# Physical Layer Security using Chaotic Antenna Arrays in Point-to-Point Wireless Communications

Thomas Ranstrom
*Department of Electrical Engineering*
*University of South Florida*
Tampa, United States
jranstrom@usf.edu

Huseyin Arslan
*School of Engineering and Natural Sciences*
*Istanbul Medipol University*
Istanbul, Turkey
huseyinarslan@medipol.edu.tr

Gokhan Mumcu
*Department of Electrical Engineering*
*University of South Florida*
Tampa, United States
mumcu@usf.edu

***Abstract*—Chaotic antenna array (CAA)s are phased antenna arrays in which individual elements are randomized in their array position, shape, and feed line length. These randomizations generate spatially dependent large scale phase errors (with respect to antenna elements of a uniform array) that enables distinct physical layer security solutions not available to other wireless systems. Herein, a preliminary study on one such novel method, developed to combat eavesdropping is presented. In the proposed method, the CAA equipped transmitter intentionally distorts its signals based on its own array factor (AF) which includes the phase errors. This distortion significantly hampers demodulation at an eavesdropper, while a legitimate receiver that is aware of the phase errors can compensate for the added distortion.**

***Index Terms*—chaotic antenna array, physical layer security, eavesdropping, phased antenna array, physically unclonable function, wireless system**

## I. Introduction

The number of devices and applications relying on wireless communications is continuing to grow due to the ease of mobile deployment and increasing data rates. On the other hand, wireless communication signals are available in the open and therefore susceptible to many third party attacks such as eavesdropping, jamming, and spoofing [1]. Secret key based cryptography techniques have typically been employed at higher software levels of the wireless systems to address security concerns [2]. However, cryptography based security measures have several disadvantages such as storage of permanent keys, utilization of specialized hardware, and additional computational overhead that may particularly be hard to incorporate in low-cost Internet of Things (IoT) devices and wireless sensors. In addition, jamming and spoofing type of attacks aiming towards the physical layer (PHY) of the system circumvents the cryptography based measures. The needs to address these concerns have more recently motivated the studies on PHY security measures in a way to complement or replace the software level security measures.

A variety of PHY security techniques have emerged, most of which can be group under categories of: artificial noise (AN) injection [3] or active jamming, channel coding, channel-based adaptation such as directional modulation (DM) [4], channel quantization based key extraction [5], and RF fingerprinting [6]. These techniques exhibit certain advantages for security, but are not without their specific drawbacks. As an example, DM, which is a prominent antenna array PHY technique, can suffer from reduced signal-to-noise ratio (SNR), weakness when eavesdropper is aligned in same direction as the legitimate receiver, and increased complexity in implementation.

This paper investigates a novel PHY security method related to the concept of CAAs first introduced in [7] for RF fingerprinting based device authentication. In [8], RF fingerprints of CAAs were shown to be detectable with very high accuracy using machine learning algorithms removing the need for the CAA employing device to store the fingerprint in digital memory or estimate the wireless channel. The key property of CAAs is the spatially varying phase delay errors unique to the antenna elements that are introduced through the randomness in antenna positions, shapes, and feed lines [8]. Such large scale randomness can be introduced in manufacturing with no cost by utilizing additive manufacturing techniques such as the multilayered and structurally integrated antennas discussed in [9]. In this manuscript, CAA is used, for the first time, as a security measure during the wireless communication data exchange following the completion of the authentication stage. The CAA equipped transmitter intentionally distorts its signals based on its own array factor (AF) which includes the phase errors. A legitimate receiver that is aware of the phase errors can compensate for the added distortion, but eavesdropper becomes incapable of demodulation. Compared to other antenna array based PHY security measures, the proposed method is effective in inhibiting eavesdropping even when the eavesdropper and legitimate receivers are in the same direction.

