M3A: Multipath Multicarrier Misinformation to Adversaries

Zhecun Liu[†], Keerthi Priya Dasala[†], Di Mu[‡], Rahman Doost-Mohammady[†], and Edward W. Knightly[†]

[†]Rice University, Houston, TX

[‡]Skylark Wireless LLC, Houston, TX

{zl83, kd32}@rice.edu, dmu@mailfence.com, {doost, knightly}@rice.edu

ABSTRACT

Wireless channels are vulnerable to eavesdroppers due to their broadcast nature. One approach to thwart an eavesdropper (Eve) is to decrease her SNR, e.g., by reducing the signal in her direction. Unfortunately, such methods are vulnerable to (1) a highly directional Eve that can increase her received signal strength and (2) Eve that is close to the receiver, Bob, or close to the transmitter, Alice. In this paper, we design and experimentally evaluate Multipath Multicarrier Misinformation to Adversaries (M3A), a system for Alice to send data to Bob while simultaneously sending misinformation to Eve. Our approach does not require knowledge of Eve's channel or location and, with multipath channels, randomly transforms Eve's symbols even if Eve is located one wavelength-scale distance from Bob (approximately 10 cm) or if Eve is located between Alice and Bob in their direct path (Eve is approximately 1/3 closer to Alice). In particular, our approach is to move each of Eve's received symbols (over time and across subcarriers), to an independently random transformation as compared to Bob, without Alice or Bob knowing Eve's location or channel. We realize this by modulating Alice's per-subcarrier beamforming weights with an *i.i.d.* random binary sequence, as if Alice had a separate antenna array for each subcarrier, and could randomly turn antennas in each array on and off. We implement M3A on a real-time Massive MIMO testbed and show that M3A can increase Eve's bit error rate more than two hundredfold compared to beamforming, even if she is positioned approximately a wavelength away, whether above, below, or beside Bob. Finally, to ensure reliability at Bob, we show that with M3A, Bob's bit error rate is approximately an order of magnitude lower than achieved with prior work.

ACM MobiCom '23, October 2–6, 2023, Madrid, Spain

ACM ISBN 978-1-4503-9990-6/23/10…$15.00

https://doi.org/10.1145/3570361.3613282

CCS CONCEPTS

• **Security and privacy → Mobile and wireless security**;
• **Hardware → Wireless devices**.

KEYWORDS

Wireless Security; Eavesdropping; Physical Layer Security; Secure Beamforming; Artificial Fast Fading; Massive MIMO

ACM Reference Format:

Zhecun Liu, Keerthi Priya Dasala, Di Mu, Rahman Doost-Mohammady, and Edward W. Knightly. 2023. M3A: Multipath Multicarrier Misinformation to Adversaries. In *The 29th Annual International Conference on Mobile Computing and Networking (ACM MobiCom '23), October 2–6, 2023, Madrid, Spain.* ACM, New York, NY, USA, 15 pages. https://doi.org/10.1145/3570361.3613282

1 INTRODUCTION

Data confidentiality, restricting data access to intended users only [1], is often compromised by dedicated adversaries in wireless networks. Such instances have been identified across a wide range of real-world deployments: by intercepting sensitive information over-the-air, an eavesdropper Eve may snoop on conversations from Voice over LTE (VoLTE) [2], localize and track legitimate users by stealth [3, 4], and hijack health-monitoring Internet-of-Things devices to perpetrate patient's mistreatment [5]. While data encryption has proven useful for mitigating eavesdropping attacks, it faces several limitations. For example, Eve could initiate a side-channel attack by exploiting flaws in protocol implementation, leading to the exposure of the private keys established between trusting users [2]. Likewise, for wireless networks with end devices that have restricted processing capabilities (such as sensor and RFID networks), supporting encryption and decryption may be prohibitive [1, 6, 7]. Complementary to the computational hardness offered by encryption at upper-layers, physical-layer (PHY) security have been also proposed to thwart eavesdropping by relying on Eve having a degraded channel compared to Bob [7–9]. Unfortunately,

such methods can be vulnerable to both Eve's efforts to enhance her signal (e.g., by moving closer to Bob or Alice, or by increasing her receive beamforming gain), and to Eve's improved decoding [10].

In this paper, we design, implement, and experimentally evaluate Multipath Multicarrier Misinformation to Adversaries (M3A). The main goal behind M3A is for Eve to receive random bits (misinformation) controlled by Alice, rather than receiving a degraded version of the same information intended for Bob. Our solution targets misinformation to Eve even if Eve is in a wavelength-scale distance from Bob or if Eve is closer to Alice than Bob is, previously impossible scenarios to secure. Thus, our approach exploits (and requires) a rich multipath channel in which channels decorrelate in space, yet need not change in time. We consider that Alice will use N_t transmit antenna MIMO and multicarrier OFDM or OFDMA transmission. In M3A, as with every standard (e.g., [11, 12]), Alice will send known PHY preambles for Bob's channel estimation and equalization. We consider that Eve also knows the standard and preambles, and can observe this procedure and all communication. In this context, M3A proactively modifies the waveform of each subcarrier received at Eve by altering its amplitude and phase, aiming to move the data symbols carried by subcarriers to random positions, with randomness over both subcarriers and time. To do so, for each subcarrier and each symbol, Alice creates an independent and identically distributed (*i.i.d.*) random binary $\{0, 1\}$ N_t-bit mask, i.e., a bit sequence that is random over both subcarriers *and* time. We use the masks to modulate each antenna's beamformed symbol so that it has the net effect of turning a subset of the N_t antennas off, yet differently for each subcarrier. We show that this operation at Alice will randomize Eve's symbols. For example, for 16-QAM, Eve is ideally equally likely to receive any of the 16 symbols for any symbol transmitted by Alice, and Eve is not aided by knowledge of the standard or training symbols sent in the preamble.

What about Bob? How can Bob decode data without distortion and without knowing Alice's random binary sequence? Our approach is to keep Bob un-modified and unaware of Alice's operations, and for Alice to help Bob without giving away the "secret" transformation that provides misinformation at Eve. In particular, we present two novel methods for Alice to calculate and update each subcarrier's precoder as a function of time in a way that trades Alice's computational complexity for Bob's bit error rate (reliability), and neither of which reveals the secret transformation to Eve, hence not compromising the ability to send misinformation. The first is based on the Maximum Ratio Transmission (MRT) principle and maximizes the reliability at Bob regardless of computational overhead. The second method is based on the principle of Channel Inversion and reduces Alice's computational complexity, yet also increases Bob's bit error rate.

