Time-Varying Metamaterial-Enabled Directional Modulation Schemes for Physical Layer Security in Wireless Communication Links

ALIREZA NOORAIEPOUR, WINLAB, Department of Electrical and Computer Engineering (ECE), Rutgers University, NJ, USA
SHAGHAYEGH VOSOUGHITABAR, Department of ECE, Rutgers University, NJ, USA
CHUNG-TSE MICHAEL WU, Department of ECE, Rutgers University, NJ, USA
WAHEED U. BAJWA, WINLAB, Department of ECE, Rutgers University, NJ, USA
NARAYAN B. MANDAYAM, WINLAB, Department of ECE, Rutgers University, NJ, USA

Novel transmission schemes, enabled by recent advances in the fields of metamaterial (MTM), leaky-wave antenna (LWA) and directional modulation, are proposed for enhancing the physical layer (PHY) security. MTM-LWAs, which offer compact, integrated, and cost-effective alternatives to the classic phased-array architectures, are particularly of interest for emerging wireless communication systems including Internet-of-Things (IoT). The proposed secure schemes are devised to accomplish the functionalities of directional modulation (DM) transmitters for orthogonal frequency-division multiplexing (OFDM) and non-contiguous (NC) OFDM transmissions, while enjoying the implementation benefits of MTM-LWAs. Specifically, transmitter architectures based on the idea of time-modulated MTM-LWA have been put forth as a promising solution for PHY security for the first time. The PHY security for the proposed schemes are investigated from the point of view of both passive and active attacks where an adversary aims to decode secret information and feed spurious data to the legitimate receiver, respectively. Numerical simulations reveal that even when the adversary employs sophisticated state-of-the-art deep learning based attacks, the proposed transmission schemes are resistant to these attacks and reliably guarantee system security.

CCS Concepts: • **Hardware → Beamforming**; **Wireless devices**; • **Security and privacy → Hardware security implementation**; • **Computing methodologies** → *Machine learning*.

Additional Key Words and Phrases: Physical layer security, Directional modulation, Deep learning, Metamaterial antennas, Internet-of-Things

1 INTRODUCTION

In the emerging applications of the Internet-of-Things (IoT), IoT devices such as intelligent sensors and controllers, often operating on small-capacity batteries and running applications on ultra-low-power processors, will need to be able to communicate with each other, while being connected to the cloud [19]. In this scenario, IoT gateways

Authors' addresses: Alireza Nooraiepour, trovato@corporation.com, webmaster@marysville-ohio.com, WINLAB, Department of Electrical and Computer Engineering (ECE), Rutgers University, P.O. Box 1212, Dublin, Ohio, NJ, USA, 43017-6221; Shaghayegh Vosoughitabar, Department of ECE, Rutgers University, 1 Thørväld Circle, Hekla, NJ, USA, larst@affiliation.org; Chung-Tse Michael Wu, Department of ECE, Rutgers University, Rono-Hills, Doimukh, Arunachal Pradesh, NJ, USA; Waheed U. Bajwa, WINLAB, Department of ECE, Rutgers University, 30 Shuangqing Rd, Haidian Qu, Beijing Shi, NJ, USA; Narayan B. Mandayam, WINLAB, Department of ECE, Rutgers University, 30 Shuangqing Rd, Haidian Qu, Beijing Shi, NJ, USA.

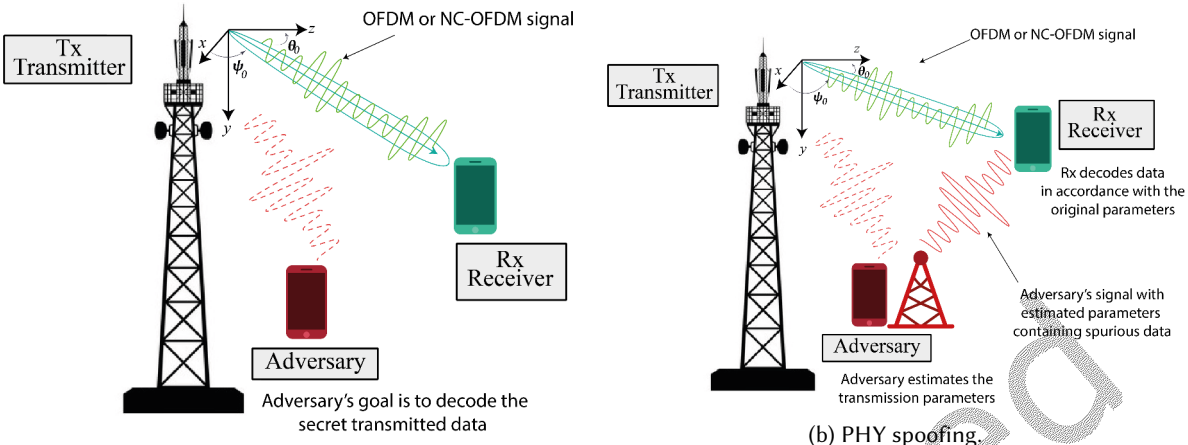
1550-4832/2022/3-ART $15.00
https://doi.org/10.1145/3513088

serve as an essential component in bridging IoT devices and the internet, thereby enabling device-to-device or device-to-cloud communication. As the IoT gateways will need to deal with critical tasks at the edge nodes, it is essential to ensure secure communication links between the gateway and the devices against any spoofing attacks by adversarial entities. Since end-to-end encrypted sessions between the edge devices and the gateway cannot be relied upon for secure communications due to the high computational and battery burden of such cryptographic strategies, there is an urgent need to develop physical-layer focused secure communication schemes [26, 34].

Directional Modulation (DM), as a promising physical-layer secure wireless communication technique, has been rapidly developed in recent years [3, 10]. It has the key property of transmitting digitally modulated signals whose waveforms are well preserved only along a pre-selected direction along which legitimate users are located in free space. DM based on phased array has been widely adopted for wireless PHY security [12, 24, 30]. This technique preserves the standard symbol constellation for the legitimate users (LUs) along predefined directions in the free space, while it intentionally scrambles the signals in all other directions. The utilization of DM for securing the IoT devices necessities the generation of high-gain beams through compact, integrated, and cost-effective antenna designs. Most common solutions to design of arrays of planar radiating elements with low or moderate directivity typically involve patch antennas, singularly activated or arranged in series to enhance the directivity of the single element. Phased arrays, however, require the use of feeding networks to control the excitation coefficients at the input ports. Digital beam-scanning technique are nowadays well established, but they involve bulky structures to accommodate multiple transceivers. More importantly, the corresponding feeding networks can be very complex, power consuming and expensive due to the heavy use of data converters [1].

An alternative, well-established solution to achieve directional beam scanning with frequency is based on metamaterial leaky-wave antennas (MTM-LWAs) [8]. These 1-D antennas enable the radiation of a high-gain fan beam leveraging on the excitation of an aperture field having exponential decay along one longitudinal direction. Furthermore, linear arrays of leaky-wave antennas (LWA) also have been put forth as an alternative to conventional two-dimensional (2-D) phased arrays, due to the possibility of obtaining narrow scannable beams with only a 1-D set of phase shifters, thereby reducing drastically the complexity and cost of the feeding network [4]. In such structures, the radiated beam can be scanned both in elevation, by acting on the operating frequency as is typical in leaky-wave radiators, and also in azimuth, by acting on the phase shift between adjacent elements. The main beam direction is determined both by the value of the phase constant of the leaky mode excited along the array and by the imposed phase shift. This LWA solution is considerably low cost with respect to conventional 2-D phased arrays and can substantially reduce the design complexity and fabrication, as well as the losses introduced by the feeding networks of the active sources of the array.

In this paper, we propose novel secure architectures to accomplish the DM functionalities through utilization of MTM-LWAs for both 1-D and 2-D spaces. As orthogonal frequency-division multiplexing (OFDM), or its variations like non-contiguous (NC) OFDM, have been widely adopted in the modern wireless communication systems, especially IoT standards [9, 31], our proposed schemes exploit the property of time-modulated arrays (TMAs) to construct OFDM/NC-OFDM DM transmitters. In TMA technique, time is used as a new degree of freedom for the array design where connecting and disconnecting the antenna elements from the feeding network in time domain would further manipulate the radiation pattern. To exploit the aforementioned benefits of the LWAs over the conventional phased arrays, our proposed secure configurations are based on the idea of time modulated MTM-LWAs which incorporate time-domain switches between the MTM unit cells. Furthermore, to enable beam scanning of LWAs at a fixed frequency we make use of tunable unit cells where a controllable inner state (On/Off) is associated with each cell. We investigate the resilience of the proposed transmission architectures against both a passive and an active adversary that either wishes to decode secret information bits or spoof a legitimate transmitter by feeding spurious data to the receiver. We assume deep learning tools are used by the adversary for conducting PHY spoofing in order to evaluate the system security against state-of-the-art powerful



(a) Passive eavesdropping.

(b) PHY spoofing.

Fig. 1. Two types of physical layer attacks.

attacks. Numerical results demonstrate that our proposed schemes indeed provide physical layer security by exploiting the unique advantages of the MTM-LWA and DM.