### A. The Chaotic Antenna Array

CAAs were first presented in [7] as a means of generating a unique radio frequency (RF) fingerprint that could be reliably used for authentication. As covered in [8], the signature is generated by introducing randomness to the feed line leading up to each element and by randomly offsetting the element locations within the array as shown for a linear array in Fig. 1. For this manuscript, antennas are assumed to be in the x-z plane and the wireless communication scenario is assumed to take place in the x-y plane. As seen in Fig. 1, $d$ denotes the initial, fixed distance between antenna elements, while

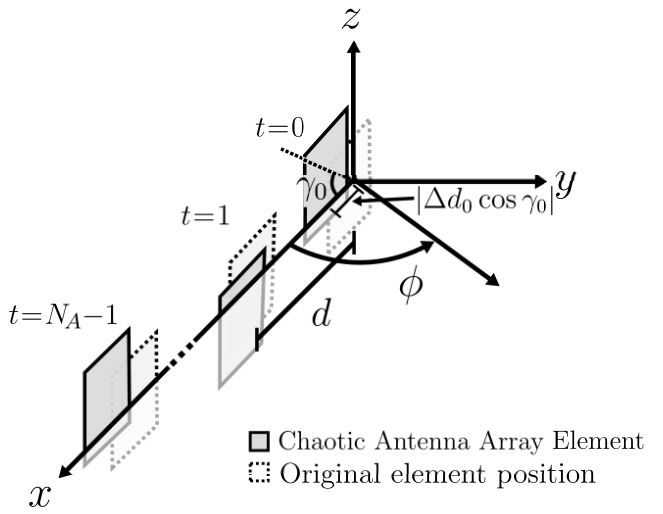


Fig. 1. Conceptual illustration of a linear CAA with randomized element locations

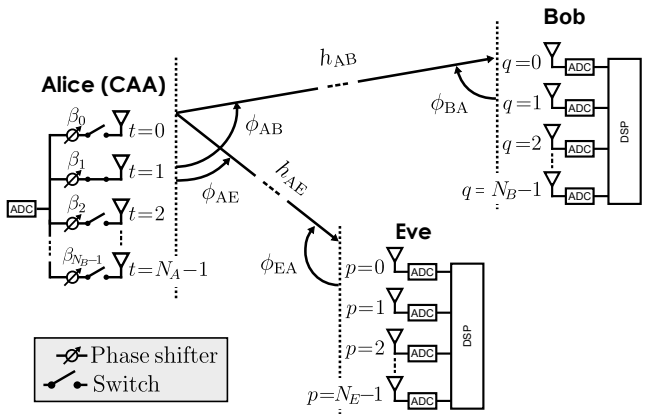


Fig. 2. System setup and scenario showing legitimate transmitter (Alice) equipped with CAA, legitimate receiver (Bob) and eavesdropper (Eve).

$\Delta d$ denotes the magnitude of the displacement vector for an antenna element relative to its original location, and $\gamma$ denotes the angle that this displacement vector makes with the x axis. Each antenna element is assigned a unique $\Delta d \in \mathcal{U}(0, \Delta d_{\max})$ and $\gamma \in \mathcal{U}(0, 2\pi)$, where $\mathcal{U}$ stands for uniform distribution. In addition, feed line length of the each antenna element is enlarged by an electrical length of $L \in \mathcal{U}(0, 2\pi)$. For an antenna with element index $t$, the phase error introduced by the position displacement and feed line length enlargement can be expressed as

$$\alpha_t(\phi) = k_0 \Delta d_t \cos\gamma_t \cos\phi - L_t, \tag{1}$$

where $k_0 = 2\pi/\lambda$ is the wave number, $\lambda$ is the wavelength of the carrier used, and $\phi$ denotes the angle-of-departure (AoD) of the plane wave emitted from the CAA in the x-y plane. A major difference of CAA over classical randomized arrays is the randomization in lengths of the element feed lines. This enhances the phase error beyond what position randomization can provide since $\Delta d$ is restricted due to inter-element mutual coupling issues that must be avoided. On the other hand, $\Delta d$ is necessary to create a spatially (i.e. $\phi$) dependent phase error to complicate the device signature as apparent from (1).

