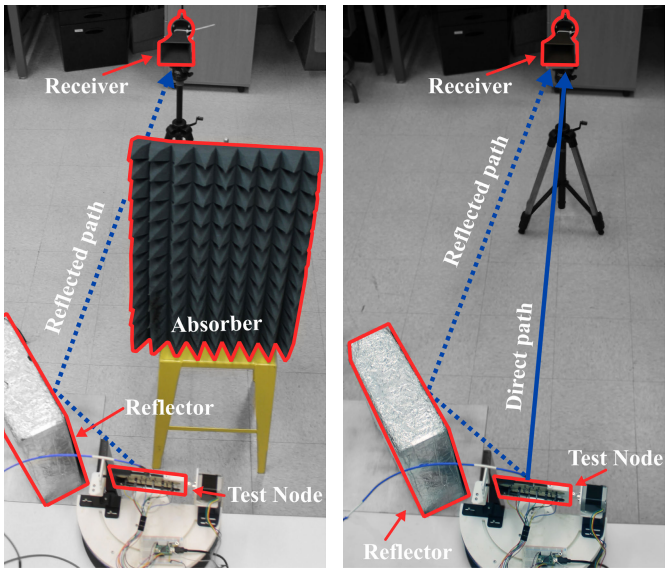


Fig. 15. Test nodes at random positions with dominant path corresponding to Scenario 1.



(a) (b)

Fig. 16. Single reflection with test node in (a) NLOS corresponding to scenario 2 (b) LOS corresponding to scenario 3.

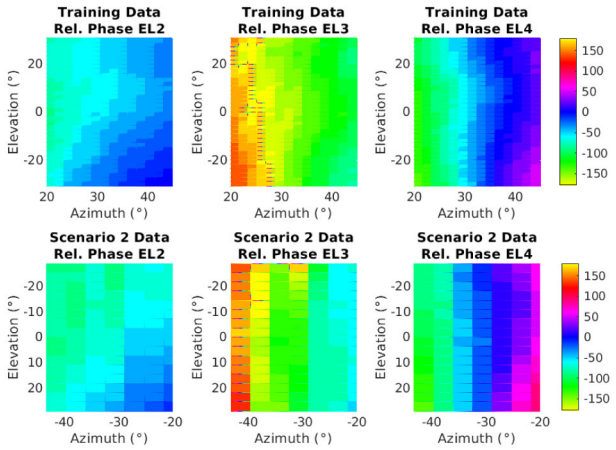


Fig. 17. Received phase comparison between training data azimuth range 20° to 45° and Scenario 2 (reflection only) data for CAA test node #2.

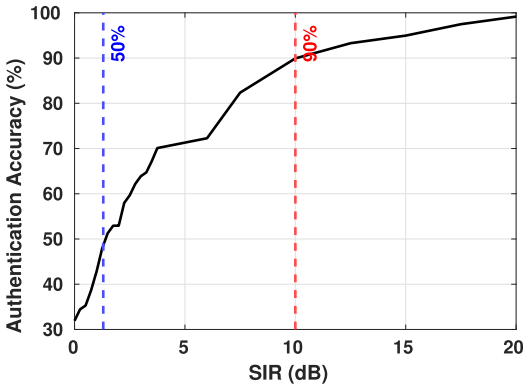


Fig. 18. CNN-3 authentication accuracy with emulated significant residual components with specific SIR. The blue and red vertical lines indicates the SIR values where the accuracy crosses 50% and 90% respectively.

which aligns closely with simulation-based expectations. The four way power divider has a theoretical loss of 6 dB due to power splitting and exhibits a simulated insertion loss (IL) of 0.5 dB. Additionally, the SP2T switch contributes an IL of 0.6 dB, while the average simulated IL of the randomized-length microstrip feed lines (accounting for both the copper trace sections and the meandered microdispensed lines from the power divider output to the antenna coupling aperture) is approximately 1.9 dB. Therefore, the realized gain expected from simulations and switch data sheet is 6.7 dB $-(6.0 + 0.5 + 0.6 + 1.9) = -2.3$ dBi. The remaining 0.7 dB discrepancy between the simulated and measured gain can be attributed to several factors, including displacement of the patch relative to the coupling slot, unaccounted connector losses, and uncertainties introduced by the screw-based mechanical assembly process. Figure 4 also shows slight ripples on the radiation patterns which is associated with the

Authorized licensed use limited to: University of South Florida. Downloaded on June 18,2026 at 02:32:01 UTC from IEEE Xplore. Restrictions apply.

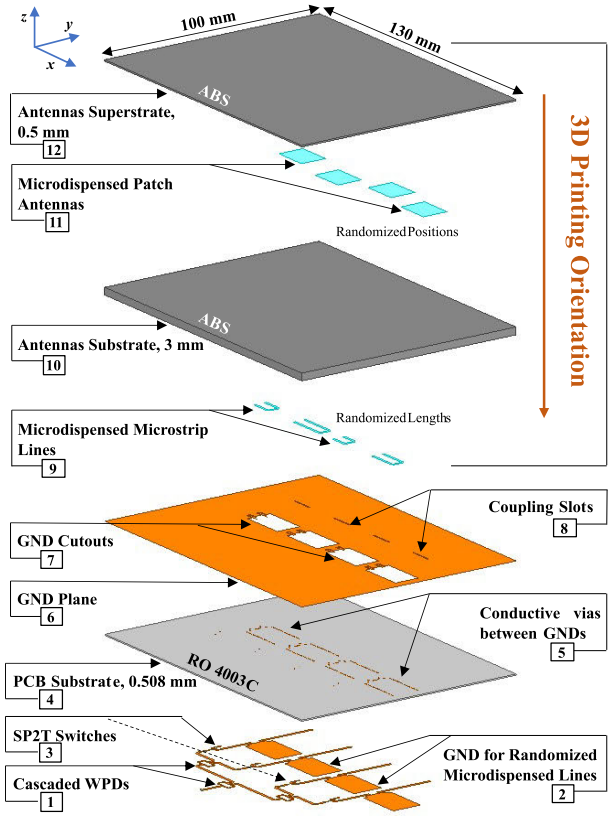


Fig. 19. Substrate stack-up of the CAA test node.