Finally, we build a real-time and end-to-end time-division-duplex (TDD) network to demonstrate M3A by using a Massive MIMO (MaMIMO) testbed. Our data communication results show that, compared to conjugate beamforming (BF), M3A increases Eve's Bit Error Rate (BER) up to more than two hundredfold (with the median approximately as 40×). Our results further show that the security benefit of M3A is retained, even when Bob and Eve are separated by a wavelength-scale distance in both horizontal and vertical directions, with Eve's median BER increased by more than 100×. While conveying Eve a stream of misinformation, M3A ensures Bob closely matches the BER of an unprotected receiver at various channel conditions, with median BER degradation less than 4× compared to BF.

The remainder of this paper is organized as follows. §2 reviews related work. §3 describes our threat model. §4 introduces the design principles of M3A and its variant. §5 describes M3A's implementation on the testbed. §6 presents experimental evaluations. §7 discusses some current limitations. §8 concludes the paper.

2 RELATED WORK

To the best of our knowledge, M3A is the first end-to-end multicarrier system that can thwart eavesdroppers even if they are a wavelength-scale distance from Bob or closer to Alice than Bob. Nonetheless, various prior studies are related to M3A in terms of both the problem and solution.

Energy Leakage Suppression. One method to increase Eve's decoding errors is to reduce her receive energy. While directional transmission such as adaptive beamforming (e.g., in 802.11n/ac) maximizes the SNR towards Bob, it does not proactively reduce that of Eve. Thus, Eve can compromise the confidentiality of beamforming via increased receive beamforming gain or by moving closer to Bob. References [13–16] studied optimization-based beamforming to minimize leaked SNR at Eve. A central premise is that the knowledge of Eve's angle position or Channel State Information (CSI), either statistical or exact, is available to Alice. In contrast, M3A does not require the CSI or angular position of Eve. Moreover, we demonstrate that even if Eve is closer to Alice than Bob is to Alice, Eve still receives random signals.

Directional Modulation Security Schemes. Directional modulation (DM) is a free-space method that targets to move constellations randomly in the I-Q plane for angles (directions) that are away from Bob [17–30]. However, a critical assumption in this body of work is that the algorithms are developed based on the narrowband transmission over free-space with Eve angularly away from Bob. Also, validated

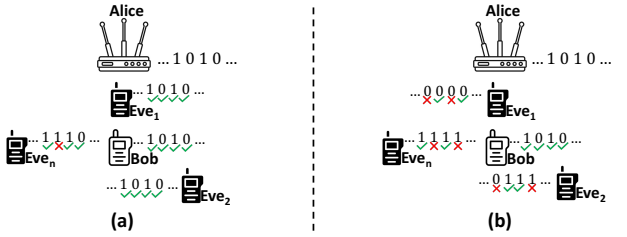


Figure 1: Threat model of M3A. (a) An ineffective protection: there exists Eve(s) correctly decoding bits with high probability; (b) M3A: Eves' decoding performance degrades while the bit-stream integrity at Bob is maintained.

experimentally by [18, 19, 25, 27, 29, 30], DM forces high decoding errors at Eve *only* when she is significantly separated from Bob in angle. Differently, M3A transcends the requirement of free-space modeling, operates with OFDM, and is not confined to physical directivity against eavesdropping.

Antenna Subset Modulation [22] is a DM method to move Eve's symbols by turning off random subsets of antennas. While our use of random binary masks is inspired by [22], in contrast to our work, common to the DM class, the security features of [22] are realized only in free-space propagation with a single-carrier. Moreover, the validation of [22] was limited to simulations and no over-the-air experiments were performed.

Non-directional Security Schemes. Multiple works have recognized the benefit of multipath channel de-correlation in protecting confidential messages. Efforts have initially been focused on secret keys generation. E.g., [31] demonstrated a key rate of 1 bps via the reciprocity of CSI between Alice and Bob, which got boosted to 3-18 kbps in [32] via cooperative jamming. Later, to secure WiFi transmissions, [33] built an 802.11ac-compliant scheme by sending streams of Additive Noise (AN). Lastly, [34] secured RFID signals by broadcasting random waveforms. Without relying on the directionality, these schemes have shown to be robust at a wavelength-scale proximity. However, the achieved rates in [31, 32] are too low to support data traffic. [34] is limited to analog backscatter communications. Finally, unlike [33], M3A aims at randomly moving Eve's constellations without AN, a key feature since the introduction of tools to guess and remove random AN [10]. Moreover, [33] does not address OFDM transmission, a crucial part of our formulation.

3 THREAT MODEL

As shown in Fig.1(a), we consider a situation where the transmitter Alice has an array of N_t transmit chains, and the intended user (named Bob) has a single receive chain. Within Alice's coverage range, there exist single antenna non-colluding adversaries named Eve, that have the malicious intent of eavesdropping on the confidential message bits sent from Alice to Bob. How adversaries utilize intercepted bits is beyond our scope.[1] Each Eve is equipped with a single receive chain, and may occupy any location with respect to Alice and Bob. To avoid exposing her presence, Eve doesn't transmit over-the-air (OTA) signals. Consequently, Alice cannot detect Eve's presence. We assume that Eve has the ability to intercept and then decode the sent baseband signals, because Eve has prior knowledge about Alice's signaling scheme (e.g., modulation format and parameters, time-frequency window) and the hardware that satisfies system requirements (e.g., sufficient sampling rate, CFO/SFO compensation).

Within the scope of this work, we employ reciprocity-based channel calibration (see §5.1 for details) for the purpose of CSIT (CSI at Transmitter) acquisition at Alice without any channel estimation feedback from Bob. After acquiring the CSIT, Alice sends physical-layer preambles in the downlink direction. We assume that the preambles are known, hence Bob can acquire his CSIR (CSI at Receiver) for the Alice-Bob channel, and each Eve can acquire the same for an Alice-Eve channel. Note that the preambles are not being broadcasted but rather beamformed towards Bob, adapting the concept of the Demodulation Reference Signal (DM-RS) introduced by the LTE/NR standard [12, 38]. Finally, we assume Eves are not colluding and that each Eve performs the same maximum likelihood decoding strategy as Bob, instead of using data-driven based counter-mechanisms against M3A. As discussed in §4.2, this is justified because M3A is a transmitter-side solution that is transparent to a receiver (i.e., Bob or Eve).

4 M3A DESIGN

In this section, we describe the design of M3A. Leveraging multiple transmit antennas, depicted in Fig.1(b), M3A achieve two goals simultaneously: (1) thwart Eves within Alice's range from decoding bits with a high probability of success (§4.1) and (2) maintain reliability at Bob with low BER (§4.2).