## II. System Model

The considered scenario is depicted in Fig. 2 consisting of the legitimate transmitter Alice equipped with a CAA, the legitimate receiver Bob and eavesdropper Eve. In comparison to Alice, Bob and Eve both have advanced capabilities with digital sampling at each antenna element. The AoD from Alice towards Bob and Eve are denoted by $\phi_{\text{AB}}$ and $\phi_{\text{BE}}$, while the angle-of-arrival (AoA) at Bob and Eve from Alice are denoted by $\phi_{\text{BA}}$ and $\phi_{\text{EB}}$, respectively. The complex channel gains are depicted with $h_{\text{AB}}$ and $h_{\text{BE}}$, which effectively capture the phase shift and path loss caused by the distinct propagation distance between the radios. Assuming that both Bob and Eve are within the far-field of Alice, we employ the traditional AF theory [10]. This entails that the attenuation between any pair of antenna elements $(q, t)$ is the same, and that the phase difference experienced between distinct pairs of antenna elements, depends only on their relative position within the array. Assuming a linear array with a regular element spacing of $d$, the phase difference generated by any transmitting (receiving) element $t$ ($q$) relative to the first element $t = 0$ ($q = 0$) is $tk_0 d\cos\phi_{BA}$ ($qk_0 d\cos\phi_{AB}$) [10]. It then follows that the $n$th received symbol at Bob's $q$th element can be written as

$$y_q[n] = h_{\text{AB}} e^{jqdk_0\cos\phi_{\text{BA}}} x[n] \frac{1}{\sqrt{N_A}} \sum_{t=0}^{N_A-1} e^{j(tdk_0\cos\phi_{\text{AB}} + \alpha_t(\phi_{\text{AB}}))} e^{j\beta_t}, \tag{2}$$

when Alice transmits symbol $x[n]$ by activating all of its $N_A$ elements and with its adjustable phase shifters set to $\beta_t$. Similarly, the received signal at one of Alice's antenna element, when Bob transmits a symbol $x[n]$ using all of its elements can be written as

$$z_t[n] = h_{\text{AB}} e^{j(tdk_0\cos\phi_{\text{AB}} + \alpha_t(\phi_{\text{AB}}) + \beta_t)} x[n] \frac{1}{\sqrt{N_B}} \sum_{q=0}^{N_B-1} e^{jqdk_0\cos\phi_{\text{BA}}}. \tag{3}$$

### A. Using Pilot Signals to Perform Beamforming at Alice

In order for Alice to distort its data symbols using phase modulation and Bob to accurately decode them as proposed in Section II-C, Alice and Bob must both acquire Alice's AF given by

$$\text{AF}(\phi_{\text{AB}}) = \frac{1}{\sqrt{N_A}} \sum_{t=0}^{N_A-1} e^{j(tdk_0\cos\phi_{\text{AB}} + \alpha_t(\phi_{\text{AB}}))} e^{j\beta_t}. \tag{4}$$

For Alice, this can be achieved by letting Bob repeatedly transmit a pilot sequence $\tilde{x}[n]$ while cycling through the $N_A$ antenna elements, receiving with only one active element at a time and always setting $\beta_t = 0$. By doing so, Alice obtains

the set $\{z_0[n], z_1[n], ..., z_{N_A-1}[n]\}$ of received symbols from (3), which can be used to calculate

$$\begin{aligned}\upsilon_t &= \arg\left(\frac{z_t[n]}{z_0[n]}\right) \\ &= tdk_0\cos\phi_{\text{AB}} + \alpha_t(\phi_{\text{AB}}) - \alpha_0(\phi_{\text{AB}}),\end{aligned} \tag{5}$$

where $\arg(.)$ refers to the argument operator. Substituting (5) into (4) allows to express Alice's AF as