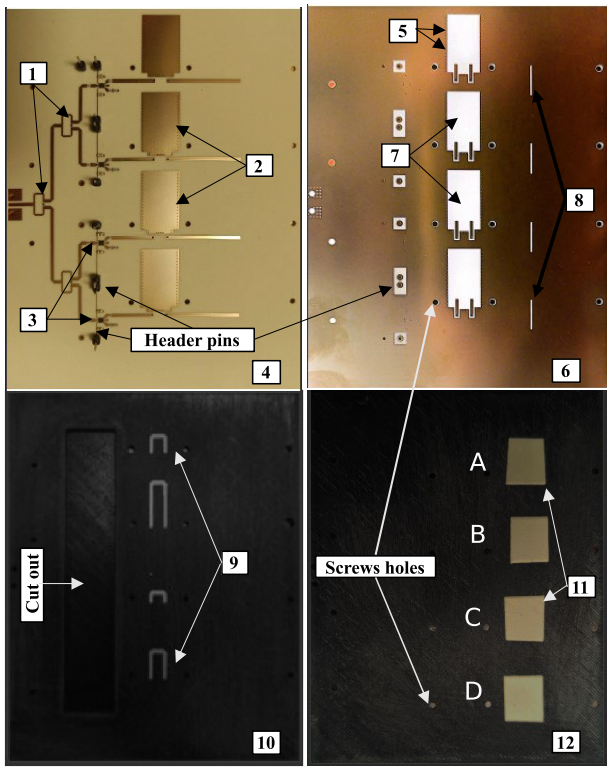


Fig. 20. Fabricated CAA test node. The numbered components correspond to the layer definitions shown in the design stack-up of Fig. 19, illustrating the physical realization of each layer in the assembled prototype.

antenna positioning relative to the large ground plane. These can be corrected in future test nodes by miniaturizing the feed network layout, reducing the substrate under the antenna elements, and/or revising the circuit layout in a way to better position the array with respect to the geometrical center of the test node.

IV. SDR-Based CAA Testbed

A. Wireless Channel Modeling

Phase errors of the CAA antenna elements get embedded into the transmitted signals. These signals also get impacted by the multipath and noise before arriving to the receiver. An analytical wireless channel model accounting for these impacts provides a mathematical basis for later signal processing steps that can be established to separate the predictable wireless channel factors from the CAA fingerprints.

As in [17], we model the complex baseband representation of the received signal $y_m(t)$ when transmitting from the CAA's mth antenna element as a linear input/output system described by

$$y_m(t) = \sum_{l=0}^{L-1} h_{l,m}(t)x(t-\tau_l(t)), \tag{3}$$

where L is the number of discrete paths, $\tau_l(t)$ is the delay of the lth path, $x(t)$ is the complex baseband representation of the transmitted signal, and $h_{l,m}(t)$ is the complex channel coefficient for element m, encapsulate the attenuation and phase shift experienced by the lth path. For short channel use duration, a time-invariant model is appropriate, allowing the time dependence in $h_{l,m}(t)$ and $\tau_l(t)$ to be dropped [17]. This assumption corresponds to operation within the channel coherence time, which was enforced through appropriate selections of authentication sequence lengths (a strategy that can also be applied in practical implementations). For a more in-depth analysis of authentication under varying channel coherence time conditions, we refer the interested reader to [15], where these effects were studied in simulations.

From sampling theory, it follows that any signal band limited within W (Hz) can be expressed as

$$x(t) = \sum_q x[q]\text{sinc}(Wt-q), \tag{4}$$

where $x[q] := x(q/W)$, $\text{sinc}(t) = \sin(\pi t)/\pi t$ and the indexing $q \in \mathbb{Z}$ is over all integers. Substituting (4) into (3) yields

$$\begin{aligned} y_m(t) &= \sum_{l=0}^{L-1} h_{l,m} \sum_q x[q]\text{sinc}(W(t-\tau_l)-q) \\ &= \sum_q x[q] \sum_{l=0}^{L-1} h_{l,m}\text{sinc}(W(t-\tau_l)-q). \end{aligned} \tag{5}$$

Sampling $y_m(t)$ at $t = n/W$ gives $y_m[n]$, and, with $p := n-q$, the discrete-time received signal, with added Gaussian noise $w[n] \sim \mathcal{CN}(0,\sigma^2)$ can be written as

$$\begin{aligned} y_m[n] &= \sum_p x[n-p] \sum_{l=0}^{L-1} h_{l,m}\text{sinc}(p-W\tau_l) + w[n] \\ &= \sum_p g_{p,m}x[n-p] + w[n], \end{aligned} \tag{6}$$

Authorized licensed use limited to: University of South Florida. Downloaded on June 18,2026 at 02:32:01 UTC from IEEE Xplore. Restrictions apply.

which is the standard convolution form with channel filter taps

$$g_{p,m} = \sum_{l=0}^{L-1} h_{l,m}\mathrm{sinc}(p - W\tau_l). \tag{7}$$

To connect the coefficients $h_{l,m}$ to the CAA in (2), we express them as

$$h_{l,m} = \tilde{h}_l e^{jk\hat{\boldsymbol{r}}_l\cdot\boldsymbol{r}'_m} e^{-jL_m}, \tag{8}$$

where $\tilde{h}_l$ captures the transmitting and receiving antenna field patterns, power loss from reflection, scattering and attenuation, and hardware impairments such as those stemming from amplification and imperfect impedance matches. A simplified illustration of a multipath propagation channel described by (3) is shown in Fig. 5 for $L = 5$ paths with the first path being the line-of-sight (LOS). The figure also shows the different θ_l for the paths once again to emphasize the fact that each path has its own unique phase error contribution due to the spatially variant phase errors of the CAA.

Unlike the classical channel model [17], (8) explicitly includes CAA-specific phase terms. The first term, $e^{jk\hat{\boldsymbol{r}}_l\cdot\boldsymbol{r}'_m}$, captures spatially variant phase errors from randomized element positions $\boldsymbol{r}'_m$ (see (1)), while e^{-jL_m} accounts for distinct feed-line lengths. These engineered variations persist across all paths and form the fingerprint. Substituting (8) into (7) gives

$$g_{p,m} = e^{-jL_m}\sum_{l=0}^{L-1}\tilde{h}_l\, e^{jk\hat{\boldsymbol{r}}_l\cdot\boldsymbol{r}'_m}\,\mathrm{sinc}(p-W\tau_l)\,, \tag{9}$$

showing that channel taps depend jointly on multipath and CAA-induced phases. This coupling makes analytical separation impractical, motivating ML-based authentication trained in multipath environments.