4.1 Sending Misinformation to Eve

Here, we describe the baseband realization of M3A to send misinformation. We begin by presenting the problem setup and a primer on BF's vulnerability to eavesdropping.

4.1.1 BF Vulnerability. We consider Alice operating in TDD mode, with each frame consisting of N_{sl} downlink transmission slots, where each slot is occupied by an OFDM symbol. Letting $s(n,k)$ be the constellation modulated onto the kth subcarrier in the nth OFDM symbol. With Alice employing a N_t transmit antenna MIMO, we use a length-N_t column vector $\boldsymbol{w}_a(n,k)$ to denote the precoder designed for $s(n,k)$. It

[1] Studies showed that Eve can initiate chosen-ciphertext attacks [35], man-in-the-middle DoS attack [36], and infer user's CSI reports from WLAN [37], irrespective of whether the bits are encrypted or unencrypted.

follows that the beamformed signal vector $\boldsymbol{x}(n,k)$ intended for Bob is expressed as:

$$\boldsymbol{x}(n,k) = s(n,k) \cdot \boldsymbol{w}_a(n,k). \tag{1}$$

Assuming the availability of *perfect CSIT*, i.e., the error-free downlink Alice-Bob channel vector $\boldsymbol{h}_{ab}(n,k)$, Alice transmits $s(n,k)$ to Bob using conjugate BF. Mathematically, it requires the precoder to be set in form of

$$\boldsymbol{w}_a(n,k) = \alpha(n,k) \cdot \boldsymbol{h}_{ab}(n,k), \tag{2}$$

where $\alpha(n,k)$ is a real scalar used to meet the per-antenna power constraint, reflecting that each transmit radio has its own independent RF front-end. Specifically, we have $\alpha(n,k) = 1/\|\boldsymbol{h}_{ab}(n,k)\|_\infty$, with the operator $\|\cdot\|_\infty$ denoting the infinity norm (the maximum row sum) of a matrix. This ensures at least one antenna transmits at maximum power, while the per-terminal transmission energy optimality is still met [39, 40]. Furthermore, by assuming the *per-frame based CSIT update rate*, the channel $\boldsymbol{h}_{ab}(n,k)$ estimated by Alice remains constant during $n = 1,\ldots,N_{sl}$. Thus, in this subsection, for $\boldsymbol{h}_{ab}(n,k)$ and $\alpha(n,k)$, we may drop their dependencies on the symbol index n.

The signal received by Eve in the kth subchannel during slot n is given by

$$y_e(n,k) = \left\langle \boldsymbol{h}_{ae}(n,k), \boldsymbol{x}(n,k) \right\rangle + v(n,k) \quad n = 1,\ldots,N_{sl}, \tag{3}$$

where $\langle\cdot,\cdot\rangle$ represents the complex inner product operation, $\boldsymbol{h}_{ae}(n,k)$ is the downlink channel vector, and $v(n,k)$ an additive noise term. From Eq. (1-3), we define the *effective channel* from Alice to Eve as:

$$\begin{aligned} h_{ae}^{\text{eff}}(n,k) &= \left\langle \boldsymbol{h}_{ae}(n,k), \boldsymbol{w}_a(n,k) \right\rangle \\ &= \alpha(k) \cdot \left\langle \boldsymbol{h}_{ae}(n,k), \boldsymbol{h}_{ab}(k) \right\rangle \\ &= \alpha(k) \cdot \left\langle \boldsymbol{h}_{ae}(k), \boldsymbol{h}_{ab}(k) \right\rangle, \end{aligned} \tag{4}$$

where the last equality is due to the fact that N_{sl} (effectively the frame length) is usually engineered to be less than a coherence interval, so that $\boldsymbol{h}_{ae}(n,k)$ *experienced by Eve* can approximately be regarded as constant throughout a frame. Consequently, the effective channel becomes independent of slot n. Now based on Eq. (3), Eve's received preamble signals can be rewritten as follows:

$$y_e(1,k) = h_{ae}^{\text{eff}}(k) \cdot s(1,k) + v(1,k). \tag{5}$$

Recalling our threat model, Eve already has knowledge of preamble symbols in the first slot (i.e., $s(n,k)$ for $n = 1$). Therefore, she can derive her CSIR for each subchannel $h_{ae}^{\text{eff}}(k)$ and perform one-tap equalization to detect the remaining data-carrying OFDM symbols, starting from $n = 2$. This suggests the vulnerability of BF: *Eve can eavesdrop up to the limits of Eve's receive directivity gains and noise floor, after equalizing out the effective channel term using her CSIR.*

4.1.2 M3A Precoding. How does M3A provide multicarrier misinformation? We design Alice's kth subchannel precoder applied in slot n to be[2]

$$\widetilde{\boldsymbol{w}}_a(n,k) = \left(\alpha(k) \cdot \boldsymbol{h}_{ab}(k)\right) \circ \boldsymbol{b}(n,k), \tag{6}$$

where $\boldsymbol{b}(n,k)$ is the associated *binary mask*, an *i.i.d.* N_t-dimensional random vector containing elements of {0,1}. In M3A, we still let Alice use Eq. (1) to generate beamformed signal, except now using $\widetilde{\boldsymbol{w}}_a(n,k)$. Comparing Eq. (6) and (2), it can be observed that if, for example, the first element in $\boldsymbol{b}(n,k)$ is set to zero, it emulates the effect of switching off the first transmit antenna specifically for subcarrier k in slot n. For simplicity, we assume a *fixed* value M_t number of antennas are turned on for each subcarrier, i.e., there exists M_t ones in each $\boldsymbol{b}(n,k)$, and M_t needs to be *strictly less than* N_t. Consequently, the effective Alice-Eve channel is:

$$\begin{aligned} h_{ae}^{\text{eff}}(n,k) &= \left\langle \boldsymbol{h}_{ae}(n,k), \widetilde{\boldsymbol{w}}_a(n,k) \right\rangle \\ &= \alpha(k) \cdot \left\langle \boldsymbol{h}_{ae}(k), \boldsymbol{h}_{ab}(k) \circ \boldsymbol{b}(n,k) \right\rangle \quad n = 1,\ldots,N_{sl}, \end{aligned} \tag{7}$$

which takes random values depending on the realization of downlink Alice-Bob and Alice-Eve channels, as well as the random binary mask $\boldsymbol{b}(n,k)$. Evidently, $h_{ae}^{\text{eff}}(n,k)$ varies with respect to slot index n, even when the downlink channels do not. This implies that Eve sees a *random per-symbol fading channel* which is independent to the choice of modulation order. As a result, using Eve's CSIR acquired from $n = 1$ and ignoring a colored noise term, her post-equalized data-carrying constellations equal to

$$\hat{s}_E(n,k) = \left[h_{ae}^{\text{eff}}(n,k) \,/\, h_{ae}^{\text{eff}}(1,k)\right] \cdot s(n,k), n = 2,\ldots,N_{sl}, \tag{8}$$

from which a random transformation is defined from $s(n,k)$ to $\hat{s}_E(n,k)$, which leads to misinformation at Eve. *Regardless of signal strength at Eve (including stronger than Bob's), Eve still cannot effectively utilize her CSIR to decode constellations $s(n,k)$ accurately.*