$$\text{AF}(\phi_{\text{AB}}) = \frac{e^{j\alpha_0(\phi_{\text{AB}})}}{\sqrt{N_A}} \sum_{t=0}^{N_A-1} e^{j\upsilon_t} e^{j\beta_t}. \tag{6}$$

implying that Alice can perform beamforming and maximize its AF simply by setting its phase shifters to $\beta_t = -\upsilon_t$. It is important to note that despite knowledge of $\upsilon_t$, Alice still does not possess the knowledge of the phase errors hidden in $\alpha_t$ terms. With the maximized AF, the received signal in antenna elements of Bob becomes from (2) as

$$y_q[n] = x[n]h_{\text{AB}}\sqrt{N_A}e^{jqdk_0\cos\phi_{\text{BA}}}e^{j\alpha_0(\phi_{\text{AB}})}. \tag{7}$$

### *B. Using Pilot Signals to Acquire Alice's Phase Errors at Bob*

It is assumed that Bob is aware of Alice's CAA through knowledge of $L_t$, $\gamma_t$ and $\Delta d_t$ $\forall t \in \{0, 1, ..., N_A - 1\}$. However, this is not satisfactory for Bob to know the phase errors of Alice since they are $\phi$ dependent as was explained with equation (1). Therefore Bob must be capable of detecting $\phi_{\text{AB}}$ to fully know Alice's phase errors. To obtain $\phi_{\text{AB}}$ at Bob, Alice needs to transmit a pilot signal. Though there are various choices, it is here assumed that Alice embeds two of its $\upsilon_t$ in the pilot sequence according to

$$x[n] = \begin{cases} e^{j\upsilon_0}, & n \text{ is even} \\ e^{j\upsilon_1}, & n \text{ is odd.} \end{cases} \tag{8}$$

The motivation for Alice to share its $\upsilon_t$ in this manner instead of transmitting a pilot sequence from one element at a time is that this approach enables Alice to have all its antenna elements beamforming towards Bob for a significant SNR advantage for the pilot sequence. Assuming $n$ is even, Bob can from its received signal form

$$\frac{y_q[n]}{y_q[n+1]} = \frac{e^{j\upsilon_0}}{e^{j\upsilon_1}} = e^{-j(dk_0\cos\phi_{\text{AB}} + \alpha_1(\phi_{\text{AB}}) - \alpha_0(\phi_{\text{AB}}))}, \tag{9}$$

where the argument can, using (1), be rewritten as

$$k_0(d + \Delta d_1\cos\gamma_1 + \Delta d_2\cos\gamma_0)\cos\phi_{\text{AB}} - L_1 - L_0. \tag{10}$$

Since Bob knows everything in (10) except $\cos\phi_{\text{AB}}$, Bob can find it through

$$\cos\phi_{\text{AB}} = \frac{-\arg(\frac{y_q[n]}{y_q[n+1]}) + L_1 - L_0}{k_0(d + \Delta d_1\cos\gamma_1 - \Delta d_0\cos\gamma_0)}. \tag{11}$$

Eve on the other hand, cannot obtain $\cos\phi_{\text{AB}}$ from the transmitted sequence as it does not have access to the CAA geometry knowledge that give raise to the phase errors. Though Eve can detect the pilot sequence and obtain $\upsilon_0$ and $\upsilon_1$, all $\upsilon_t$ are required in order for Eve to circumvent the security measure proposed in the following section. In contrast, transmission of only two $\upsilon_t$ values are satisfactory for Bob and Alice to operate as shown here. Another more sophisticated attack is an actual software hack which is beyond the situation of eavesdropping. However, if such scenario occurs, Alice is not aware of its own CAA errors, only its current $\upsilon_t$, and leaking these will only let Eve circumvent the proposed technique for the current transmission angle. If the angle between Bob or Alice changes due to either radio moving, Alice will be required to update its phase shifters and a new set of $\upsilon_t$ are generated. As such, Eve must repeatedly hack Alice to obtain the current set of $\upsilon_t$.