The rest of the paper is organized as follows. The system model is described in Section 2 along with the adversary model describing the state-of-the-art deep learning tools for PHY spoofing attack. The principles of the MTM-LWAs are presented in Section 3. We then propose our secure configurations in Section 4. Numerical results are presented in Section 5, and finally, the paper is concluded in Section 6.

2 SYSTEM MODEL

We consider a system composed of a transmitter (Tx), a receiver (Rx) and a potential active/passive adversary as depicted in Fig. 1 where the Rx, unlike the adversary, is located at certain θ and ψ angles w.r.t. the Tx. We mainly analyze two scenarios for the adversary where its goal is either to decode the secret data that is being transmitted by Tx (passive eavesdropping) or devise a PHY spoofing attack (active adversary), assuming the angles corresponding to the Rx's location are known by the Tx at the time of transmission. For passive attacks shown in Fig. 1a, the adversary is merely listening to the ongoing transmission with the aim of inferring secret messages without any form of communication with the legitimate parties. On the other hand, in the PHY spoofing attacks, the adversary overhears the signals sent by the Tx to the Rx, and its goal is to send spurious data to the Rx using signals that have similar PHY characteristics to the ones sent by the Tx as shown in Fig. 1b. When the spoofing detection algorithms based on channel frequency response fail [35, 36], the Rx cannot distinguish the source of the original and the spurious data anymore, and by decoding the latter, the underlying system security might be compromised. In practical systems, a passive eavesdropper can steal sensitive information while active attacks could compromise patients' medical devices [5] or autonomous vehicles [6], which may not only cause economic losses to individuals but also threaten peoples' lives.

The communication link between the Tx and Rx is assumed to operate over a total bandwidth B composed of a set of K subcarriers. The transmitter can either transmit over the whole band in the case of OFDM signals, or a subset of subcarriers (known as active subcarriers) in the case of NC-OFDM transmissions. OFDM/NC-OFDM

signals corresponding to one symbol duration can be written as

$$S(t) = \sum_{k=1}^{K} \mathbf{v}(k) s_k p_k e^{j2\pi f_k t}, \tag{1}$$

where $s_k \in \mathbb{C}$ and $p_k \in \mathbb{R}$ are the complex modulated symbol and a power factor applied upon the kth subcarrier, respectively. The total duration of one NC-OFDM/OFDM symbol is given by $T_o = T_s + T_{cp}$, with T_s and T_{cp} being the NC-OFDM/OFDM symbol duration and the duration of the cyclic prefix, respectively. Furthermore, $\mathbf{v}$ is called *subcarrier occupancy pattern*, which is a binary vector of size K whose kth element is zero when the kth subcarrier is inactive, and it is one when the subcarrier is active. Particularly, for an OFDM transmission $\mathbf{v}$ amounts to an all-one vector of size K. The center frequency of each subcarrier is denoted by $f_k = f_0 + k\Delta f$ where f_0 is the carrier frequency and $\Delta f = 1/T_s$ represents the width of each subcarrier.

The actual signal radiated to the wireless medium depends on the specific antenna architecture that is utilized by the Tx. Denoting the radiated OFDM/NC-OFDM signal by $R(t)$, the received signal by a party is given by the convolution $y(t) = R(t)^* h(t) + n(t)$, where $n(t)$ is additive white Gaussian noise, and $h(t)$ is the corresponding channel impulse response (CIR) between the two parties. The discrete received samples are given by $y(t_i)$, where $i = 0, \ldots, n_1 - 1$ and n_1 represents the number of (complex) samples. We assume noise samples at different time instances t_i's are independent and identically distributed (i.i.d.) with zero mean and variance $N_0/2$. Denoting $\mathbf{R} = [R(t_0), \ldots, R(t_{n_1-1})]$, the signal power is computed by $E_{\mathbf{R}} = \|\mathbf{R}\|^2/n$ where $\|\cdot\|$ is the l_2-norm. Then, SNR and SNR per bit equal $E_{\mathbf{R}}/N_0$ and $E_b/N_0 = \frac{E_{\mathbf{R}}}{QN_0}$, respectively, assuming $Q \overset{def}{=} \frac{N_a b}{N}$ where N_a denotes the number of active subcarriers, and b is the number of bits sent over each subcarrier.

Regarding the passive PHY spoofing attacks, we suppose the Tx is utilizing OFDM transmission and the decoding at both Rx and adversary is done with perfect synchronization assumption through the IFFT process similar to the prior existing works [10, 11]. However, as noted in [21, 32] OFDM signals are inherently susceptible to PHY spoofing attacks as the corresponding transmission parameters can be inferred with no ambiguity by cylcostationary analysis [23]. Therefore, in order to investigate the performance of the PHY spoofing attacks, we assume the Tx employs NC-OFDM signals which are known for their low probability of exploitation characteristics and enhanced security in comparison to an OFDM-based transmission [25, 32]. Specifically, the Tx chooses the parameters Δf, $\mathbf{v}$ and K and transmits NC-OFDM signals. The positions of active subcarriers in $\mathbf{v}$ are chosen in a random fashion for each NC-OFDM symbol. The adversary seeks to find these transmission parameters in order to generate waveforms similar to (1), inject spurious data in place of s_k, and transmit them to the receiver. We assume the Rx only decodes data that are being sent over the active subcarriers with the correct Δf and K chosen by Tx; otherwise, a decoding failure will occur. Therefore, we utilize bit error rate (BER) at Rx as a measure to evaluate the performance of the adversary in terms of spoofing. If this BER is close to that of the baseline transmission (where the parameters are perfectly known at the Rx), it is an indication of maximum spoofing performance of the adversary. At the other extreme, a BER close to 0.5 suggests that the adversary cannot do much in terms of spoofing, i.e., Tx-Rx transmission is secured against PHY spoofing. We note the subcarrier allocation pattern is assumed to be known at the Rx in a setting similar to a code division multiple access (CDMA) system where different users share spreading codes (a binary sequence) with a base station (BS) which are assumed to be known by the BS as part of the multiuser detection process [13].

Regarding the model for the active attacks, we note that the adversary has access to radio equipment for overhearing the transmissions between two legitimate parties. Furthermore, we assume the adversary is aware of the antenna architecture used by the Tx and is able to generate NC-OFDM signals with the estimated parameters and transmit them to the Rx. We also consider a setting where the adversary has resources for data processing via deep learning algorithms. The adversary can sample the received signals, and build up a dataset out of these samples where each data entry corresponds to an NC-OFDM signal. The data samples may or may not

be associated with the corresponding true transmission parameters, i.e., Δf, K and $\mathbf{v}$, referred to as labels. Depending on the availability of the labels during the training stage, two types of deep learning algorithms are useful: supervised and unsupervised. The former makes use of the labels for training the DNNs while the latter exploits possible data structure and clustering methods without using labels. We consider the state-of-the-art algorithms proposed in [21] for PHY spoofing where feed-forward fully connected deep neural networks are utilized for the supervised scenario while the unsupervised attack relies on variational auto-encoders (VAEs).

3 METAMATERIAL LWA

An MTM LWA can be realized by a cascade of composite right/left-handed (CRLH) unit cells, which has recently been utilized in various scenarios, such as radar sensing [18, 28, 37], 2D beamforming [17, 27], and active antennas [33] . A schematic of a LWA is depicted in Fig. 2.a with $N = 6$ unit cells, where p is the length of each unit cell. The total radiated pattern in the 1D space is then approximated by the array factor function [14] as

$$S(\psi) = \sum_{n=1}^{N} I_0 e^{-\alpha(n-1)p} e^{j(n-1)k_0 p \sin\psi + j\zeta_n}, \tag{2}$$

where the phase function equals

$$\zeta_n = -(n-1)k_0 p \sin\psi_0, \tag{3}$$

α denotes the leakage factor, I_0 represents the input signal of frequency f, and $k_0 = \frac{2\pi}{\lambda}$ is the wave number, where λ denotes the wavelength. For MTM-based LWA, the beam scanning angle ψ_0 is a function of the input frequency and is expressed by

$$\psi_0 = \sin^{-1}\left(\frac{\beta(w)}{k_0}\right), \tag{4}$$

where $\beta(w)$ is the phase constant as a function of $w = 2\pi f$ [1]. For the CRLH LWAs, $\beta(w)$ is determined by the equivalent circuit model for each unit cell. In [8], the authors have proposed the circuit shown in Fig. 2.b for all the unit cells, which makes it possible to obtain the directivity of a LWA of arbitrary length (N) by analyzing only one unit cell. For this case, the phase constant can be obtained via [14]

$$j\beta(w)p = \mathrm{Im}\left\{\sqrt{\left(R + jwL_R + \frac{1}{jwC_L}\right)\left(G + jwC_R + \frac{1}{jwL_L}\right)}\right\}. \tag{5}$$

It should be noted that the beam scanning angle defined in (4) only corresponds to the conventional beam scanning array with uniform cells where the phase constant remains the same across the array. In nonuniform cases, each MTM cell may have different phase constants depending on the internal mode as will be discussed in the next section.