On the other hand, when the channel exhibits a clear dominant path, as commonly assumed in array-based PHY security schemes such as directional modulation (DM), time-modulated array (TMA) [18], and more recently, [13], the CAA's impact becomes easier to separate from general channel effects. This occurs in a single-tap regime, where the delay spread is within $1/W$, a common condition for narrowband systems even at higher frequencies [19]. It can also be enforced by using a low sampling rate [20], for which it has been shown in [15], that the ML-based authentication can be quite successful. For a single-tap channel ($g_{p,m} = 0$ except for $p = 0$), we can separate the dominant path from the rest in (9) according to

$$\begin{aligned} g_{0,m} &= e^{-jL_m}\,\tilde{h}_{l'}\,e^{jk\hat{\boldsymbol{r}}_{l'}\cdot\boldsymbol{r}'_m}\,\mathrm{sinc}(-W\tau_{l'}) \\ &\quad + e^{-jL_m}\sum_{\substack{l=0\\ l\neq l'}}^{L-1}\tilde{h}_l\,e^{jk\hat{\boldsymbol{r}}_l\cdot\boldsymbol{r}'_m}\,\mathrm{sinc}(-W\tau_l) \\ &= e^{-jL_m}\left(\tilde{g}_0\,e^{jk\hat{\boldsymbol{r}}_{l'}\cdot\boldsymbol{r}'_m} + \bar{g}_{0,m}\right), \end{aligned} \tag{10}$$

where l' corresponds to the index of the strongest path, $\tilde{g}_0$ is common across all elements and $\bar{g}_{0,m}$ depends on residual paths. If $|\tilde{g}_0| \gg |\bar{g}_{0,m}| \forall m$ (i.e., $|\tilde{h}_{l'}| \gg |\tilde{h}_l|$), it is possible to approximate (6) as

$$y_m[n] \approx e^{-jL_m}\,\tilde{g}_0\,e^{jk\hat{\boldsymbol{r}}_{l'}\cdot\boldsymbol{r}'_m}\,x[n] + w[n]. \tag{11}$$

If noise is ignored, it can be seen that under dominant path condition $y_m[n]$ no longer depends on a combination of directional phase errors making the task of the separating the impact of the CAA from that of the channel tangible. This motivates processing strategies that employs normalization to separate the fingerprints from the residual channel effects. Moreover, it also suggests that a one-time ML-based authentication training conducted in a multipath environment exhibiting a clear dominant propagation path can be employed for inferring the CAAs in any similar environments for device authentication.

B. Phase Estimation and Signal Processing

The received signal in (11) contains both the CAA-induced phase and predictable variations from the channel and array factor. If left unaddressed, these variations unnecessarily increase the complexity of the learning task, requiring the ML model to generalize over environment-dependent effects. To simplify training and improve robustness, the proposed framework applies processing that removes these predictable contributions, leaving only the CAA-specific signature. This process begins with accurate estimation of the received signal phase (combined channel and CAA) from element m, denoted Φ_m, under noisy conditions. Rewriting (11) as

$$y_m[n] = \upsilon_m x[n] + w[n] = |\tilde{g}_0|e^{j\Phi_m}x[n] + w[n], \tag{12}$$

where $\upsilon_m = |\tilde{g}_0|e^{j\Phi_m}$. As shown in [21], the form in (12) lets us write the probability density function (PDF) of $y_m[n]$ parameterized by the unknown υ_m according to

$$p\left(y_m[n];\upsilon_m\right) = \frac{1}{\pi\sigma^2}e^{-\frac{1}{\sigma^2}|y_m[n]-\upsilon_m x[n]|^2}. \tag{13}$$

Assuming N samples with independent noise, it follows that the log-likelihood function for this case can be written as

$$\begin{aligned} \ln\mathcal{L}(y_m[n];\upsilon_m) &= \sum_{n=0}^{N-1}\ln p(y_m[n];\upsilon_m) \\ &= -2N\ln\pi\sigma^2 \\ &\quad - \frac{1}{\sigma^2}\sum_{n=0}^{N-1}|y_m[n]-\upsilon_m x[n]|^2, \end{aligned} \tag{14}$$

for which finding the υ_m that maximizes the function becomes equivalent to minimizing the sum of the square differences. This can be done by taking the derivative of the sum in (14) and setting it equal to zero, yielding

$$\sum_{n=0}^{N-1} -2(y_m[n]-\hat{\upsilon}_m x[n])x^*[n] = 0, \tag{15}$$

where $\hat{\upsilon}_m$ stands for the maximizing value of υ_m and $(^*)$ denotes complex conjugate. This can be rearranged to give the maximum likelihood estimator (MLE)

$$\hat{\upsilon}_m = \frac{\sum_{n=0}^{N-1} y_m[n]x^*[n]}{\sum_{n=0}^{N-1}|x[n]|^2}, \tag{16}$$

for υ_m. The final phase estimator becomes

$$\hat{\Phi}_m = \mathrm{Arg}(\hat{\upsilon}_m) = \mathrm{Arg}\left(\sum_{n=0}^{N-1} y_m[n]x^*[n]\right), \tag{17}$$

Authorized licensed use limited to: University of South Florida. Downloaded on June 18,2026 at 02:32:01 UTC from IEEE Xplore. Restrictions apply.

with Arg(.) denoting the principal argument. Unlike estimation of υ_m in (16), there is no need to normalize by the energy of the transmitted signal as this will not affect the phase estimate.

The accuracy of the estimate $\hat{\Phi}_m$ directly impacts the reliability of the fingerprint used for authentication [15]. To quantify this, under varying signal lengths N and SNR = $|\tilde{g}_0|^2|x[n]|^2/\sigma^2$, we evaluate the estimation error

$$\epsilon = |\hat{\Phi}_m - \Phi_m|, \tag{18}$$

which is the absolute difference between the estimated ($\hat{\Phi}_m$) and the true (Φ_m) received signal phase. Monte Carlo simulations over 10,000 sequences show that increasing N significantly improves accuracy, as expected from averaging effects. Figure 6 plots the 99% confidence bound on ϵ versus SNR for different N. For $N = 1000$, the error remains below 5° for all SNR >0 dB, which is sufficient to maintain separability between fingerprints. This observation guides the choice of N in experiments.

A secondary study investigates the estimator performance subject to the signals captured from the residual paths, $\bar{g}_{0,m}$ from (10). This study aims to evaluate for which scenarios the strongest path approximation given in (11) becomes reasonable. Introducing the residual paths component into (12) results in

$$y_m[n] = (|\tilde{g}_{0,m}|e^{j\Phi_m} + |\bar{g}_{0,m}|e^{j\psi_m})x[n]. \tag{19}$$

where we represent the residual paths term in (19) with its magnitude $|\bar{g}_{0,m}|$ and phase ψ_m. Applying the estimator in (17) to (19) yields

$$\begin{aligned}\hat{\Phi}_m &= \text{Arg}\left(|\tilde{g}_{0,m}|e^{j\Phi_m} + |\bar{g}_{0,m}|e^{j\psi_m}\right)\\ &= \text{Arg}\left(e^{j\Phi_m}(|\tilde{g}_{0,m}| + |\bar{g}_{0,m}|e^{j(\psi_m-\Phi_m)})\right).\end{aligned} \tag{20}$$