### *C. Digital Phase Distortion based on Alice's Array Factor*

With the knowledge of $\phi_{\text{AB}}$ from (11), Bob becomes aware of Alice's CAA phase errors transmitted towards itself and can therefore extract Alice's AF given in (4) or (6). We propose to distort the digital symbols transmitted by Alice by adding a phase modulation based on Alice's AF in (6), exculding the $\alpha_0(\phi_{\text{AB}})$ term which is not known to Alice, according to

$$x[n] = m[n]e^{j\arg\left(\sum_{t=0}^{N_A-1} e^{j\upsilon_t}e^{j\eta_{t,n}}\right)}. \tag{12}$$

where $m[n]$ is the $n$th message symbol and $\eta_{t,n} \in \{\eta_{0,n}, \eta_{1,n}, ..., \eta_{N_A-1,n}\}$ are phase shifts added to the terms of the AF. $\eta$ terms are unique for each symbol and each term of the AF. The set of all $\eta_{t,n}$ are assumed known at both Alice and Bob so that demodulation can be carried out at each of Bobs antennas according to

$$\begin{aligned}&y_q[n]e^{-j\alpha_0(\phi_{\text{AB}})}e^{-j\arg\left(\sum_{t=0}^{N_A-1} e^{j\upsilon_t}e^{j\eta_{t,n}}\right)} \\ &= m[n]h_{\text{AB}}\sqrt{N_A}e^{jqdk_0\cos\phi_{\text{BA}}}.\end{aligned} \tag{13}$$

which corresponds to the original message symbol $m[n]$ with an added phase rotation and attenuation caused by $h_{\text{AB}}$ and $e^{jqk_0\cos\phi_{\text{BA}}}$. However, this can be conveniently equalized as done in standard wireless communications.

## III. Results

In the following, the proposed CAA based PHY security method was evaluated through simulations. The following steps were simulated: pilot signaling from Bob to Alice using a pseudorandom BPSK sequence of 100 symbols, estimation of $\upsilon_t$ as in (5), beamforming as performed for (7), transmission of pilot sequence (8) from Alice to Bob, estimation of $\cos\phi_{\text{BA}}$ at Bob according to (9) and (11), and finally, Alice adding distortion to the QPSK modulated data as in (12), transmitting the symbols over the channels and Bob demodulating the signal according to (13). A carrier frequency of 5.8 GHz and a maximum $\Delta d_{\text{max}}$ of 4 mm was assumed. The number of antenna elements in each of the three arrays (Alice, Bob and Eve) was set to four and the SNR was set to 10 dB during both pilot signaling and data transmission. Two distinct scenarios were considered.

In the first, $\phi_{\text{AB}} = 110°$, $\phi_{\text{BA}} = 80°$, $\phi_{\text{AE}} = 55°$,$\phi_{\text{EA}} = 145°$ which approximately corresponds to the positioning in Fig. 2 where Bob and Eve are assumed to be in very

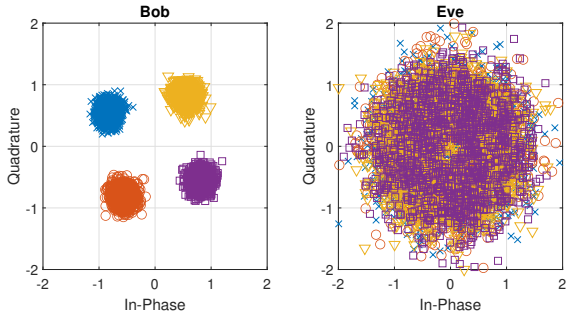


Fig. 3. QPSK constellation diagram for Bob and Eve, for the scenario in which Bob and Eve have distinct positions relative to Alice. Bob is clearly able to compensate for the added distortion and demodulate the signal, while Eve is not.