4.1.3 Multicarrier Security. How does M3A prevent Eve from reversing misinformation through knowledge of OFDM parameters? In each OFDM symbols, pilot subcarriers are employed to estimate and correct phase noise [41, 42]. Nonetheless, in the context of M3A, these pilots' positions and values could be exploited by Eve as well to eliminate the random transformation in Eq. (8). To elaborate on this vulnerability, consider a pilot indexed by j and an adjacent data subcarrier at $j+1$. Referring back to Eq. (7), because of potentially strong subchannel correlation, the two channels $\boldsymbol{h}_{ae}(n,j)$ and $\boldsymbol{h}_{ae}(n,j+1)$ exhibit high similarity when they lie within the coherence bandwidth, and so do the estimated quantities $\boldsymbol{h}_{ab}(n,j)$ and $\boldsymbol{h}_{ab}(n,j+1)$.[3] Next, suppose two subcarriers

[2]The operation $\boldsymbol{a} \circ \boldsymbol{b}$ denotes element-wise product of two vectors.

[3]Adjacent subcarriers may even share the same CSIT (e.g., 802.11ac, band AMC in LTE) to reduce traffic overhead.

both choose the same set of antennas, i.e., the generated binary masks $\boldsymbol{b}(n,j) = \boldsymbol{b}(n,j+1)$; consequently, the two effective channels $h_{ae}^{\text{eff}}(n,j)$ and $h_{ae}^{\text{eff}}(n,j+1)$ experienced at Eve would be as well similar. *This offers Eve a chance to compare received and expected pilot subcarriers, thereby reversing the per-symbol fading effect imposed by M3A.*

Instead, leveraging multiple digital basebands, M3A generates binary masks *independently across subcarriers,* thereby emulating that antennas have been chosen independently for each subcarrier. This mitigates Eve making inferences across subcarriers within the coherence bandwidth. Notably, achieving subcarrier-independent switching is *not* feasible using physical switches, as they typically function as a post-IFFT module.

4.1.4 Wavelength Proximity Protection. How does M3A thwart Eves located at wavelength-scale distances to Bob? Additional to the use of random binary masking, in order to confuse Eve located only a wavelength-scale distance from Bob, it requires to have $\boldsymbol{h}_{ab}(n,k)$ and $\boldsymbol{h}_{ae}(n,k)$ to be statistically independent. Otherwise, due to the strong correlation between $\boldsymbol{h}_{ae}(n,k)$ and $\boldsymbol{h}_{ab}(n,k)$, even the per-symbol fading induced by random antenna switching deteriorates into a coherent beamformed transmission at Eve. Fortunately, due to the rich multipath characteristics, a typical indoor environment can provide sufficient degree of channel de-correlation in unit of wavelength [31, 43]. *Spatial channel de-correlation in rich multipath propagation environments is the key property for confusing Eve, even if she is a wavelength-scale distance away from Bob, or even in front of Bob. Such scenarios cannot be secured by our method in free-space.*

Finally, can Alice also use non-binary masks to confuse Eve? Not only is the binary mask simpler, but more importantly, it allows M3A conjugate beamforming towards Bob. In cases where a random subset of antennas is selected and non-binary masks are used, Alice may assign a small (large) beam weight toward a strong (weak) channel. This could significantly degrade Bob's SNR, hence his decoding performance.

4.2 Reliability at Bob

The next goal of M3A is to let Bob detect $s(n,k)$ reliably even when Eve receives misinformation. Similar to Eq. (8), Bob's post-equalized data-carrying constellations is:

$$\hat{s}_B(n,k) = \left[h_{ab}^{\text{eff}}(n,k)\,/\,h_{ab}^{\text{eff}}(1,k)\right]\cdot s(n,k), n = 2,\ldots,N_{sl}. \quad (9)$$

We claim that the *fading term* (the ratio) in Eq. (9) possesses the following properties: (P1) it does not equal 1 even under perfect CSIT and a fixed sized antenna subset, hence must be equalized out for any n,k; (P2) it varies with respect to symbol index n, hence Bob cannot effectively equalize via the observed preamble; (P3) it is unknown a priori, hence needs real-time computing. Indeed, similar to Eq. (6), the raw effective Alice-Bob channel can be evaluated as:

$$\begin{aligned} h_{ab}^{\text{eff}}(n,k) &= \left\langle \boldsymbol{h}_{ab}(n,k), \widetilde{\boldsymbol{w}}_a(n,k)\right\rangle \\ &= \alpha(k)\cdot\left\langle \boldsymbol{h}_{ab}(k), \boldsymbol{h}_{ab}(k)\circ\boldsymbol{b}(n,k)\right\rangle \\ &= \alpha(k)\cdot\|\boldsymbol{h}_{ab}(k)\circ\boldsymbol{b}(n,k)\|^2 \quad n=1,\ldots,N_{sl}. \end{aligned} \quad (10)$$

Combining with Eq. (9), we obtain

$$\hat{s}_B(n,k) = \left[\frac{\|\boldsymbol{h}_{ab}(k)\circ\boldsymbol{b}(n,k)\|^2}{\|\boldsymbol{h}_{ab}(k)\circ\boldsymbol{b}(1,k)\|^2}\right]\cdot s(n,k) \quad n=2,\ldots,N_{sl},$$

from which we see (P1) holds due to different channel gains across transmit-receive (Tx-Rx) antenna pairs by multipath effect (measured SNR difference across Tx-Rx pairs can reach up to 40 dB [40]); (P2) holds due to randomly chosen $\boldsymbol{b}(n,k)$ per-symbol time; and (P3) holds due to randomly realized $\boldsymbol{h}_{ab}(k)$. Also, letting Bob compute the fading term directly will require exchanging binary mask $\boldsymbol{b}(n,k)$ with Bob at the PHY layer, which causes significant overhead (e.g., by adopting a mask-then-data alternating pattern), not to mention the need for an authenticated and confidential channel to ensure Eve doesn't intercept it.