3.1 LWA antenna beam scanning at a fixed frequency

As the frequency-dependent beam scanning feature of the LWAs may be a limiting factor in certain applications, novel LWA designs have been proposed in the literature in order to enable beam scanning at a fixed frequency. In particular, the authors in [20] have put forward a digitally modulated array factor (DMAF) method for the MTM array in which each unit cell is associated with an ON/OFF state. This is made feasible by considering a two symmetrical J-shaped pattern for each unit cell whose equivalent circuit model contains an extra element compared to Fig. 2, called capacitance C_g, that is produced between the patch near the inductance chip and the RF ground. Furthermore, a pair of surface-mounted p-i-n diodes is applied for electrically opening (mode 0) or

[1] In the remainder of the paper, we may suppress the dependence of β on w for notational simplicity.

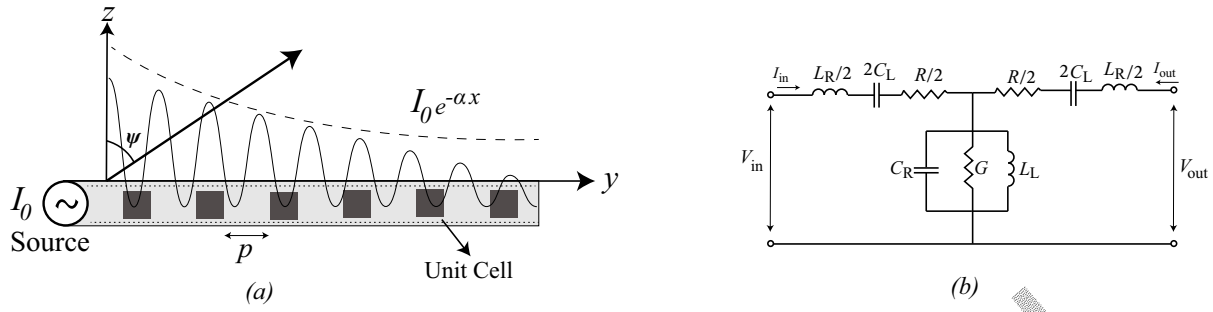


Fig. 2. a) Configuration of a periodic-structure CRLH LWA, with period p. b) Equivalent circuit model of the unit-cell in the CRLH LWA.

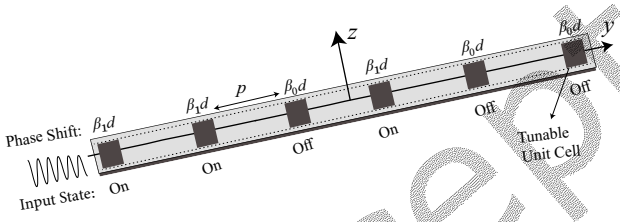


Fig. 3. LWA with tunable unit cells.

shorting (mode 1) the slots in each J-shaped pattern, which result in tuning the capacitance C_g. A schematic of LWAs with tunable unit cells is depicted in Fig. 3. The equivalent phase constant β for this configuration is computed as [20]

$$\beta(w)p = \mathrm{Im}\left\{\sqrt{jwL_R\,\frac{w^2 - w_{se}^2}{w^2}\;jwC_R\,\frac{w^2 - w_{sh}^2}{w^2 - \frac{1}{L_L C_g}}}\right\}, \tag{6}$$

where p is the length of one unit cell, and w_{sh} and w_{se} are given by

$$w_{se} = \frac{1}{\sqrt{L_R C_L}},\; w_{sh} = \sqrt{\frac{1}{L_L C_g} + \frac{1}{L_L C_R}}. \tag{7}$$

Note that tuning the capacitance C_g through the p-i-n diodes associated with each unit cell could result in two different phase constants with opposite signs in a fixed frequency. This is illustrated in Fig. 4 where the dispersion curves of a unit cell are simulated with two aforementioned modes. In fact, opening and shorting p-i-n diodes in the unit is equivalent to moving the dispersion curves up and down. Specifically, in the overlap frequency band which is highlighted in the figure, a unit cell can have both negative and positive β base on the underlying mode. When diodes are turned off (mode 0), the phase constant is negative, and it is positive when they are on (mode 1), respectively.

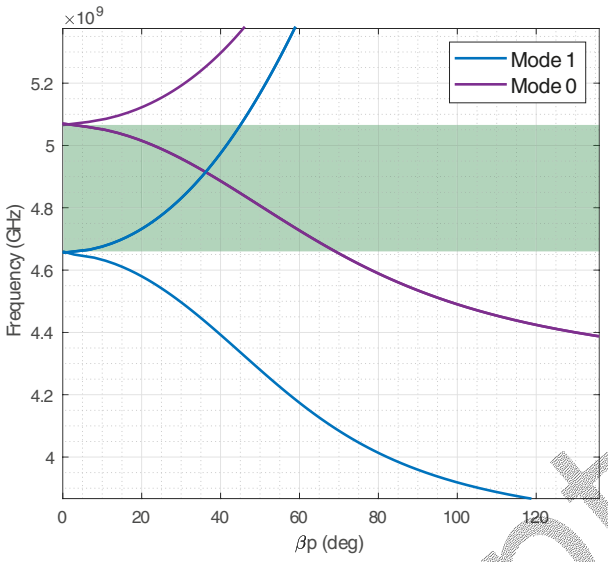


Fig. 4. Dispersion curves of a tunable unit cell with two different modes. The circuit parameters are $C_R = 0.82$ pF, $L_R = 3.45$ nH, $C_L = 0.78$ pF, $L_L = 4.38$ nH.

As the unit cells can have two different phase constants in this configuration the phase delay equation in (3) is altered as follows

$$\zeta_n = -\sum_{m=1}^{n} \phi(m), \tag{8}$$

where

$$\phi(m) \overset{def}{=} \begin{cases} \beta_0 p, & \text{if } m\text{th unit cell is in mode 0,} \\ \beta_1 p, & \text{if } m\text{th unit cell is in mode 1.} \end{cases} \tag{9}$$

Consequently, the final radiation pattern for this tunable MTM configuration can be obtained by plugging (8) in (2)

$$S(\psi) = \sum_{n=1}^{N} I_0 e^{-\alpha(n-1)p} e^{j(n-1)k_0 p \sin\psi - j\sum_{m=1}^{n}\phi(m)}. \tag{10}$$

Fig. 5 provides three different examples of the radiation patterns produced based on (10) for a frequency of 4.9 GHz. From the dispersion curves in Fig. 4, it can be deduced that $\beta_1 p = 35.6°$ and $\beta_0 p = -38.21°$ for each unit cell. We consider the number of unit cells to be $N = 10$ and the underlying working modes are denoted by a binary sequence of length 10 which is used to label the corresponding curves in Fig. 5. It is shown that continuous beam scanning between $-30°$ and $30°$ at a fixed frequency is feasible through LWAs with tunable unit cells.

4 PROPOSED CONFIGURATIONS

In this section, we propose transmitter architectures enabled by MTM LWAs which enable secure transmission to a legitimate receiver at a known location. To this end, tunable unit cells introduced in Section 3.1 are utilized

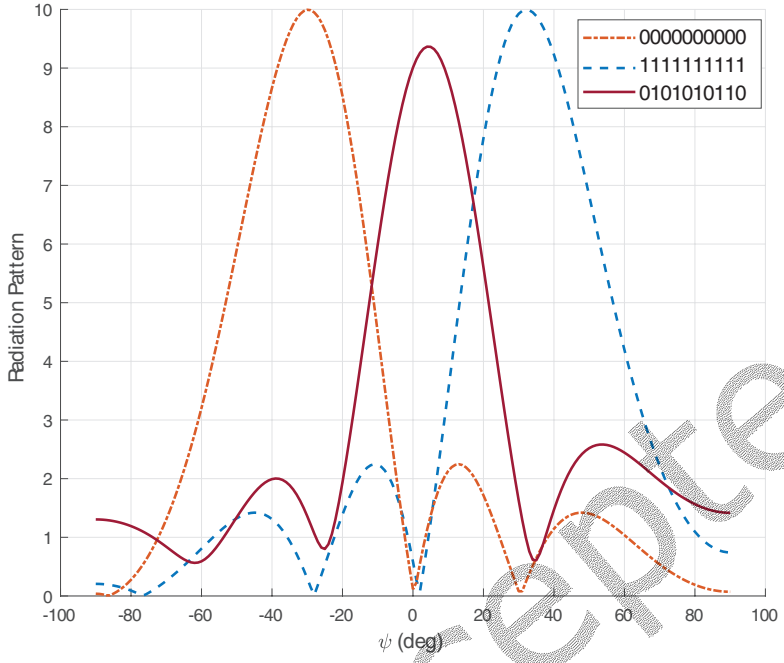


Fig. 5. Simulated radiation pattern for LWA with tunable unit cells for a fixed frequency of $f = 4.9$ GHz.

which enables the beam scanning capability of the LWAs at a fixed frequency. We start with the 1D case and further extend the idea to 2D setting.