We note that if the difference $\hat{\Phi}_m - \Phi_m$ in (18) is wrapped to fall inside $(-\pi, \pi]$, then the phase estimation error with residual paths ϵ_{wR} can be written as

$$\begin{aligned}\epsilon_{wR} &= \Big|\text{Arg}\left(e^{j\Phi_m}\right) + \text{Arg}\left(|\tilde{g}_{0,m}| + |\bar{g}_{0,m}|e^{j(\psi_m-\Phi_m)}\right)\\ &\quad - \Phi_m\Big| = \left|\text{Arg}\left(1 + \frac{1}{\sqrt{\text{SIR}}}e^{j(\psi_m-\Phi_m)}\right)\right|,\end{aligned} \tag{21}$$

where the signal-to-interference ratio (SIR) is equal to $|\tilde{g}_{0,m}|^2/|\bar{g}_{0,m}|^2$ and corresponds to the power ratio between the signal from the dominant path and residual paths. We note that the SIR is equivalent to the definition of K-factor for a Rician channel in which the dominant path is assumed to be the LOS path [20]. Using (21), we can compute ϵ_{wR} for any given SIR and $\psi = \psi_m - \Phi_m$ difference. Figure 7 shows this evaluation for the expected value of ϵ_{wR} when $\psi \in \mathcal{U}(0, 2\pi)$. The largest phase estimation error that can be experienced occurs when $\psi = 90°$, and corresponds to the line labeled *maximum* in Fig. 7. However, on average, the error is smaller ($\approx 5°$ at lower SIR), and gives a good indication to the estimation accuracy that can be expected at a given SIR. As such, if the system tolerance is a 20° estimation error, the SIR would typically only need to be around 5 dB. Comparing to a Rician channel, this is equivalent to having a K-factor of 5 dB which is not uncommon even in indoor environments such as an open office space [22].

With $\hat{\Phi}_m$ available, and assuming a clear dominant path, the received signal can be normalized to suppress channel and array-factor contributions. The first approach, *Processing Scheme 1*, removes the common channel phase and transmitted symbol phase:

$$r_m[n] = \frac{y_m[n]e^{-j\hat{\Phi}_{m'}}x^*[n]}{|x[n]|^2}, \tag{22}$$

where m' is a reference element and its associated received phase estimate is

$$\Phi_{m'} = \text{Arg}\left(\tilde{g}_0 e^{jk\hat{\mathbf{r}}\cdot\mathbf{r}'_{m'}}e^{-jL_{m'}}\right). \tag{23}$$

We note that the operation in (22) preserves the element-specific phase differences while eliminating the common channel effects. A second approach, *Processing Scheme 2*, additionally cancels the regular array-factor term $kd_x \sin\theta\cos\phi$ using a linear combination of phase estimates

$$r'_m[n] = \frac{y_m[n]e^{-j\hat{\Phi}_m}x^*[n]}{|x[n]|^2}e^{j(\hat{\Phi}_{\tilde{m}}-2\hat{\Phi}_{\tilde{m}+1}+\hat{\Phi}_{\tilde{m}+2})}, \tag{24}$$

where $\tilde{m} = [(m-1) \bmod (M-2)] + 1$. The final exponential term in (24) is a linear combination of phase estimates from three consecutive elements. Substituting each of these estimates with the corresponding true phase values, as given by (23), reveals that the terms depending on $kd_x \sin\theta\cos\phi$ cancel out. Hence, this scheme effectively removes this regular phase variations which is expected to improve training performance, particularly in scenarios with limited training data.

C. Testbed Configuration for Authentication

Figure 8 shows the CAA testbed configuration used to validate the proposed ML-based authentication framework under controlled wireless conditions. An Ettus N210 SDR is utilized for emulating four users CAA-equipped user nodes, each transmitting from their own CAA test nodes. Another Ettus N210 SDR is utilized as the access point (AP) receiving the transmitted data from the users. As will be detailed in Section V, objects and reflectors are introduced to create multipath propagation conditions while maintaining a dominant path, consistent with the channel conditions modeled earlier. Frequency and time synchronization between the two radios is achieved using a 10 MHz reference and 1 PPS signal from a signal generator. Signal processing is handled by a PC (workstation) which also communicates with the microcontrollers (MC) responsible for switching among the four CAA test nodes and among the antenna elements of each test node. The authentication experiments employ 1 MHz sampling rate and 0.25 MHz symbol rate. The transmit waveform from a user consists of four authentication sequences, with one sequence transmitted from each antenna element in turn. Figure 9 depicts one of the manufactured test nodes and illustrates the timing of the one-element-at-a-time signaling strategy. Although any known sequence can be used, a 1023-symbol BPSK-modulated maximum length sequence (MLS) is selected, truncated to $N = 1000$ symbols, followed by a 100-symbol (0.4 ms) guard interval to enhance robustness to timing errors. Combined with the correlation operation, this sequence allows for precise timing synchronization, compensating for hardware latency beyond the 1 PPS

Authorized licensed use limited to: University of South Florida. Downloaded on June 18,2026 at 02:32:01 UTC from IEEE Xplore. Restrictions apply.

reference [23]. As detailed in Section IV-B, the received authentication sequences are pre-processed prior to being passed on to the authenticator by normalizing the phase relative to the first antenna element in the array and scaling the signal power of each sequence to unity.

D. Training Configuration

Figure 10 shows the configuration used to collect training data for the ML-based authenticator. The same waveform described for authentication is employed during training. Each CAA test node is mounted on a custom 3D-printed motorized stand that precisely sweeps the angles between the node and the receiving antenna. The sweep covers $-45°$ to $45°$ in azimuth (rotation around the y-axis) and $-30.8°$ to $30.8°$ in elevation (rotation around the x-axis) with a step size of $1.8°$. Training is performed at two distances, 1.5 m and 2.0 m, in a regular laboratory environment under LOS conditions.

This setup ensures that the classifier learns the CAA fingerprint across a range of orientations rather than memorizing a single configuration. As discussed earlier, the following sections demonstrate that training once under LOS conditions is sufficient for authentication in multipath environments, provided a dominant path exists and SNR/SIR requirements are met.

E. Verifying the CAA RF Fingerprints

Until now, the ability of the CAA to generate a unique RF fingerprint has been demonstrated analytically and through simulation. While these results confirm the concept, real-world validation, beyond ML-based authentication performance, is necessary to prove the presence of the RF fingerprints. To address this, we present experimental evidence using data collected from the training configuration of the testbed (Section IV-D) in Figs. 12–14.

Although the authenticator operates on processed IQ samples, interpreting the raw 4×1000 time-series data is not intuitive. For visualization, we extract the estimated phase $\hat{\Phi}_m$ for each antenna element (as defined in (17)) and subtract the phase of the first element to obtain relative phase values. These are plotted against the relative azimuth and elevation angles between the CAA and the receiver.

Figure 11 shows simulated phase differences for a conventional array, where vertical bands reflect the deterministic array-factor term $k(m-1)d_x \sin\theta \cos\phi$, confirming the dominance of the direct path during training. In contrast, Fig. 12 shows measured phase differences for a CAA at 2 m, where vertical bands indicate spatial variation from randomized element positions and shifts in average values reveal contributions from distinct feed-line delays. Similarity between measurements at 2 m and 1.5 m (Fig. 13) reinforces the separability of channel and fingerprint effects under dominant-path conditions. Finally, Fig. 14 illustrates that different CAAs produce distinct phase distributions, providing direct evidence of the fingerprint concept in practice.