Instead, *M3A keeps Bob's OFDM reception pipeline unmodified, and lets Alice help Bob pre-cancel the fading term without giving away the secret transformation to Eve.* Below, we present two novel methods to calculate and update each precoder $\widetilde{\boldsymbol{w}}_a(n,k)$ using the real-time PHY layer metrics that are available *only at Alice.* Specifically, those metrics are used to adjust $h_{ab}^{\text{eff}}(n,k)$ perceived at Bob, such that it becomes time-invariant within a frame.

4.2.1 MRT-based Technique. M3A dynamically changes the precoder values on a *per-symbol* basis. Analogous to MRT, Alice uses metrics $\boldsymbol{h}_{ab}(k)$ and $\boldsymbol{b}(n,k)$ to scale the transmitted signals on each transmit antenna proportional to conjugate channel $\boldsymbol{h}_{ab}(k)^*$, where operator * denotes the complex conjugate operation. First, Alice calculates $h_{ab}^{\text{eff}}(n,k)$ for each slot n via Eq. (10) based on the frame's CSIT and the masks $\boldsymbol{b}(n,k)$. Second, for each n, Alice normalizes the precoder $\widetilde{\boldsymbol{w}}_a(n,k)$ in Eq. (6) by $h_{ab}^{\text{eff}}(n,k)$, in order to average out different effective channel gains. Third, this normalized precoder is multiplied with the minimum effective channel attained among all slots. The reason of doing so is to avoid clipping that may otherwise occur at each transmit radio. We name the first step as a procedure called h^{eff} *Calculation*, and the second plus third step the *Inter-Symbol Normalization.* Together, they can be represented as:

$$\widetilde{\boldsymbol{w}}_a^{mrt}(n,k) = \widetilde{\boldsymbol{w}}_a(n,k)\cdot\left(\min_n h_{ab}^{\text{eff}}(n,k)\,/\,h_{ab}^{\text{eff}}(n,k)\right) \quad \forall n,$$

from which we re-derive the effective Alice-Eve channel as:

$$\begin{aligned} h_{ae}^{\text{eff}}(n,k)^{\text{mrt}} &= \left\langle \boldsymbol{h}_{ae}(n,k), \widetilde{\boldsymbol{w}}_a^{mrt}(n,k) \right\rangle \\ &= \alpha(k) \cdot \left(\min_n h_{ab}^{\text{eff}}(n,k) / h_{ab}^{\text{eff}}(n,k) \right) \\ &\cdot \left\langle \boldsymbol{h}_{ae}(k), \boldsymbol{h}_{ab}(k) \circ \boldsymbol{b}(n,k) \right\rangle, \end{aligned} \tag{11}$$

in which the secret transformation imposed at Eve, i.e., the ratio term $[h_{ae}^{\text{eff}}(n,k)^{\text{mrt}} / h_{ae}^{\text{eff}}(1,k)^{\text{mrt}}]$, is not exposed and still vary in both frequency and time. Hence, it does not compromise Alice's goal to send misinformation and is independent to the modulation order of $s(n,k)$. In §4.2.3, we further show that the Alice-Bob effective channel is indeed a constant within a frame.

4.2.2 Channel Inversion Technique. Since the number of subcarriers and data slots (symbols) within each TDD frame can be large, the computational cost of the h^{eff} Calculation and Inter-Symbol Normalization can likewise be high. To this end, we propose a variant called M3A_{lc}, where the subscript stands for *low complexity*. For each transmit antenna, the idea is to *inject less (more) energy along a stronger (weaker) signal path*. Using this technique, the amplitude of the superimposed waveform at Bob is kept constant across slots (and its phase value also remains constant due to the perfect CSIT assumption), irrespective of the random antenna selection. M3A_{lc} realizes this procedure at digital baseband by performing *Per-Antenna Normalization*, defined as follows. For subcarrier k, denote the estimated Alice-Bob channel vector by $\boldsymbol{h}_{ab}(k) = [h_0, \ldots, h_{N_t-1}]$. Without loss of generality, suppose the channel gains are *ordered*, such that $|h_0| \geq |h_1| \geq \cdots \geq |h_{N_t-1}|$. First, per-antenna normalization calculates a scaling vector $\boldsymbol{c}(k) = [1/|h_0|^2, \ldots, 1/|h_{N_t-1}|^2]$, and then performs

$$\boldsymbol{h}_{ab}^{lc}(k) = \boldsymbol{c}(k) \circ \boldsymbol{h}_{ab}(k), \tag{12}$$

which is followed by the second step called the *Per-Subcarrier Normalization* (across all antennas), by multiplying a scalar $\alpha^{lc}(k) = 1/\|\boldsymbol{h}_{ab}^{lc}(k)\|_\infty = |h_{N_t-1}|$, so that the per-antenna power constraint is met. Finally, the kth precoder in M3A_{lc} is obtained from Eq. (6), which yields

$$\widetilde{\boldsymbol{w}}_a^{lc}(n,k) = \left(\alpha^{lc}(k) \cdot \boldsymbol{h}_{ab}^{lc}(k)\right) \circ \boldsymbol{b}(n,k). \tag{13}$$

Now based on Eq. (7) and Eq. (13), the resultant Alice-Eve effective channel is expressed as:

$$\begin{aligned} h_{ae}^{\text{eff}}(n,k)^{lc} &= \left\langle \boldsymbol{h}_{ae}(n,k), \widetilde{\boldsymbol{w}}_a^{lc}(n,k) \right\rangle \\ &= \alpha^{lc}(k) \cdot \left\langle \boldsymbol{h}_{ae}(k), \boldsymbol{h}_{ab}(k) \circ \boldsymbol{c}(k) \circ \boldsymbol{b}(n,k) \right\rangle, \end{aligned} \tag{14}$$

from which Eve still observes a per-symbol fading, and hence she still cannot detect data symbols of each subchannel coherently via estimated CSIR. In addition, we show that M3A_{lc} also ensures the Alice-Bob effective channel to be constant with respect to slot index n (§4.2.3).

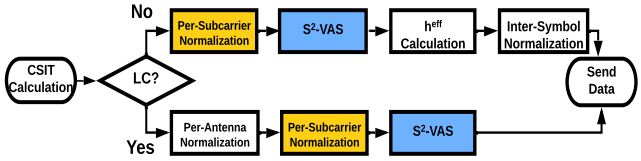


Figure 2: Data-processing flowchart of M3A and M3A_{lc}, where the block S^2-VAS represents the mechanism per-Symbol per-Subcarrier Virtual Antenna Switching.