4.1 Time-Modulated CRLH LWA

The first secure architecture we propose is time-modulated LWAs. Before getting into the details of our proposed architechture, we briefly describe the idea of time-modulation proposed in [11]. TMAs are phased arrays consisting of linear antenna elements whose radiated power patterns are controlled by periodically enabling and disabling the excitation corresponding to each individual array element. A standard TMA system consisting of an N-element linear antenna array is illustrated in Fig. 6. For the case that the elements are uniformly half-wavelength ($\lambda/2$) spaced, the radiated signal from this phased TMA can be expressed as [11]

$$R(\theta, t) = \sum_{n=1}^{N} \frac{1}{\sqrt{N}} S(t) U_n(t) e^{j(n-1)\pi(\cos\theta - \cos\theta_0)}, \tag{11}$$

where θ_0 represents the desired secure angle and $\theta \in [0, \pi]$. The authors in [11] designed the time-domain switches $U_n(t)$ in order to achieve two equally-important goals: 1) Preservation of the original transmitted signal waveform along the desired spatial direction, 2) Distortion of the transmitted signal waveform along the undesired directions. To this end, as the nth switch, a rectangular pulse starting at time t_n^s and ending at t_n^e is employed

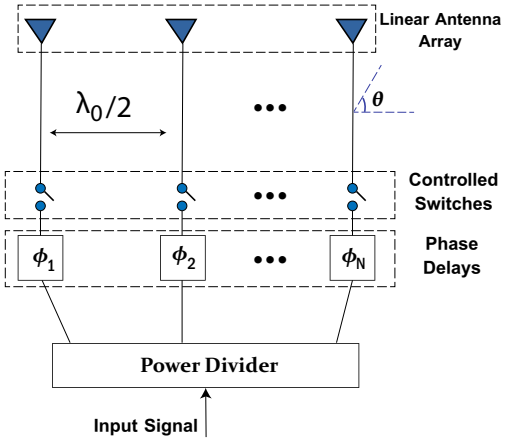


Fig. 6. Time-modulated parallel feeding.

which is defined by

$$U_n(t) = \begin{cases} 1 & \text{if } t_n^s \le t \le t_n^e, \\ 0 & \text{otherwise,} \end{cases} \quad \text{and} \quad U_n(t) = \begin{cases} 1 \text{ if} & 0 \le t \le t_n^e, \\ 1 & \text{if } t_n^s \le t \le T_p, \\ 0 & \text{otherwise,} \end{cases} \tag{12}$$

for the cases $t_n^e > t_n^s$ and $t_n^e < t_n^s$, respectively, where T_p denotes the repetition time period of the switch waveform. The *on-time* period for the nth switch is always less than T_p and equal to $\Delta t_n = t_n^e - t_n^s$ when $t_n^e > t_n^s$, or $\Delta t_n = T_p + t_n^e - t_n^s$ when $t_n^e < t_n^s$. Through Fourier series analysis, it is shown in [11] that choosing unique starting times while having identical on-time periods, denoted by Δt, for all the switches leads to the fulfillment of the two goals along θ_0, given the following is satisfied:

$$\frac{t_n^s}{T_p} \in \{\frac{i-1}{N} | i = 1, 2, \ldots, N\}, \tag{13}$$

$$\frac{\Delta t_n}{T_p} \in \{\frac{i-1}{N} | i = 1, 2, \ldots, N\}. \tag{14}$$

By comparing the radiated signal formula for LWAs in (2) or (10) with that of the above phased array (11), we conjecture that the time-modulated idea can be realized through MTM LWAs as well if one is able to control (On/Off) the input signal to each unit cell. Towards this goal, one may naively place a switch between the unit cells in the leaky guiding structure which could either incite or suppress the subsequent unit cell. However, under this architecture, if a switch located before a unit cell is off, the input signal can not reach to the subsequent units. To circumvent this impediment, we propose the architecture in Fig. 7 in which for each CRLH unit cell with microstrip implementation there exists its equivalent circuit model realized with lumped elements. Furthermore, Double-Pole-Double-Throw (DPDT) RF switches are employed between each pair of the unit cells. In this way, depending on the logic voltage level applied to the switches, the port 1 and port 2 pins connect to one of the two other port pins (port 3 or port 4) through a low insertion loss path, while maintaining a high isolation path to the alternate port. If the switches located before a unit cell are off, the input signal can still reach the switch located after this unit cell, through the other pass created by the lumped realization of the CRLH unit cells. For

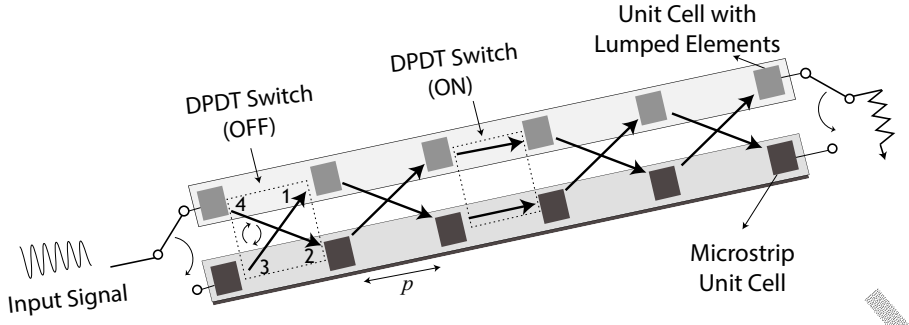


Fig. 7. Time-modulated CRLH LWA.

this configuration, the radiated signal can be expressed by

$$R(\psi,t)=\sum_{n'=1}^{N'}S(t)e^{-\alpha(n'-1)p}U_{n'}^{'}(t)e^{j(n'-1)k_0p\sin\psi-j\sum_{l=1}^{n'}\beta_l p} \tag{15}$$

where N' denotes the number of microstrip unit cells. We note that for a typical LWA the values of αp is pretty small[2] and thus the exponential term ($e^{-\alpha(n'-1)p}$) can be approximated by one. Under this assumption, one can conclude that the choice of the switches in (13) would result in time-modulated LWAs. For the remainder of the paper, we consider time-modulated LWAs that only have one unit cell on at a time. Then, the DM functionality goals can be achieved if the switch parameters are chosen as

$$\frac{t_n^s}{T_p}\in\{\frac{i-1}{N}|i=1,2,\ldots,N\}, \tag{16}$$

$$\frac{\Delta t_n}{T_p}=\frac{1}{N},\ \forall n. \tag{17}$$

We note that with the above choices for the switches, the beginning of the OFDM signal, $S(t)$, is transmitted through the first unit cell. As a result, the existing timing synchronization methods, e.g., Schmidl & Cox synchronization for OFDM [29], can be utilized by a receiving party to estimate the start of an OFDM symbol.

4.2 Time-Modulated parallel feeding with plain CRLH LWA

For this architecture, a standard TMA system consisting of an N-element linear antenna array is considered where two consecutive antenna elements are placed a certain distance d apart, and have identical isotropic active element patterns. We propose to equip each branch with a CRLH LWA, which would enable radiation in a 2D space. The input signal is split into N copies with identical power, phase-delayed and then sent through a time-domain *On-Off* RF switch $U_n(t)$. These switches are designed based on the parameters described in the previous section. However, before reaching the end of the branch, the time-domain manipulated signal is fed to a CRLH LWA in each branch with N' unit cells spaced p apart. A schematic of this configuration is presented in Fig. 8. Mathematically, the radiated signal into the space for this configuration can be obtained based on the

[2]The typical value of α was reported as a constant at the average value of 0.02 while p was taken to be in the order of a centimeter (0.01) in [8].

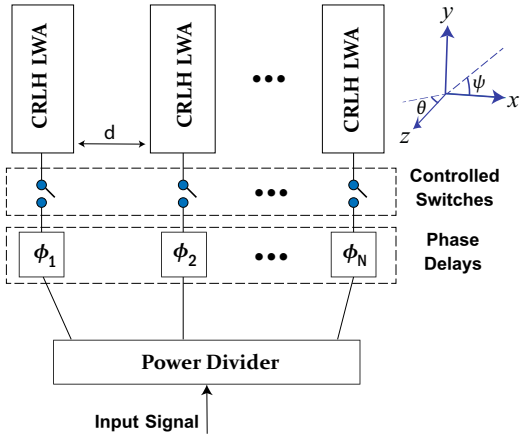


Fig. 8. Time-modulated parallel feeding with plain CRLH LWA.