V. CAA Authentication Scenarios

To evaluate the robustness of the proposed CAA-based authentication framework, we considered several experimental scenarios that reflected different wireless channel conditions. By doing so, we assessed whether the authenticator could generalize beyond its training environment and maintain reliability when channel characteristics varied. The scenarios were chosen to test whether the processing schemes effectively isolated the fingerprint from channel and array-factor effects. In the following, each scenario that we considered is described in detail.

1) Dominant Path with Test Nodes at Random Positions: This scenario deploys the four test nodes at 10 different sets of positions in a confined area over a standard laboratory test bench. One such set is shown in Fig. 15. In addition to the positions, the test nodes are also rotated with respect to each other. However, no test node is positioned in a way to block each other with respect to the authenticator receiver and all test nodes maintain LOS condition. This scenario effectively demonstrates that processing Scheme 1 (22) and Scheme 2 (24) are both reliable ways of removing the channel dependency when a direct dominant path is achieved. This scenario also verifies that the ML-based authenticator can be trained only once and then be deployed in environments where users can have a dominant path which can be likely achieved with LOS conditions.

2) Single Reflection with Test Node in non-LOS (NLOS): The derivations in the previous section require a dominant path, which does not necessarily imply LOS. This scenario, shown in Fig. 16a, demonstrates these derivations by deploying the test node so that communication with the authenticator occurs through a reflected path. Absorbers are placed between the test node and the authenticator to block LOS, and a single metallic reflector is positioned close to the CAA to ensure that the reflected path is not attenuated by the directivity of the horn antenna. Successful authentication in this case confirms that a dominant path, not necessarily LOS, is sufficient for operation. Moreover, high performance in this scenario highlights the vulnerability of using a single authenticator in potential replay attacks, as an attacker might replicate the reflected signal if the location of the test node is not verified.

3) LOS with Significant Reflection Components: This scenario combines the conditions of a direct LOS path and strong reflected components. As depicted in Fig. 16b, the absorbers used in the previous scenario are removed, enabling the test node to have a direct path to the authenticator. This creates a simple multipath environment where both the direct LOS path and strong reflected paths contribute to the received signal. In this case, authentication is expected to perform worse, showing that the absence of a dominant path can reduce reliability. This confirms that a dominant path improves performance and that training only on LOS conditions may not generalize to other environments.

4) Authentication Scenario with Anomalous Transmitter: We evaluate a practical scenario, where the authenticator encounters illegitimate transmitters that were not present during training, e.g., an intrusion. We consider the dominant path environment without reflectors using four CAA devices (Baseline dataset in Table I). Devices 1–3 are treated as legitimate transmitters, while device 4 is treated as an illegitimate transmitter whose data are excluded from the training stage.

Authorized licensed use limited to: University of South Florida. Downloaded on June 18,2026 at 02:32:01 UTC from IEEE Xplore. Restrictions apply.

TABLE I
CLASSIFICATION ACCURACY ON EXPERIMENTAL TEST DATA SETS

Dataset Identifier	Comment	*CNN-3 (%)	*InceptionV3 (%)	**CNN-3 (%)	**InceptionV3 (%)
Baseline	Using training data captured according to Section IV-D with a 80-20 training to verification data split	99.15	99.02	99.65	99.11
Scenario 1	CAAs in random locations within confined area as in Fig. 15 with LOS (dominant) path maintained	95.83	96.64	99.08	99.05
Scenario 2	NLOS channel with reflector present to establish dominant reflecting path as seen in Fig. 16a	77.10	58.57	87.66	68.67
Scenario 3	LOS channel with single reflector that yields reflecting signal path as seen in Fig. 16b	19	20	16	29

* Processing Scheme 1, normalizing the phase to the first element.

** Processing Scheme 2, aiming to remove the regular phase term between consecutive elements.

VI. AUTHENTICATION USING ML AND REAL DATA

Our previous work, with emphasis on simulated data, demonstrated that convolutional neural networks (CNNs) exhibit the highest authentication performance for CAA fingerprints [15]. The superior performance of CNNs is attributed to their ability to learn local correlations among neighboring IQ samples and progressively integrate these correlations into higher-level features that capture transmitter- and channel-specific characteristics. This finding prompted us to explore two CNN-based classifiers for authentication based on the real-world data collected from the developed testbed. The learning rate was set at 5×10^{-5} for both models, and we used Adam optimizer [24] for updating the weights during training. All the models were developed in Pytorch package in Python and trained with an NVIDIA RTX 4090 GPU with 24 GB of VRAM.

Our first model which we refer to as CNN-3 (Three Layer Convolutional Neural Network) consists of three convolutional layers followed by a fully connected classification stage. The input to CNN-3 is two-dimensional sample data of size 1000×8 The first convolutional layer applies a set of learnable filters. This, to extract low level features from the input followed by a Rectified Linear Unit (ReLU) activation and pooling operation. The second convolutional layer increases the receptive field and captures higher level feature combinations again followed by ReLU and pooling. The third convolutional layer further refines the learned representations and emphasizes discriminative patterns useful for separating transmitting devices. The output of the convolutional layer is flattened and passed to a fully connected layer whose dimensionality equals the number of target devices. A softmax activation function produces class probabilities. The second CNN model we used for authentication is InceptionV3 [25]. InceptionV3 is a 48-layer convolutional network that replaces the simple "stack 3×3 then pool" pattern of VGG-16 [26] with a sequence of *Inception modules*, mini-networks that process the same feature map through several parallel branches (1×1, split 3×3, split 5×5 and max-pool paths) and concatenate their outputs. A five-layer stem first reduces the raw input to 35×35 resolution; three Inception-A blocks refine those maps, a *Reduction-A* block downsamples to 17×17, four Inception-B blocks add deeper factorised 7×7 context, and a *Reduction-B* block compresses to 8×8, where two Inception-C blocks complete the feature extractor. Global average pooling, 40 % dropout and a dense layer produce the final class scores. Every convolution is followed by batch normalisation and ReLU, yielding about 23 M trainable parameters, far fewer than VGG-16's 138 M while retaining strong representational power. We added an extra convolutional layer in the beginning to change the single channel 2D input to 3 channels which is what is expected as InceptionV3's input. We modify the 1000×8 single-channel IQ frames used for CAA authentication by copying the eight-column input 64 times along the width dimension producing a 1000×512 map whose modified width better serves the network's early stride-2 reduction. The final layer of the CNN produces a vector of real-valued outputs (logits), which are converted into posterior class probabilities using a softmax function. Let $p_i = P(\text{device } i \mid \mathbf{x})$ denote the posterior probability assigned to the i-th device for an input signal $\mathbf{x}$. The final decision is made using a *maximum a posteriori (MAP)* decision rule:

$$\hat{y} = \arg\max_i \; p_i, \tag{25}$$

which is standard practice for multi-class classification. Performance is primarily evaluated using *classification accuracy*, which directly reflects the operational objective of correctly identifying the transmitting device.