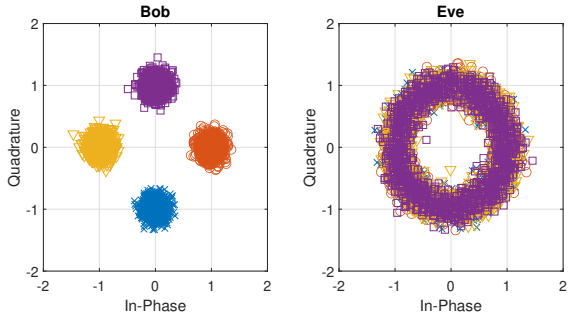


Fig. 4. QPSK constellation diagram for Bob and Eve, for the scenario in which Bob and Eve have the same relative angles to Alice. Bob is clearly able to compensate for the added distortion and demodulate the signal, while Eve is not.

different locations. The constellation diagram of the received symbols, corresponding to (13) is shown in Fig. 3, where the remaining phase rotation for Bob is due to the $h_{\text{AB}}e^{jqk_0\cos\phi_{\text{BA}}}$ in (13). Eve's received symbols can be seen to suffer from significant distortion. The effect seen, is a combination of the distortion applied by Alice and the low gain resulting from Alice beamforming towards Bob.

In the second scenario, Alice and Eve are assumed to be at the same direction, so that $\phi_{\text{AB}} = \phi_{\text{AE}} = 55°$ and $\phi_{\text{BA}} = \phi_{\text{EA}} = 145°$. The constellation diagram of the resulting received signals are shown in Fig. 4. Though Bob's constellation is similar, once again showing a phase rotation because of $h_{\text{AB}}e^{jqk_0\cos\phi_{\text{BA}}}$ that can be equalized, Eve's constellation is now in the shape of a ring. This is because Eve no longer suffers from beamforming gain, meaning the distortion is because of the added modulation at Alice, which effectively hinders Eve from demodulating the symbols.

## IV. Conclusion

It was shown that a CAA equipped transmitter can reduce an eavesdropper's ability to decode sensitive data by distorting symbols based on its own AF. A legitimate receiver on the other hand, knowing the CAA phase errors, can obtain this AF through pilot signaling and has therefore an advantage when decoding. As the legitimate transmitter does not need to know its own phase errors, a hacking attack revealing the current AF does only give limited information to an eavesdropper as the AF changes if the transmission direction changes. Additionally, as the distortion is added directly to the digital symbol, even an eavesdropper that is in the same direction as legitimate receiver will suffer.

## Acknowledgment

This work was supported by the U.S. National Science Foundation under Award # 2233774.

## References

[1] K. N. Vaishnavi, S. D. Khorvi, R. Kishore, and S. Gurugopinath, "A Survey on Jamming Techniques in Physical Layer Security and Anti-Jamming Strategies for 6G," in *2021 28th International Conference on Telecommunications (ICT)*, 2021, pp. 174–179.

[2] W. Shi, X. Jiang, J. Hu, Y. Teng, Y. Wang, H. He, R. Dong, F. Shu, and J. Wang, "Physical Layer Security Techniques for Future Wireless Networks," *arXiv preprint arXiv:2112.14469*, 2021.

[3] Y. Yang and B. Jiao, "Artificial-noise strategy for single-antenna systems over multi-path fading channels," in *2015 International Wireless Communications and Mobile Computing Conference (IWCMC)*, 2015, pp. 96–101.

[4] O. Ansari and M. Amin, "Directional modulation techniques for secure wireless communication: a comprehensive survey," *EURASIP Journal on Wireless Communications and Networking*, vol. 2022, no. 1, Sep. 2022.

[5] J. M. Hamamreh, H. M. Furqan, and H. Arslan, "Classifications and Applications of Physical Layer Security Techniques for Confidentiality: A Comprehensive Survey," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1773–1828, 2019.

[6] 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.

[7] 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, 2021.

[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, 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.

[10] D. Tse and P. Viswanath, *Fundamentals of Wireless Communication*. USA: Cambridge University Press, 2005.