array factor approach of a 2D LWA structure [2] and TMA principle

$$R(\theta,\psi,t)=\sum_{n=1}^{N}\frac{1}{\sqrt{N}}S(t)\Big(\sum_{n'=1}^{N'}e^{-\alpha(n'-1)p}e^{j(n'-1)k_0p\sin\theta\sin\psi-j\sum_{l=1}^{n'}\beta_lp}\Big)U_n(t)e^{j(n-1)k_0d(\sin\theta\cos\psi-\sin\theta_0\cos\psi_0)}, \quad (18)$$

where $\theta\in[0,\pi/2]$ and $\psi\in[0,2\pi]$. Also, the wave number is defined as $k_0=\frac{2\pi f_0}{c}$ where f_0 and c denotes the carrier frequency of the input signal and the speed of light, respectively. The choices of switches $U_n(t)$ in (13) and (14) will realize the DM functionalities, i.e., preserving the input signal along θ_0 and ψ_0 during transmission and distorting it along any other direction. By utilizing such switches in (18) for the desired angles θ_0 and ψ_0, we have

$$R(\theta_0,\psi_0,t)=\frac{\Delta t}{T_p}\sqrt{N}\Big(\sum_{n'=1}^{N'}e^{-\alpha(n'-1)p}\Big)S(t), \quad (19)$$

which indicates that the original signal is preserved. In fact, $S(t)$ is scaled by a gain which is a function of beamforming, switches' on-time period, and the LWA characteristics. For the undesired spatial angles, on the other hand, the received signal is distorted in the time domain as follows

$$R(\theta,\psi,t)=\frac{1}{\sqrt{N}}S(t)\Big(\sum_{n'=1}^{N'}e^{-\alpha(n'-1)p}e^{j(n'-1)k_0p\sin\theta\sin\psi-j\sum_{l=1}^{n'}\beta_lp}\Big)\sum_{m=-\infty}^{\infty}V(t,m,N,t_n^s,\Delta t_n,\theta,\psi), \quad (20)$$

where

$$V(t,m,N,t_n^s,\Delta t_n,\theta,\psi)=\sum_{n=1}^{N}\Big(\frac{\sin\big(m\pi f_p\Delta t_n\big)}{m\pi}e^{j2m\pi f_p(t-t_n^s-\Delta t_n/2)}\Big)e^{j(n-1)k_0d(\sin\theta\cos\psi-\sin\theta_0\cos\psi_0)}. \quad (21)$$

In fact, for this architecture the DM functionalities along the both θ and ψ angles are realized via only one set of switches denoted by $U_n(t)$.

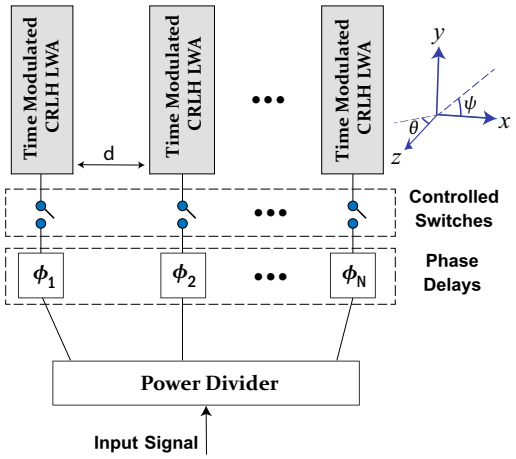


Fig. 9. Time-modulated parallel feeding with time modulated CRLH LWA.

4.3 Time-modulated parallel feeding with switch-enabled CRLH LWA

This configuration is envisaged based on a combination of the previous two cases. Specifically, as shown in Fig. 9 the plain LWA in each branch is replaced with a time-modulated LWA introduced in Section 4.1. The radiated signal into the 2D space for this configuration can be obtained in a similar fashion to (18) as

$$R(\theta,\psi,t)=\sum_{n=1}^{N}\frac{1}{\sqrt{N}}S(t)\Big(\sum_{n'=1}^{N'}e^{-\alpha(n'-1)p}U_{n'}^{'}(t)e^{j(n'-1)k_0p\sin\theta\sin\psi-j\sum_{l=1}^{n'}\beta_lp}\Big)U_n(t)e^{j(n-1)k_0d(\sin\theta\cos\psi-\sin\theta_0\cos\psi_0)}, \tag{22}$$

where $\theta\in[0,\pi/2]$ and $\psi\in[0,2\pi]$. Similar to the previous configuration, the switches $U_n(t)$ and $U_{n'}^{'}(t)$ are designed based on the set of solutions in (16) and (17). As a result, for the desired angles θ_0 and ψ_0, the received signal becomes

$$R(\theta_0,\psi_0,t)=\frac{\Delta t}{T_p}S(t), \tag{23}$$

while for every other angle the received signal is distorted as

$$R(\theta,\psi,t)=\frac{1}{\sqrt{N}}S(t)\sum_{m=-\infty}^{\infty}V'(t,m,N^{'},t_{n'}^{s},\Delta t_{n'},\theta,\psi)\sum_{m=-\infty}^{\infty}V(t,m,N,t_n^s,\Delta t_n,\theta,\psi), \tag{24}$$

where the V function is given in (21) and V' is defined by

$$V'(t,m,N',t_{n'}^{s},\Delta t_{n'},\theta,\psi)=\sum_{n'=1}^{N'}\Big(\frac{\sin\big(m\pi f_p\Delta t_{n'}\big)}{m\pi}e^{j2m\pi f_p(t-t_{n'}^{s}-\Delta t_{n'}/2)}\Big)e^{j(n'-1)k_0d\sin\theta\sin\psi-j\sum_{l=1}^{n'}\beta_lp}. \tag{25}$$

For this configuration, one can verify that the DM functionalities are implemented via two set of switches corresponding to that of the phased array and that of the LWAs.

5 NUMERICAL RESULTS

In this section, we use numerical simulations to characterize the performance of the proposed secure transmission schemes in Section 4 against the passive and active PHY attacks (see Section 2). We begin with the time-modulated

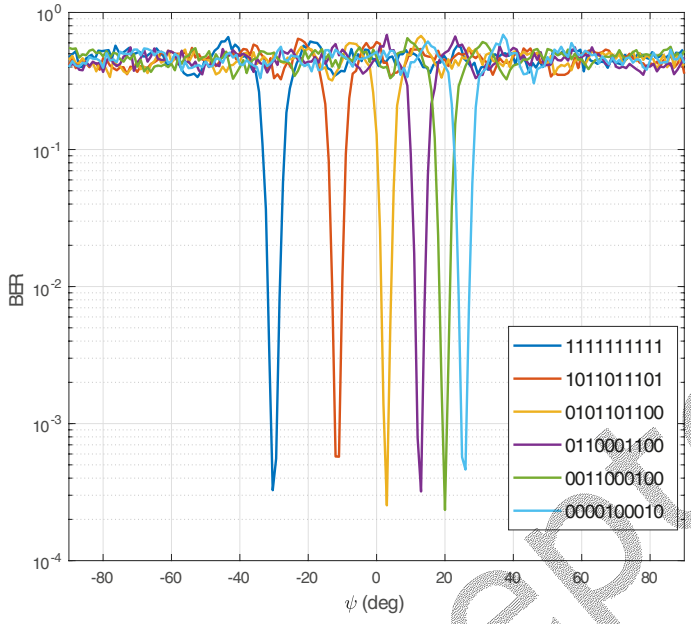


Fig. 10. Simulated BERs of the proposed time-modulated LWA in Section 4.1 with the corresponding input modes for the tunable unit cells.

CRLH LWA proposed in section 4.1 where the number of unit cells and the period is set to $N^{'} = 10$ and $p = 0.012$ m, respectively. The input signal is considered to be an OFDM signal with $K = 16$ subcarriers, carrier frequency $f_0 = 4.9$ GHz, $\Delta f = 15$ KHz, and QPSK modulation is used at each subcarrier to map the bits into complex symbols. Fig. 10 illustrates the BER simulations across the 1D space as a function of the angle between the Rx and Tx under the assumption of perfect synchronization and AWGN channel at an SNR of $E_b/N_0 = 8\ dB$. These assumptions make the current analysis a best-case scenario for the adversary as these may not be totally realizable depending on the underlying physical circumstances for adversary, which would subsequently deteriorate its decoding performance. Here E_b/N_0 is measured along the desired secure communication direction, and the noise power is assumed identical along every direction. Two choices of E_b/N_0 are equivalent to different distances between transmitter and receivers that include the legitimate one along the desired angle and potential eavesdroppers along all other directions. Fig. 10 shows that by tuning the constituent unit cells based on the input modes described in Section 3.1, the time-modulated LWA radiates the signal in a certain desired angle for which low BERs are achievable as the received signal is interference free. By deviating from this angle, on the other hand, the received signal is more and more corrupted which precludes a receiver from achieving decoding performances with high reliability.