Training and testing data are collected using the testbed configurations in Section V. As noted in Section IV-B, the data is processed using both Scheme 1 (22) and Scheme 2 (24). Each sequence's average power is normalized to unity, consistent with our previous study [15]. Results of the ML-based authentication appear in Table I.

The first test, Baseline Test Set, uses 80% of captured training data for training and 20% for validation. Although not tied to a specific scenario, this test achieves greater than 99% accuracy, confirming reliable RF signature extraction and providing a performance baseline when training and deployment occur in the same environment.

The second test corresponds to Scenario 1 in Section V. Data was collected at 10 unique locations and orientations for four CAAs, with the receiving antenna at two heights (0.0 m and 0.2 m). The environment features a dominant LOS path. Authentication exceed 95%, showing both schemes

Authorized licensed use limited to: University of South Florida. Downloaded on June 18,2026 at 02:32:01 UTC from IEEE Xplore. Restrictions apply.

effectively remove channel dependence under LOS conditions. Scheme 2 improves accuracy by 5% over Scheme 1, indicating that removing the array factor helps CNN models focus on feed line and positional randomness. Training once suffices for reliable authentication when a dominant path exists.

The third test corresponds to Scenario 2. Here, LOS is blocked with absorbers, leaving a single dominant reflected path (NLOS). Despite training under LOS, performance remains high (above 87%), suggesting dominant-path NLOS resembles LOS behavior. The transmitting CAA was rotated in azimuth and elevation (3.6° steps) with limits constrained to keep reflector angles within the same bounds as the direct path during training in order to maintain consistency in learned spatial features. This is exemplified by Fig. 17 where the observed phase (relative to the first element) is plotted for both the LOS training data in the azimuth range 20° to 45° (Fig. 13) and the captured Scenario 2 data for CAA #2. The two captures are noticeably similar, and from the authenticator's perspective, there is no clear distinction between the phase observed at azimuth 30° via a LOS path and that observed at −30° via reflection. This, as indicated by the dominant path approximation (11) and processing schemes, confirms that the CAA authentication can function in NLOS as long as there is a dominant path present. Nevertheless, as the reflected signal power is inherently weaker, it makes it more susceptible to interference from scattered paths such as those originating from the edges of nearby objects or the metallic ground plane, resulting in a decrease in performance. Additionally, if only perceived direction is of importance, it may expose the CAA authentication to replay attacks. Without assessing the actual direction during authentication, the authenticator would not inherently know if a signal is coming from a reflected path, or from an adversary replaying a previously recorded signal. Our future work on adversarial attacks in CAA systems will address this potential vulnerability and explore strategies to mitigate it.

The fourth test corresponds to Scenario 3 of Section V. Authentication performance drops significantly, ranging from 16% to 29%, which aligns with the residual path analysis in Section IV-B. The low performance is expected due to two reasons: 1) The two components arriving from different directions, each with distinct phase contributions (two different phase errors), hinders the subsequent processing schemes, which rely on the dominant-path assumption. The schemes cannot remove the channel contribution, yielding a received phase that is substantially different from what was trained on. 2) If there is strong destructive interference between the two signal components, manifested as deep fades, the reduction in received signal power may lead to poorer phase estimation as shown in Fig. 6 to further impact the performance. In this test, the transmitting CAA was rotated in both azimuth and elevation over the same range used during training. This ensured that the directionally dependent phase error of the direct path remained within the model's trained range. However, the relative angle between the CAA and the reflector could occasionally extend beyond what the model had previously encountered. As shown in the radiation pattern of the CAA elements in Fig. 4, antenna gain decreases significantly at wider angles, meaning that reflected signals from those directions are naturally attenuated. Consequently, their impact on authentication is limited but still insufficient to maintain high accuracy. Constraining the angular sweep, as in Scenario 2, provides no benefit. Additionally, the processing schemes offer limited performance gains in this scenario, since both rely on the presence of a dominant path, an assumption that becomes less reliable with multiple scattered components.

To assess how SIR affects phase resolution and authentication accuracy, we emulated different SIR conditions by introducing controlled phase errors into the validation data from the baseline test set, since direct SIR control in the testbed is impractical. The results in Fig. 18 show that accuracy improves as SIR increases because $|\tilde{g}_0|$ becomes larger than $|\bar{g}_{0,m}|, \forall m$. When $|\tilde{g}_0| \gg |\bar{g}_{0,m}|, \forall m$, the dominant path assumption holds and the single-tap approximation in (11) is valid. This in turn means that the processing scheme can more accurately remove the effect of the channel, extracting a less distorted fingerprint, leading to the increased authentication performance. At an SIR of 10 dB, corresponding to a phase estimation error of about 12.5° (Fig. 7), accuracy exceeds 90%. This confirms that the ML authenticator can tolerate moderate phase errors while maintaining high accuracy, provided interference remains sufficiently weaker than the dominant path, a condition that was shown to fail in Scenario 3.

For the last scenario, first, a CNN classifier is trained using IQ measurements from the legitimate devices. Second, an autoencoder-based anomaly detector is trained using the legitimate IQ data. During testing, the reconstruction error of the autoencoder is used as an anomaly score to detect transmissions from previously unseen devices. The anomaly detection threshold is determined using the 75th percentile of the reconstruction error distribution obtained from the legitimate training samples which is set after trial and error. The CNN classifier achieves accuracy of 99.72% when evaluated on legitimate test samples. The anomaly detection stage is evaluated using a dataset containing both legitimate transmissions (devices 1–3) and anomalous transmissions from device 4. The system achieves an area under the curve (AUC) of 0.75 and an F1-score of 0.81 for distinguishing legitimate and anomalous transmissions with a false positive rate of 0.41. When considering the combined decision across the four output classes by using first the anomaly detector and then the classifier, the system achieves an overall accuracy of 73%. These results demonstrate that CAA-based authentication can maintain high accuracy for legitimate devices while detecting transmissions from previously unseen devices. While the observed false positive rate indicates that some anomalous transmissions may be incorrectly accepted as legitimate devices, this value can be improved with more advanced anomaly detection models and threshold optimization strategies in future work.

VII. Conclusion

This work presents a comprehensive validation of CAA-based device authentication through wireless channel modeling and experiments with a custom SDR testbed and fabricated CAA nodes. The results demonstrate that training performed under LOS conditions can generalize effectively to diverse scenarios, as long as a dominant path exists, regardless

Authorized licensed use limited to: University of South Florida. Downloaded on June 18,2026 at 02:32:01 UTC from IEEE Xplore. Restrictions apply.

of whether the setup is LOS or NLOS. In such cases, CAA fingerprints are reliably extractable from the channel response, enabling accurate ML-based authentication.