We contrast the two techniques in Fig.2. First, Alice calculates the CSIT based on received uplink pilot and a channel calibration matrix, as discussed in §3. Next, Alice chooses a complexity mode to use. For M3A_{lc}, it sequentially does per-antenna normalization, per-subcarrier normalization, and per-symbol per-subcarrier virtual switching (i.e., element-wise multiplying the already-normalized vector with a binary mask) before sending precoded data. The h^{eff} calculation and inter-symbol normalization are required only for M3A, however the per-antenna normalization is no longer required. Both techniques cancel unwanted per-symbol fading at Bob adaptively by using real physical channel measurement.

4.2.3 Reliability Comparison. We compare the reliability performance between M3A and M3A_{lc} formally in the proposition below and provide its proof in Appendix A.

Proposition. *Consider vector $\boldsymbol{h}_{ab}(k) = [h_0, \ldots, h_{N_t-1}]$, ordered such that $|h_0| \geq |h_1| \geq \cdots \geq |h_{N_t-1}|$. In a TDD frame containing N_{sl} downlink slots, Alice lets each subcarrier virtually selects M_t out of N_t antennas, resulting in the raw effective channel $h_{ab}^{eff}(n,k)$ for each slot n. Both M3A and M3A_{lc} yield a time-invariant effective Alice-Bob channel, particularly*

- *in M3A_{lc}, we have $h_{ab}^{eff}(k)^{lc} = M_t|h_{N_t-1}|$;*
- *in M3A, we have $h_{ab}^{eff}(k) = \min_{n=1,\ldots,N_{sl}} h_{ab}^{eff}(n,k)$, where a diversity gain of M_t can be achieved.*

We observe that both techniques realize time-invariant effective channel, independent to the modulation order of $s(n,k)$. Next, in the case of M3A_{lc}, we observe that Bob's SNR suffers whenever the gain of the weakest Tx-Rx pair $|h_{N_t-1}|$ falls into a deep fade. This stems from emulating channel inversion, by which significantly more transmit power is needed when channel quality is poor; subjected to limited power budgets, the resultant SNR at Bob may become insufficient. On the other hand, M3A provides greater resilience against multipath fading, due to its higher diversity gain through M_t-antenna conjugate BF. We empirically validate and compare their performance in §6.1.

4.2.4 Computational Complexity. As depicted in Fig.2, for both schemes, virtual antenna switching and per-subcarrier normalization are two common modules. Given N_{sl} TDD

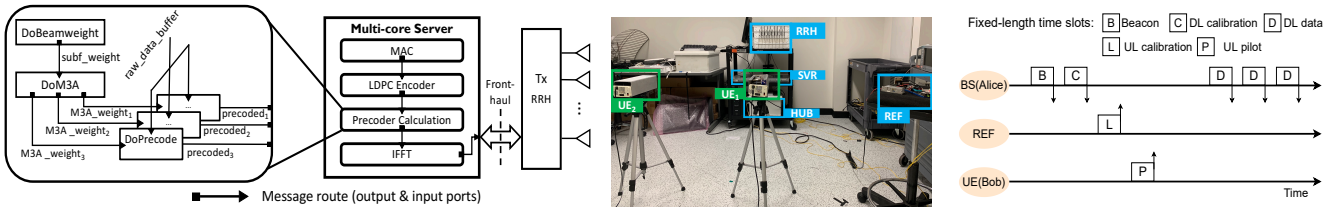


Figure 3: (a). An overview of software implementation, running on a multi-antenna transmitter (receiver side is un-modified and not shown); (b). Indoor testbed setup, including two user nodes (UE) and one base-station (BS); (c). A complete TDD frame that contains five types of timeslot (idle slots not shown).

slots per frame and N_{sc} subcarriers in total, virtual antenna switching first generates $N = N_{sl} \times N_{sc}$ random binary vectors, and does $N \times N_t$ multiplications. Per-subcarrier normalization first finds the minimum of length-N_t array N times, and $N \times N_t$ divisions subsequently. Per-antenna normalization is required only by M3A_{lc}, leading to $N_t \times N$ multiplications, and $N_t \times N$ divisions. In addition, M3A requires h^{eff} calculation, during which there are N inner product operations performed. This translates into and $N_t \times N$ multiplications plus $(N_t - 1) \times N$ summations. Next, inter-symbol normalization stage requires finding the minimum for N_{sc} different length-N_{sl} arrays, and $N \times N_t$ multiplications plus $N \times N_t$ divisions. Put together, in each TDD frame, we see that M3A requires additional $N \times N_t$ multiplications, $(N_t - 1) \times N$ summations, and N_{sc} times size-N_{sl} array minimum searching.

5 TESTBED AND IMPLEMENTATION

We implement M3A on a *commercial* software-defined radio (SDR) testbed; the software of M3A closely emulates the PHY layer of the *NR standard*. Together, they demonstrate the feasibility of applying M3A on multi-antenna systems compliant with NR/LTE or 802.11.

5.1 Hardware

Our key methodology is to leverage multiple independent transmit chains for emulating antenna switching. By putting element(s) of Alice's precoding vector to zero, the associated antenna(s) can be effectively turned off. We use *RENEW* MaMIMO platform [44] to conduct our experiments in a lab environment, as shown in Fig. 3(b), which includes two *user nodes* (UE) and one *base-station* (BS). The BS consists of four main components: a *remote radio head* (RRH), a *hub unit* (HUB), a *reference node* (REF), and a *multi-core server* (SVR).

Each UE is equipped with an Iris SDR module[4], capable of supporting two RF chains. Irises can further be daisy chained in a LEGO-like fashion to form a linear antenna array. Our RRH features four daisy chains, each consisting of eight Iris modules. The four chains (linear arrays) are connected in parallel to the HUB, which distributes clock and time trigger synchronization signals to enable coherent beamforming transmissions [46]. We reserved RRH's top array to perform our experiments and activated a single RF-chain per Iris module. We let each radio provides up to -3 dBm of transmit power. Finally, we let all communications run on a CBRS channel centered at 3.6 GHz, which is unoccupied with other commercial wireless devices in range. The BS and two UEs are configured to be Alice, Bob, and Eve respectively.