Next, we consider a scenario where Tx, Rx and adversary are placed in a 2D space where Tx utilizes the proposed configurations proposed in Sections 4.2 and 4.3 for transmission. We first investigate the performance of the passive eavesdropping assuming the OFDM signal is being transmitted. Here, the OFDM carrier frequency is set to $f_0 = 4.9$ GHz and a tunable LWA, as described in Section 3.1, is used at each branch to enable beam scanning at a fixed frequency. The desired angles are set to $\theta_0 = 40°$ and $\psi_0 = 186°$. For the switches in each branch and

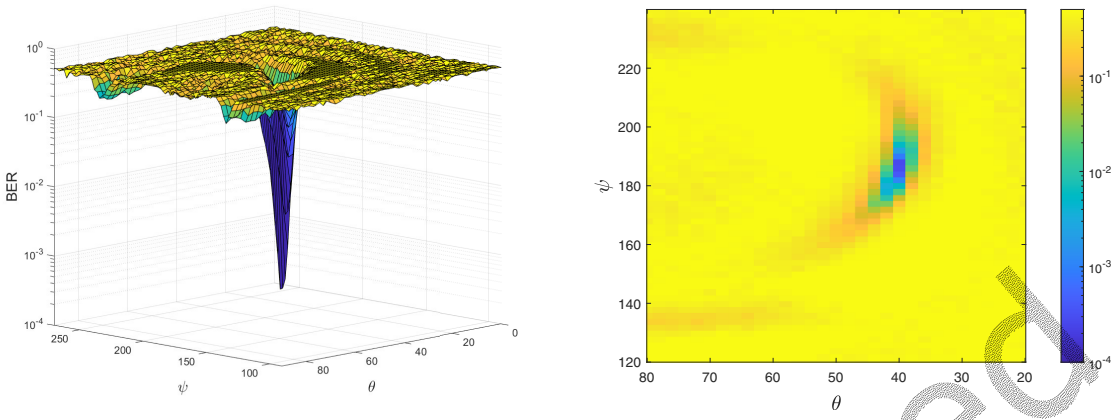


Fig. 11. BER performance of a receiver in 2D space when Tx is using time-modulated parallel feeding with plain CRLH LWA proposed in Section 4.2 for transmission. $N = 10$, $N^{'} = 10$.

the switches between unit cells, we have used identical on-time duration of $\Delta t_n/T_p = 1/N$ and $\Delta t_{n'}/T_p = 1/N^{'}$, respectively, where T_p is set to be T_o. The BER-based decoding performances are reported as a function of a receiver's spatial angles w.r.t. the Tx, and $E_b/N_0 = 8$ dB which is computed in a similar fashion to the case of Fig. 10. We present the results for the configuration Time-modulated parallel feeding with plain CRLH LWA in Figs. 11 and 12, which results in a 2D directional modulation scheme. By comparing Figs. 11 and 12, it is shown that the number of unit cells in each branch plays an important role towards achieving a BER performance with a narrow lobe. Moreover, Figs. 13 and 14 present the results obtained from the time-modulated parallel feeding with switch-enabled CRLH LWA configuration. In fact, for the same number of unit cells and branches, one can see that the latter scheme would result in much narrower BER lobe by employing the proposed time-modulated LWAs.

Next, we investigate the resilience of the proposed configurations against state-of-the-art PHY spoofing attacks as an instance of the active adversary scenario. To this end, we assume the adversary is equipped with resources to build a dataset out of the received signals and launch complicated data-driven attacks based on deep learning algorithms introduced in [21, 22]. These algorithms are powerful tools for extracting structural information from a given dataset when labels are not available (unsupervised), or finding a mapping function to the available labels (supervised). The labels in our case correspond to specific transmission parameters, i.e., subcarrier occupancy pattern (v), total number of subcarriers (K) and the subcarrier width Δf.

For supervised spoofing (SS) attacks, we consider two deep neural networks (DNNs) illustrated in Fig. 15 for estimating the transmission parameters. The input to each DNN is the concatenation of the real and imaginary parts corresponding to the samples of a received signal while the output is set to be estimated transmission parameter(s). Also, the architecture of each DNN is presented in Table 1. Regarding training, we minimize the l_2-loss between the true labels and output of each DNN using Adam optimizer [15] with a learning rate of 0.0001 for mini-batches of size 100.

The authors in [21] introduce unsupervised spoofing (US) attacks using the VAEs [16] which work based on the idea of variational inference. In fact, they show that by training a VAE on a dataset of NC-OFDM signals, important PHY characteristics can be inferred through the analysis of the latent variables. The basic idea of a US attack is that a DNN (encoder) is capable of capturing information from the NC-OFDM signals, which can be

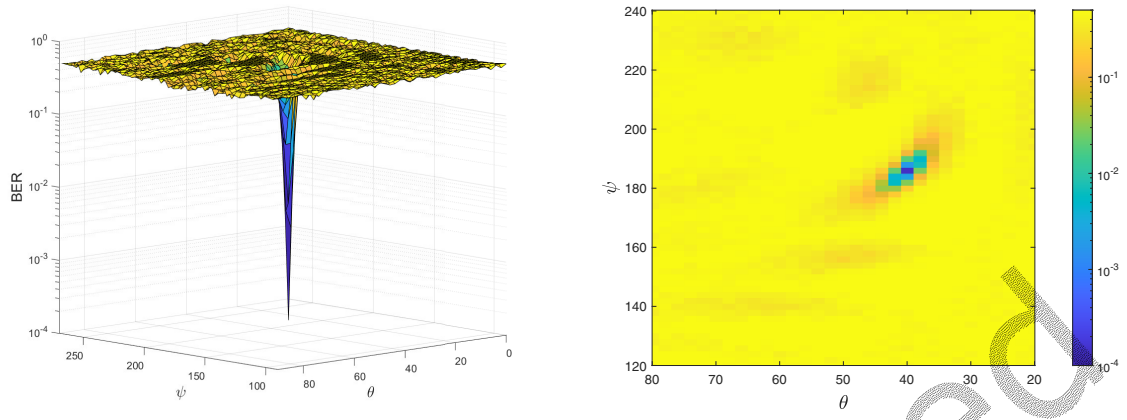


Fig. 12. BER performance of a receiver in 2D space when Tx is using time-modulated parallel feeding with plain CRLH LWA proposed in Section 4.2 for transmission. $N = 10$, $N^{'} = 20$.

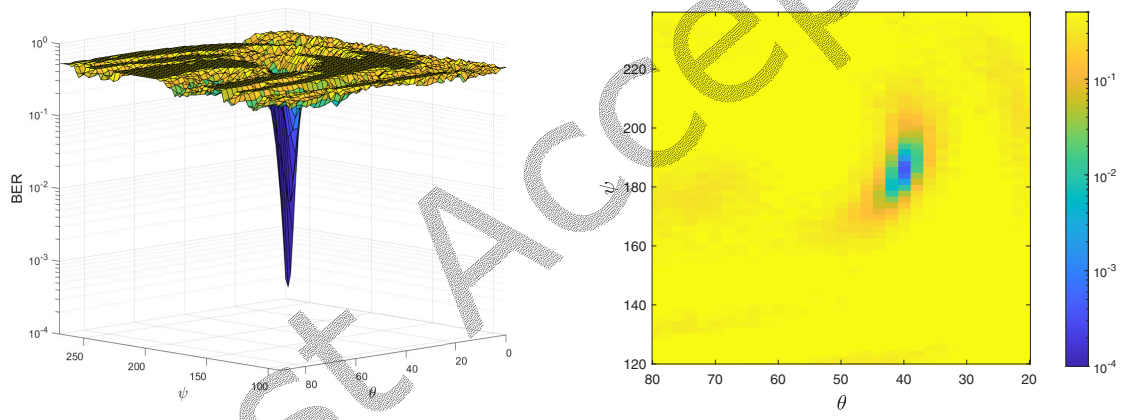


Fig. 13. Simulated BERs for the decoding performance of a receiver corresponding to the configuration time-modulated parallel feeding with switch-enabled CRLH LWA proposed in Section 4.3. $N = 10$, $N^{'} = 10$.

Table 1. Number of neurons in the hidden layers for the DNNs described in Fig. 15.

Hidden layer index	1	2	3	4
DNN 1	200	400	400	100
DNN 2	400	600	400	100

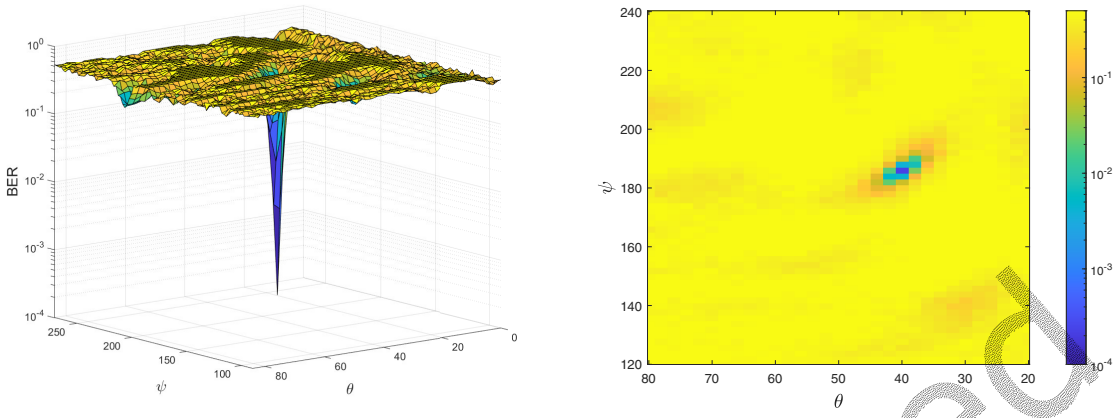


Fig. 14. Simulated BERs for the decoding performance of a receiver corresponding to the configuration time-modulated parallel feeding with switch-enabled CRLH LWA proposed in Section 4.3. $N = 10$, $N' = 20$.