This is supported by the experimental results, with over 90% authentication accuracy achieved in LOS, and up to 87% in NLOS conditions where a single dominant reflected path was present, as commonly found in satellite-to-ground links, rural or open areas, and air-to-ground scenarios. In contrast, performance dropped below 30% in simple multipath environments, where the direct path and a strong reflection were present with comparable strength, resulting in no clearly dominant component. These NLOS cases are more challenging due to how the RF fingerprint is intertwined with the channel effect and need a distinct processing or additional ML training, this will be investigated in future work along with replay attacks and outdoor environments with varying channel conditions.

APPENDIX
CAA DESIGN AND MANUFACTURING

The design details of the antenna element used in the CAA and its randomized feed line are extensively reported in our recent work [15] and therefore omitted from discussion. The test nodes employ four such antennas and they are realized using the capabilities of the laser enhanced direct print additive manufacturing (LE-DPAM) technology for randomized geometries (i.e., antenna elements and feed line lengths) and standard printed circuit board (PCB) technology for the non-randomized geometries (i.e., feed line network, power divider, SP2T network). The additively manufactured part is fabricated from top to bottom in order of material layers following the approach presented in [27] and [28] as depicted in Fig. 19. The printing process begins with the deposition of a 0.5 mm thick black colored ABS base ($\epsilon_r = 2.6, \tan\delta = 0.0085$) which serves as the antenna superstrate and conceals the antennas. Milling is applied after each dielectric layer to ensure surface flatness. The patch antenna elements are subsequently microdispensed with the CB028 conductive paste ($\sigma = 1 \times 10^6$ S/m) into their randomized positions. Prior to dispensing, the CB028 ink is thoroughly mixed to ensure proper viscosity and flow consistency. The deposited conductive patches are cured by heating the printer bed to 90 °C for one hour. Next, the 3 mm thick ABS acting as the antenna substrate is printed. This is followed by the dispensing of the randomized-length feed lines with the CB028. Although not implemented in this work, the microdispensed patch and feed line edges could be further refined using laser micromachining or precision milling along the contour. Such post-processing may be considered in future fabrication to improve conductivity and edge definition [29].

The PCB, which is identical for all CAAs, is fabricated independently prior to integration to host the CAA feeding network. The design is carried out with 50Ω and 70.7Ω microstrip lines over a 0.508 mm thick RO4003C ($\epsilon_r = 3.55$, $\tan\delta = 0.0027$) substrate by providing the proper lengths and spacings to host the 0402 sized 100Ω isolation resistors. The full wave electromagnetic simulation (Ansys EDT HFSS) of the four-way divider shows a 0.5 dB IL over the theoretical value of 6 dB with a $|S_{11}| < -20$ dB within the 5.8 GHz ISM band. As expected, the power divider has a $|S_{11}| < -10$ dB bandwidth that significantly exceeds the ISM bandwidth, hence, the test node bandwidth is mainly determined by the antenna elements. Surface-mounted components, including the SP2T switches (CEL CG2409 × 3), DC blocking capacitors (2.9 pF), bypass capacitors (100 nF), and 100Ω resistors used in the Wilkinson power dividers, are assembled using a standard pick-and-place process. Header pins are soldered for microcontroller interfacing, and a cutout is created in the 3D-printed antenna substrate to host the header pins protruding from the back of the PCB. Silver epoxy is applied at the ends of the randomized, microdispensed feed lines to ensure electrical continuity with the copper traces on the PCB. Before final assembly, holes are drilled in the printed layers to match those on the PCB for precise alignment, and the two parts are secured using black-oxide alloy steel socket head screws. An RF edge-mount SMA connector is attached at the input using conductive epoxy. The fully assembled test node is then baked at 80 °C for three hours to cure the epoxy.

REFERENCES

[1] A. Barenghi, L. Breveglieri, I. Koren, and D. Naccache, "Fault injection attacks on cryptographic devices: Theory, practice, and countermeasures," *Proc. IEEE*, vol. 100, no. 11, pp. 3056–3076, Nov. 2012.

[2] K. Zeng, K. Govindan, and P. Mohapatra, "Non-cryptographic authentication and identification in wireless networks [security and privacy in emerging wireless networks]," *IEEE Wireless Commun.*, vol. 17, no. 5, pp. 56–62, Oct. 2010.

[3] J. A. Gutierrez del Arroyo, B. J. Borghetti, and M. A. Temple, "Fingerprint extraction through distortion reconstruction (FEDR): A CNN-based approach to RF fingerprinting," *IEEE Trans. Inf. Forensics Security*, vol. 19, pp. 9258–9269, 2024.

[4] X. Wang, P. Hao, and L. Hanzo, "Physical-layer authentication for wireless security enhancement: Current challenges and future developments," *IEEE Commun. Mag.*, vol. 54, no. 6, pp. 152–158, Jun. 2016.

[5] P. Tang, G. Ding, Y. Xu, Y. Jiao, Y. Song, and G. Wei, "Causal learning for robust specific emitter identification over unknown channel statistics," *IEEE Trans. Inf. Forensics Security*, vol. 19, pp. 5316–5329, 2024.

[6] G. Baldini, I. Amerini, F. Dimc, and F. Bonavitacola, "Convolutional neural networks combined with feature selection for radio-frequency fingerprinting," *Comput. Intell.*, vol. 39, no. 5, pp. 734–758, Oct. 2023.

[7] X. Wang, Q. Wang, L. Fang, M. Hua, Y. Jiang, and Y. Hu, "Radio frequency fingerprint authentication based on feature fusion and contrastive learning," *Expert Syst. Appl.*, vol. 255, Dec. 2024, Art. no. 124537.

[8] C. Liu, G. Gui, Y. Wang, T. Ohtsuki, D. Niyato, and X. Shen, "A comprehensive survey on self-supervised learning for specific emitter identification," *IEEE Commun. Surveys Tuts.*, vol. 28, pp. 1749–1775, 2026.

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

[10] N. Miguélez-Gómez and E. A. Rojas-Nastrucci, "Antenna additively manufactured engineered fingerprinting for physical-layer security enhancement for wireless communications," *IEEE Open J. Antennas Propag.*, vol. 3, pp. 637–651, 2022.

[11] J. McMillen, G. Mumcu, and Y. Yilmaz, "Deep learning-based RF fingerprint authentication with chaotic antenna arrays," in *Proc. IEEE Wireless Microw. Technol. Conf. (WAMICON)*, Apr. 2023, pp. 121–124.

[12] T. Ranstrom, H. Arslan, and G. Mumcu, "Physical layer security using chaotic antenna arrays in point-to-point wireless communications," in *Proc. IEEE Wireless Microw. Technol. Conf. (WAMICON)*, Apr. 2024, pp. 1–4.

[13] C. Li, M. Boloori, E. Jorswieck, and A. Sezgin, "Optimized frequency-diverse movable antenna arrays for directional secrecy in wireless systems," in *Proc. IEEE 36th Int. Symp. Personal, Indoor Mobile Radio Commun. (PIMRC)*, Sep. 2025, pp. 1–6.