In this work, we operate the platform under TDD mode. By the principle of channel reciprocity, the uplink and downlink channels are equal for a given pair of nodes, except for the response induced by their respective RF hardware [47]. The REF, as shown in Fig. 3(b), is treated as a standalone BS radio for completing a procedure named reciprocity calibration, which enables the BS to calibrate out such hardware effect. The outcome is a channel calibration matrix, which is calculated at the BS. Once receiving an UE's uplink pilot, the downlink CSIT can be computed readily through a simple multiplication (between the calibration matrix and received pilot) without any channel estimation feedback from the UE. This way, the cost of channel estimation is reduced greatly.

5.2 Implementation and Software

Fig. 3(a) shows the transmitter-side of M3A, with signal processing blocks implemented using *Agora*—a complete software realization of real-time MaMIMO baseband [48]. We highlight the *Precoder Calculation* module, which is where the M3A's precoding is implemented. For each subcarrier, *DoBeamweight* takes the uplink CSI and the calibration vector as input and generates the single-user beamforming beamweight array *subf_weight* with the size of N_t-by-1. Then, *DoM3A* takes *subf_weight* as input and create N_{sl} (which is 3 in our implementation) updated beamweight arrays $M3A\_weight_{\{1,2,3\}}$ based on the M3A algorithm. Next, *DoPrecode* computes N_{sl} precoded data vectors $precoded_{\{1,2,3\}}$

[4]Commercially available from Skylark Wireless [45].

based on raw I-Q data samples and the $M3A\_weight_{\{1,2,3\}}$. This procedure is repeated for all subcarriers. After the IFFT operation, the SVR sends time-domain samples to the RRH via a front-haul link. Currently, due to the limited UE's streaming rate and front-haul capacity, our tests are restricted to a transmission bandwidth of 5 MHz; specifically, we adopt 15 kHz subcarrier spacing, FFT size of 512, and 7.68 MHz sampling frequency, a typical downlink configuration in LTE [38]. Operational parameters such as amplifier gains, modulation order, and the number of subcarriers, are configured using JSON files. Finally, we use the C++ logging library *spdlog* [49] to record real-time PHY layer statistics (SNR, BER, etc.,) and store them in CSV files.

It is worth mentioning that Bob is completely un-modified, because M3A is transparent to Bob's side, as explained in §4.2. M3A follows the IFFT signal construction pipeline, and makes online precoding updates efficiently without the need of any real-time optimization. Furthermore, as the switching process is implemented entirely in digital baseband, M3A does not require any hardware modification at Alice either.

6 OVER-THE-AIR EVALUATION

In this section, we perform OTA measurements to evaluate the reliability and security performance of M3A in comparison to conjugate beamforming as a baseline.

6.1 Reliability at Bob

Research Question. As previously discussed, to adaptively cancel per-symbol fading is a critical factor for retaining the reliability at Bob. Here, we experimentally investigate the overall system reliability with four following transmission schemes: (1)conjugate beamforming (BF), (2)M3A, (3)M3A_{lc}, and (4)FASM. Note that the Free-space Antenna Subset Modulation (FASM) is our digital multicarrier implementation of [22] that switched antennas physically (see §2). There is no fading cancellation in FASM. Here, we solely consider Alice and Bob to study the reliability at Bob, and defer the analysis of Eve to §6.2. We adopt Bob's BER as the metric for system's reliability.

Setup. Alice adopts a TDD-based transmission protocol, as illustrated in Fig. 3(c). Among three time slots reserved for downlink beamforming transmission, the first D slot is occupied by a pilot symbol for letting Bob compute the CSIR, and each of the rest twos is occupied by an 512-subcarrier OFDM symbol, with 285 data subcarriers modulated using randomly generated 16-QAM constellations. LDPC decoding has been turned off on receivers, in order to investigate the error rate of raw received bits.

Using BF, Alice employs all eight vertically-polarized omnidirectional antennas in RRH's top array, shown in Fig. 3(b). In contrast, she only employs five randomly selected antennas in the other schemes. To fairly compare eight transmit antennas with five, we increase the antennas' transmit gain in five-antenna cases until the SNR at Bob matches the BF. Compensating this known effect will help us to isolate additional factors that can potentially lead to reliability discrepancies of M3A schemes.

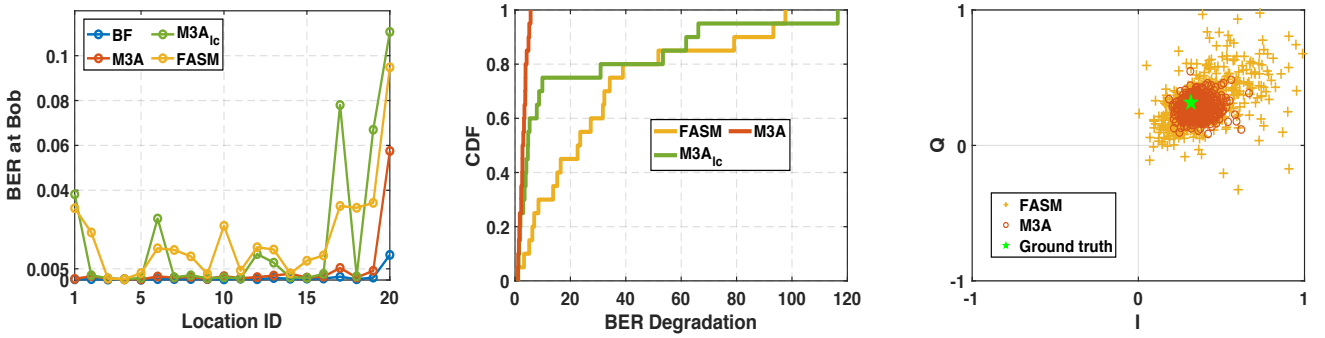
We vary Bob's location in order to investigate reliability for different Alice-Bob channels. As depicted in Fig. 5, we move Bob sequentially from location 1 to 20 (indicated by circles) and at each location, we measure average BER at Bob based on 5,000 TDD frames transmitted by Alice over-the-air. This lab room consists of multiple objects, namely chairs, tables, and numerous other objects which create a natural multipath environment. There is an obstacle near location 20, deteriorating signal strength between Alice and Bob there. We use a fixed MCS (Modulation and Coding Schemes) during our experiments, in order to decouple the impact from MCS selection criteria.

BER Performance at Different Locations for Bob. Fig. 4(a) depicts Bob's average BER as a function of user locations. First, the BER variation across *locations 1-19 (i.e., no obstacle nearby)* for M3A_{lc} and FASM are significantly greater than that of BF and M3A; observing closely at Fig. 4(a), average BER values associated with M3A_{lc} and FASM can be up to around 0.08 and 0.04, significantly greater than that of BF and M3A which both stay within 0.005. Thus, M3A and BF are much better adapted to diverse channel conditions as long as there is no LOS blockage. Second, at location 20, notice that Bob's decoding ability degrades drastically due to the presence of obstacle regardless of which scheme used. There, the BER maxima, in order of BF, M3A, M3A_{lc}, and FASM, are 26.3, 59.5, 43.2, and 7.03 times greater than their medians across all locations. Third, at each location measured, either M3A_{lc} or FASM yields the worst reliability performance. Specifically, there are 15 locations at which FASM yields the highest BER, followed by M3A_{lc}.