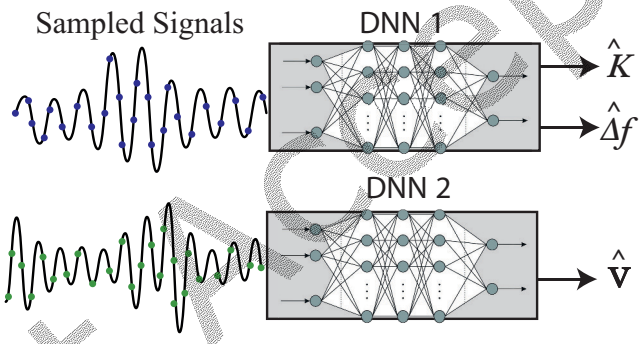


Fig. 15. Block diagrams of two DNNs used for estimating transmission parameters by the adversary.

used by a second DNN (decoder) to reconstruct the signal. This information is encoded in the fixed number of latent variables. A US attack first identifies those latent variables which are used by the decoder, and refers to them as informative latent variables. Then, it is shown in [21] that the number of informative latent variables is related to the total number of subcarriers K. Furthermore, through the latent traversal technique [7], the value of an informative latent variable is shown to be related to the amount of power in a certain subcarrier. As there is zero power associated with an inactive subcarrier, this procedure would lead to estimation of the subcarrier allocation pattern ($\mathbf{v}$).

In terms of specifics of the attack model, the transmission is assumed to take place over an NC-OFDM scheme, with $\Delta f \in \{15, 30, 45, 60\}$ KHz and $p_n \in [1, 2]$, utilizing QPSK modulation with random subcarrier occupancy pattern using the total number of subcarriers $K = 16$ and $K = 32$, which give rise to 2^{16} and 2^{32} distinct subcarrier occupancy patterns, respectively. The adversary overhears the transmissions at a certain *spoofing SNR* and builds up a dataset out of the received noisy signals, where 80 complex samples are collected from each signal. The size of the training and the test dataset is set to 2×10^6 and 25×10^4, respectively. Fig. 16 illustrates the spoofing

performance for several supervised and unsupervised learning algorithms when the adversary receives signal from different θ and ψ angles. The channel between the Tx and adversary is assumed to be a multi-path channel with amplitudes $\{1, 0.8, 0.6\}$ and delays $\{0, 2, 4\}\mu s$, and a Rayleigh flat-fading for both the Adversary-Rx and Tx-Rx channels. For the unsupervised cases, we assume the adversary is utilizing the VAE model to infer the total number of subcarriers and the corresponding latent variables for each subcarrier via latent traversal. During the test stage, it obtains the corresponding learned representation for a test signal and decides whether a subcarrier is active or inactive.

Here, we primarily focus on the configuration proposed in Section 4.3, and investigate the performance of deep learning-based PHY spoofing attacks for the case that $N = 10$ and $N' = 20$. Fig. 16 demonstrate the BER performance at Rx while decoding the spurious data sent by the adversary over a long range of SNR for the OFDM and NC-OFDM systems. As mentioned in Section 2, as the adversary's accuracy in estimating the transmission parameters improves, it can generate signals whose PHY characteristic is more similar to that of the Tx, and as a result the Rx will proceed with decoding the spurious data assuming the received signal is legitimate. Therefore, higher BERs here correspond to a transmission scheme which is more secure against PHY spoofing. For example, for the case of OFDM transmission the BER hits very small values as OFDM signals are particularly susceptible to PHY spoofing attacks. Firstly, we observe that for the case of OFDM signals, illustrated by dark blue curve, the adversary is able to infer the true transmission parameters, which results in the same BER performance as the baseline OFDM transmission. For the case of NC-OFDM systems, when the adversary receives signals at angles where signals are distorted in comparison to the desired angles, the corresponding PHY spoofing attack deteriorates. The θ and ψ angles corresponding to the adversary's location with respect to the Tx are denoted by ψ_A and θ_A here, respectively. Higher amounts of perturbance from the desired angle, is particularly shown to exacerbate the adversary's performance. Notably, we have observed that when the receiving angles, ψ_A and θ_A, have more than 7 degrees difference from the desired angles, ψ_0 and θ_0, the BER at the Rx is close to 0.5 which indicates the complete failure of such attacks. For smaller levels of degree differences, Fig. 16 demonstrates that the sophisticated deep learning-based spoofing attacks are affected at different levels by the proposed Tx architecture. Specifically, deviation from the desired received angles has much more detrimental effects on the performance of the US attack in comparison to the supervised one. This can be associated with the fact that unsupervised spoofing relies heavily on the structure of the received signals to find the subcarrier occupancy pattern. When the received signals are distorted due to the directional modulation functionality at the undesired angles, the resulting US spoofing performance is also substantially deteriorated. On the other hand, SS attacks show more resiliency against the variation from the desired received angles, although they rely on true labels for training which might not be easy to acquire for a malicious party in a real-world setting. Finally, Fig. 16 illustrates the US performance corresponding to the time-modulated parallel feeding with plain CRLH LWA architecture via the curve labeled as 'US*'. It is observed that this architecture has inferior security capabilities in comparison to the time-modulated parallel feeding with switch-enabled CRLH LWA structure proposed in Section 4.3.

6 CONCLUSIONS

We have proposed transmission architectures to enhance the physical layer security through the utilization of MTM-LWAs. Specifically, in the proposed configurations, the DM functionalities of the TMAs are realized in 1-D and 2-D spaces through the MTM-LWAs which have much lower complexity in comparison to the classic alternatives like phased arrays. Furthermore, we have investigated the resilience of these architectures against passive eavesdropping and active PHY spoofing attacks. For the former case, the TMAs with OFDM signals are considered while NC-OFDM transmission is employed for the latter scenario. In particular, we have assumed the adversary has access to state-of-the-art deep learning tools for PHY spoofing. We have shown as part of the numerical results that the proposed transmission schemes substantially enhance the physical layer security

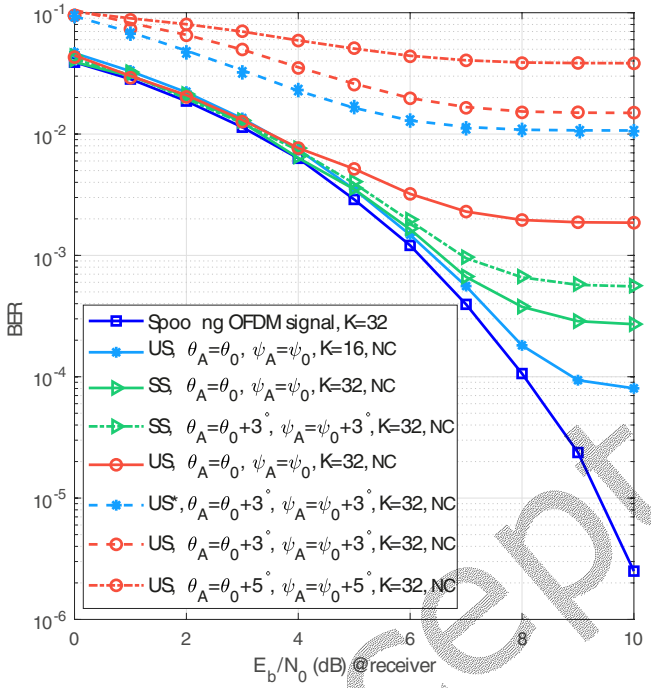


Fig. 16. BER at the Rx associated with the spurious data sent by the adversary. The adversary launches either a supervised spoofing (SS) or an unsupervised spoofing (US) attack. 'NC' refers to spoofing NC-OFDM signals. Also, the curve labeled as 'US*' corresponds to the time-modulated parallel feeding with plain CRLH LWA while the remaining ones relate to time-Modulated parallel feeding with switch-enabled CRLH LWA architecture.

through the generation of highly directive beams which cause substantial interference to the adversary's received signal even with small perturbation w.r.t. the desired angles.

ACKNOWLEDGMENTS

This work was supported by the National Science Foundation (NSF) under Grant ECCS-2028823 and in part by ECCS-1818478. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

REFERENCES

[1] 1998. *Planar and Circular Array Pattern Synthesis.* John Wiley & Sons, Ltd. 106–126 pages.
[2] 2005. *Radiated-Wave Applications.* John Wiley & Sons, Ltd, Chapter 6, 261–315. https://doi.org/10.1002/0471754323.ch6 arXiv:https://onlinelibrary.wiley.com/doi/pdf/10.1002/0471754323.ch6
[3] A. Babakhani, D. B. Rutledge, and A. Hajimiri. 2009. Near-field direct antenna modulation. *IEEE Microwave Magazine* 10, 1 (2009), 36–46. https://doi.org/10.1109/MMM.2008.930674
[4] P. Baccarelli, P. Burghignoli, F. Frezza, A. Galli, and P. Lampariello. 2003. Novel modal properties and relevant scanning behaviors of phased arrays of microstrip leaky-wave antennas. *IEEE Transactions on Antennas and Propagation* 51, 12 (2003), 3228–3238. https://doi.org/10.1109/TAP.2003.820962
[5] Bigthink. 2016. *Hacking the human heart.* http://bigthink.com/future-crimes/hacking-the-human-heart

[6] Buisnessinsider. 2015. *The most hackable cars on the road.* http://www.businessinsider.com/the-most-hackable-cars-on-the-road-today-2015-8

[7] Christopher P. Burgess, Irina Higgins, Arka Pal, Loïc Matthey, Nick Watters, Guillaume Desjardins, and Alexander Lerchner. 2018. Understanding disentangling in β-VAE. *CoRR* abs/1804.03599 (2018).