[14] T. Ranstrom, H. Arslan, and G. Mumcu, "Physical layer security using joint directional modulation and encoding for distributed receivers serving chaotic antenna arrays," *IEEE Wireless Commun. Lett.*, vol. 14, no. 6, pp. 1658–1662, Jun. 2025.

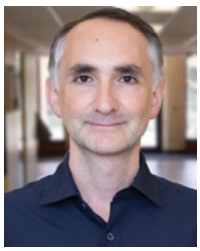
Authorized licensed use limited to: University of South Florida. Downloaded on June 18,2026 at 02:32:01 UTC from IEEE Xplore. Restrictions apply.

[15] J. O. McMillen, F. Abdul Razak, G. Mumcu, and Y. Yilmaz, "Hardware and deep learning-based authentication through enhanced RF fingerprints of 3D-printed chaotic antenna arrays," *IEEE Access*, vol. 13, pp. 6893–6908, 2025.
[16] D. M. Pozar, *Microwave Engineering*, 3rd ed., Hoboken, NJ, USA: Wiley, 2005. [Online]. Available: https://cds.cern.ch/record/882338
[17] D. Tse and P. Viswanath, *Fundamentals of Wireless Communication*. Cambridge, U.K.: Cambridge Univ. Press, 2005.
[18] O. Ansari and M. Amin, "Directional modulation techniques for secure wireless communication: A comprehensive survey," *EURASIP J. Wireless Commun. Netw.*, vol. 2022, no. 1, Sep. 2022.
[19] T. S. Rappaport et al., "Millimeter wave mobile communications for 5G cellular: It will work!," *IEEE Access*, vol. 1, pp. 335–349, 2013.
[20] H. Arslan, *Wireless Communication Signals: A Laboratory-Based Approach*. Hoboken, NJ, USA: Wiley, 2021, p. 278.
[21] S. M. Kay, *Fundamentals of Statistical Signal Processing: Estimation Theory*, 20th ed., Upper Saddle River, NJ, USA: Prentice-Hall, 2013, p. 176.
[22] Q. Wang, S. Li, X. Zhao, M. Wang, and S. Sun, "Wideband millimeter-wave channel characterization based on LOS measurements in an open office at 26GHz," in *Proc. IEEE 83rd Veh. Technol. Conf. (VTC Spring)*, May 2016, pp. 1–5.
[23] V. Wollesen and B. McHugh. (Oct. 2021). *Why is Latency Important in SDRs?*. [Online]. Available: https://www.everythingrf.com/community/why-is-latency-important-in-sdrs
[24] D. P. Kingma and J. Ba, "Adam: A method for stochastic optimization," 2014, *arXiv:1412.6980*.
[25] C. Szegedy, V. Vanhoucke, S. Ioffe, J. Shlens, and Z. Wojna, "Rethinking the inception architecture for computer vision," in *Proc. IEEE Conf. Comput. Vis. Pattern Recognit. (CVPR)*, Jun. 2016, pp. 2818–2826.
[26] K. Simonyan and A. Zisserman, "Very deep convolutional networks for large-scale image recognition," 2014, *arXiv:1409.1556*.
[27] M. Kacar, T. M. Weller, and G. Mumcu, "3D printed wideband multilayered dual-polarized stacked patch antenna with integrated MMIC switch," *IEEE Open J. Antennas Propag.*, vol. 2, pp. 38–48, 2021.
[28] M. Kacar, C. Perkowski, P. Deffenbaugh, J. Booth, G. Mumcu, and T. Weller, "Wideband Ku-band antennas using multi-layer direct digital manufacturing," in *Proc. IEEE Int. Symp. Antennas Propag. USNC/URSI Nat. Radio Sci. Meeting*, Jul. 2017, pp. 1243–1244.
[29] M. Kacar, T. Weller, and G. Mumcu, "Conductivity improvement of microdispensed microstrip lines and grounded coplanar waveguides using laser micromachining," *IEEE Trans. Compon., Packag., Manuf. Technol.*, vol. 10, no. 12, pp. 2129–2132, Dec. 2020.

Thomas Ranstrom received the M.Sc. degree in electrical engineering from Linköping University, Sweden, in 2018. He is currently pursuing the Ph.D. degree in electrical engineering with the University of South Florida, Tampa. He was a Research Engineer with Swedish Defence Research Agency (FOI), Linköping, where he focused on full-duplex radio operations and power interference mitigation. He is a member of the Reconfigurable Devices and Systems (ReDS) Laboratory. His research interests include joint communication and radar, OFDM radar, physical layer security, 5G and 6G wireless communications, physical layer wireless system security using chaotic antenna arrays, and wireless testbed development for investigating novel wireless security measures.

Omar Jebreil (Member, IEEE) received the M.Sc. degree in electrical engineering with a focus on wireless communications from Jordan University of Science and Technology (JUST), Irbid, Jordan, in 2019. He is currently pursuing the Ph.D. degree in electrical engineering with the Center for Wireless and Microwave Information Systems (WAMI), University of South Florida (USF), Tampa, FL, USA. He has worked on the design, analysis, and implementation of passive microwave components. His research interests include phased antenna arrays design, additive manufacturing for RF applications, mm-wave beam steering, and physical layer security using chaotic antenna arrays.

Fawaz Abdul Razak received the Master of Technology degree in communication engineering from the University of Calicut, in 2016. He is currently pursuing the Ph.D. degree in electrical engineering with the University of South Florida. He was a Senior Research Fellow with Indian Institute of Technology, Palakkad. His research interests include adversarial machine learning, radio frequency-based authentication, anomaly detection, information theory, and communication engineering.



Yasin Yilmaz (Senior Member, IEEE) received the B.S. degree in electrical and electronics engineering from Middle East Technical University, Ankara, Türkiye, in 2008, the M.S. degree in electrical and computer engineering from Koc University, Istanbul, Türkiye, in 2010, and the Ph.D. degree in electrical engineering from Columbia University, New York City, NY, USA, in 2014. He is currently an Associate Professor with the Department of Electrical Engineering, University of South Florida, Tampa, FL, USA. His research interests include machine learning, computer vision, cybersecurity, and their applications in communication, environmental, biomedical, energy, and transportation systems.

Gokhan Mumcu (Senior Member, IEEE) received the B.S. degree in electrical engineering from Bilkent University, Ankara, Türkiye, 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 with the Electrical Engineering Department, 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, and polymers) for designing conformal, miniature, and multifunctional antennas. He was a recipient of the 2014 CAREER Award from U.S. National Science Foundation; the 2014 and 2024 Faculty Outstanding Research Awards from the University of South Florida; the 2008 Outstanding Dissertation Award of ElectroScience Laboratory, The Ohio State University; and the 1999 International Education Fellowship of 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 for 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 Chair and the General Chair for IEEE WAMICON, in 2023 and 2024, respectively.

Authorized licensed use limited to: University of South Florida. Downloaded on June 18,2026 at 02:32:01 UTC from IEEE Xplore. Restrictions apply.