[8] C. Caloz and T. Itoh. 2004. Array factor approach of leaky-wave antennas and application to 1-D/2-D composite right/left-handed (CRLH) structures. *IEEE Microwave and Wireless Components Letters* 14, 6 (2004), 274–276. https://doi.org/10.1109/LMWC.2004.828009

[9] J. Schwarz D. Rohde. Aug. 2016. Narrowband Internet of Things. (Aug. 2016). Available: https://www.rohde-schwarz.com/us/applications/narrowband-internet-of-things-application-note_56280-314242.html/.

[10] Michael P Daly and Jennifer T Bernhard. 2009. Directional modulation technique for phased arrays. *IEEE Transactions on Antennas and Propagation* 57, 9 (2009), 2633–2640.

[11] Y. Ding, V. Fusco, J. Zhang, and W. Q. Wang. 2019. Time-Modulated OFDM Directional Modulation Transmitters. *IEEE Transactions on Vehicular Technology* 68, 8 (2019), 8249–8253. https://doi.org/10.1109/TVT.2019.2924543

[12] M. Hafez, M. Yusuf, T. Khattab, T. Elfouly, and H. Arslan. 2018. Secure Spatial Multiple Access Using Directional Modulation. *IEEE Transactions on Wireless Communications* 17, 1 (2018), 563–573. https://doi.org/10.1109/TWC.2017.2768419

[13] S. Hara and R. Prasad. 1997. Overview of multicarrier CDMA. *IEEE Communications Magazine* 35, 12 (1997), 126–133. https://doi.org/10.1109/35.642841

[14] David R. Jackson and Arthur A. Oliner. 2008. *Leaky-Wave Antennas.* John Wiley & Sons, Ltd, Chapter 7, 325–367. https://doi.org/10.1002/9780470294154.ch7 arXiv:https://onlinelibrary.wiley.com/doi/pdf/10.1002/9780470294154.ch7

[15] Diederik P. Kingma and Jimmy Ba. 2014. Adam: A Method for Stochastic Optimization. *CoRR* abs/1412.6980 (2014). http://dblp.uni-trier.de/db/journals/corr/corr1412.html#KingmaB14

[16] Diederik P. Kingma and Max Welling. 2014. Auto-Encoding Variational Bayes. In *ICLR*.

[17] Qun Li, Yonghong Zhang, and Chung-Tse Michael Wu. 2018. Noncontact Vital Sign Detection using 24GHz Two-Dimensional Frequency Scanning Metamaterial Leaky Wave Antenna Array. In *2018 IEEE/MTT-S International Microwave Symposium-IMS*. IEEE, 255–258.

[18] Chunchi Lu, Yichao Yuan, Chao-Hsiung Tseng, and Chung-Tse Michael Wu. 2019. Multi-target continuous-wave vital sign radar using 24 GHz metamaterial leaky wave antennas. In *2019 IEEE MTT-S International Microwave Biomedical Conference (IMBioC)*, Vol. 1. IEEE, 1–4.

[19] Lu Tan and Neng Wang. 2010. Future internet: The Internet of Things. In *2010 3rd International Conference on Advanced Computer Theory and Engineering(ICACTE)*, Vol. 5. V5–376–V5–380. https://doi.org/10.1109/ICACTE.2010.5579543

[20] Y. Luo, K. Qin, H. Ke, B. Xu, S. Xu, and G. Yang. 2021. Active Metamaterial Antenna With Beam Scanning Manipulation Based on a Digitally Modulated Array Factor Method. *IEEE Transactions on Antennas and Propagation* 69, 2 (2021), 1198–1203. https://doi.org/10.1109/TAP.2020.3010941

[21] A. Nooraiepour, W. U. Bajwa, and N. B. Mandayam. 2021. Learning-Aided Physical Layer Attacks Against Multicarrier Communications in IoT. *IEEE Transactions on Cognitive Communications and Networking* 7, 1 (2021), 239–254. https://doi.org/10.1109/TCCN.2020.2990657

[22] Alireza Nooraiepour, Kenza Hamidouche, Waheed U. Bajwa, and Narayan Mandayam. 2018. How Secure are Multicarrier Communication Systems Against Signal Exploitation Attacks?. In *MILCOM 2018 - 2018 IEEE Military Communications Conference (MILCOM)*. 201–206. https://doi.org/10.1109/MILCOM.2018.8599849

[23] A. Punchihewa, Q. Zhang, O. A. Dobre, C. Spooner, S. Rajan, and R. Inkol. 2010. On the Cyclostationarity of OFDM and Single Carrier Linearly Digitally Modulated Signals in Time Dispersive Channels: Theoretical Developments and Application. *IEEE Transactions on Wireless Communications* 9, 8 (August 2010), 2588–2599. https://doi.org/10.1109/TWC.2010.061510.091080

[24] B. Qiu, L. Wang, J. Xie, Z. Zhang, Y. Wang, and M. Tao. 2020. Multi-Beam Index Modulation With Cooperative Legitimate Users Schemes Based on Frequency Diverse Array. *IEEE Transactions on Vehicular Technology* 69, 10 (2020), 11028–11041. https://doi.org/10.1109/TVT.2020.3007003

[25] Rakesh Rajbanshi, Alexander M Wyglinski, and Gary J Minden. 2006. An efficient implementation of NC-OFDM transceivers for cognitive radios. In *1st International Conference on Cognitive Radio Oriented Wireless Networks and Communications*. 1–5.

[26] Sina Rezaei Aghdam, Alireza Nooraiepour, and Tolga M. Duman. 2019. An Overview of Physical Layer Security With Finite-Alphabet Signaling. *IEEE Communications Surveys Tutorials* 21, 2 (2019), 1829–1850. https://doi.org/10.1109/COMST.2018.2880421

[27] Mehdi Salarkaleji, Mohammad Ashraf Ali, and Chung-Tse Michael Wu. 2016. Two-dimensional full-hemisphere frequency scanning array based on metamaterial leaky wave antennas and feed networks. In *2016 IEEE MTT-S International Microwave Symposium (IMS)*. IEEE, 1–4.

[28] Mehdi Salarkaleji, Mohammadreza Eskandari, Jimmy Ching-Ming Chen, and Chung-Tse Michael Wu. 2017. Frequency and polarization-diversified linear sampling methods for microwave tomography and remote sensing using electromagnetic metamaterials. *Electronics* 6, 4 (2017), 85.

[29] T.M. Schmidl and D.C. Cox. 1997. Robust frequency and timing synchronization for OFDM. *IEEE Transactions on Communications* 45, 12 (1997), 1613–1621. https://doi.org/10.1109/26.650240

[30] F. Shu, T. Shen, L. Xu, Y. Qin, S. Wan, S. Jin, X. You, and J. Wang. 2020. Directional Modulation: A Physical-Layer Security Solution to B5G and Future Wireless Networks. *IEEE Network* 34, 2 (2020), 210–216. https://doi.org/10.1109/MNET.001.1900258

[31] Rashmi Sharan Sinha, Yiqiao Wei, and Seung-Hoon Hwang. 2017. A survey on LPWA technology: LoRa and NB-IoT. *ICT Express* (2017), 14 – 21. https://doi.org/10.1016/j.icte.2017.03.004

[32] Gokul Sridharan, Ratnesh Kumbhkar, Narayan B Mandayam, Ivan Seskar, and Sastry Kompella. 2016. Physical-layer security of NC-OFDM-based systems. In *Military Communications Conference (MILCOM)*. 1101–1106.

[33] Chung-Tse Michael Wu, Yuandan Dong, Jim S Sun, and Tatsuo Itoh. 2012. Ring-resonator-inspired power recycling scheme for gain-enhanced distributed amplifier-based CRLH-transmission line leaky wave antennas. *IEEE transactions on microwave theory and techniques* 60, 4 (2012), 1027–1037.

[34] L. Xiao, L. J. Greenstein, N. B. Mandayam, and W. Trappe. 2008. Using the physical layer for wireless authentication in time-variant channels. *IEEE Transactions on Wireless Communications* 7, 7 (2008), 2571–2579. https://doi.org/10.1109/TWC.2008.070194

[35] L. Xiao, L. J. Greenstein, N. B. Mandayam, and W. Trappe. 2009. Channel-based spoofing detection in frequency-selective rayleigh channels. *IEEE Transactions on Wireless Communications* 8, 12 (December 2009), 5948–5956. https://doi.org/10.1109/TWC.2009.12.081544

[36] L. Xiao, A. Reznik, W. Trappe, C. Ye, Y. Shah, and N. Mandayam. 2010. PHY-Authentication Protocol for Spoofing Detection in Wireless Networks. In *Proc. 2010 IEEE Global Telecommunications Conference GLOBECOM 2010*. 1–6. https://doi.org/10.1109/GLOCOM.2010.5683463

[37] Yichao Yuan, Chunchi Lu, Austin Ying-Kuang Chen, Chao-Hsiung Tseng, and Chung-Tse Michael Wu. 2019. Multi-target concurrent vital sign and location detection using metamaterial-integrated self-injection-locked quadrature radar sensor. *IEEE Transactions on Microwave Theory and Techniques* 67, 12 (2019), 5429–5437.