BER Degradation Compared to Beamforming. Next, to directly compare against the baseline, at each location x we define the *BER degradation* metric under scheme s to be

$$\gamma(x, s) = \frac{\text{BER}_{Bob}(x, s)}{\text{BER}_{Bob}(x, BF)}. \tag{15}$$

We then aggregate all the BER measurements and report a Cumulative Distribution Function (CDF) plot of BER degradation in Figure 4(b). In addition, the median and 95-th percentile data are summarized in Table 1. Together, they reveal the following: (i) M3A yields similar BER values as the baseline, as attested with CDF curve of $\gamma(x, M3A)$ being tightly concentrated around its median which is, according to Table 1, less than three. Here, the degradation roots in a lumped effect caused by non-ideal SNR compensation and experimentation uncertainties. (ii) A comparison between median



(a) Bob's Average BER at different locations. (b) Empirical CDF of BER degradation. (c) Received constellations at Bob (one frame).

Figure 4: Reliability evaluation results at Bob using different approaches.

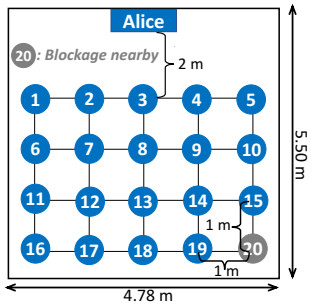


Figure 5: Test topology for indoor experimental evaluations.

Scheme	Median	95-th percentile
M3A	2.98	4.86
$M3A_{lc}$	4.09	66.2
FASM	22.6	93.3

Table 1: Median and 95-th percentile BER degradation using different schemes.

BER degradation of $M3A_{lc}$ and M3A indicates that the reliability penalty for $M3A_{lc}$ is modest, barring outliers leading $\gamma(x, M3A_{lc})$ to be greater than 66. (iii) M3A attains a significantly lower 95-th percentile BER degradation than others. In particular, M3A provides more than an order of magnitude BER reduction when channel condition is *not* favorable for FASM and/or $M3A_{lc}$.

Distorted Constellations at Bob with FASM. To understand the underlying reason for performance degradation of FASM over M3A, we closely examine the received constellations at Bob. In this separate experiment, for the ease of illustration, we let Alice repeatedly transmits only a single 16-QAM symbol. We randomly select and analyze one out of 5000 frames that were transmitted to location 19, where FASM yields a greater BER than M3A. Fig. 4(c) depicts Bob's post-equalized constellations under M3A and FASM. Notably, there is a substantial amount of constellations by FASM that are separated from the ground truth by large distances: they are moving diagonally towards/away from the ground truth symbol. This is because Bob fails to equalize artificial fading of effective channel; during this frame, the number of incorrectly decoded constellations by FASM equals 53 whereas M3A is of three. Hence, the per-symbol fading can significantly compromise the reliability of FASM in practical indoor scenario.

Receive SNR Degradation at Bob with $M3A_{lc}$. On the other hand, $M3A_{lc}$, by design, avoids per-symbol fading at Bob. To reveal the reason behind $M3A_{lc}$'s high BER degradation, recall that the Alice-Bob link is limited by the *weakest* channel gain among all Tx-Rx antenna pairs (§4.2.3). Towards this end, we report the average SNR values at Bob in addition to his BERs in Table 2; the three sampled locations correspond to high, medium, and low BER at Bob with the use of $M3A_{lc}$. Within each TDD frame, Bob's SNR is measured from preamble OFDM symbol; subsequently, for each location, the average SNR is taken across all 5,000 such frames. Indeed,

Location ID	Average SNR (dB) at Bob	Average BER (%) at Bob
20	13.0	11.1
19	16.1	6.70
18	24.8	0.16

Table 2: At three sampled locations, with $M3A_{lc}$, Bob's average BER and SNR values.

Table 2 illustrates the increase of BER with decreasing SNR; particularly, from location 19 to 18, Bob's BER dropped by 42×, owing to added eight dB of SNR. Summarizing, subjected to per-antenna power constraint, the resultant SNR at Bob may not be sufficient. On the other hand, with M3A obtaining a higher diversity, the Alice-Bob link SNRs are seen to be improved.

Discussion. Granted, from reliability's perspective, there exists locations at which it is of trivial matter as to which

scheme to employ. For example, consider location 4, where three BER degradation values are upperbounded by 1.14. At such locations, the channel gain difference between each Tx-Rx antenna pair is expected to be at a less extent, which explains why FASM is on par with M3A. Also, the reliability gap between $M3A_{lc}$ and M3A tends to be closed, once the weakest channel gain is sufficiently strong. Nonetheless, considering that Bob can locate arbitrarily and to ensure his reliability, we opted to employ M3A at Alice to confuse Eve.

Findings: Despite virtually switching antennas to confuse Eve, M3A and $M3A_{lc}$ median BER at Bob is within a factor of 2.98 and 4.09 compared to 8-antenna beamforming, provided that Alice appropriately increases her transmit gain. In contrast, FASM performs quite poorly in the multipath environment, with median BER 22.6 times higher than beamforming. M3A outperforms $M3A_{lc}$ and FASM in adapting to varying channel conditions, with 95-th percentile value being 13 and 19 times lower, respectively. The central condition to maintain high reliability at Bob is Alice-Bob link being free of unpredictable gain changes and not in a deep fade.

6.2 Security Performance Comparison

Research Question. So far, we have evaluated our system's reliability to serve intended user Bob under multipath channel conditions. Now, we empirically evaluate the resilience of constructed Alice-Bob link against passive eavesdropping. We adopt Eve's BER values as a metric. Here, our experiments address two issues: (i). How effective is BF in protecting information bits from being decoded by Eve in a practical indoor deployment? (ii). How well does M3A impose higher BER at randomly located Eves, compared to BF as the baseline?

Setup. To compare the security performance against the baseline, at each location x, we propose the *BER Gain* metric under scheme s as follows:

$$\eta(x,s) = \frac{\mathrm{BER}_{Eve}(x,s)}{\mathrm{BER}_{Eve}(x,BF)}, \tag{16}$$

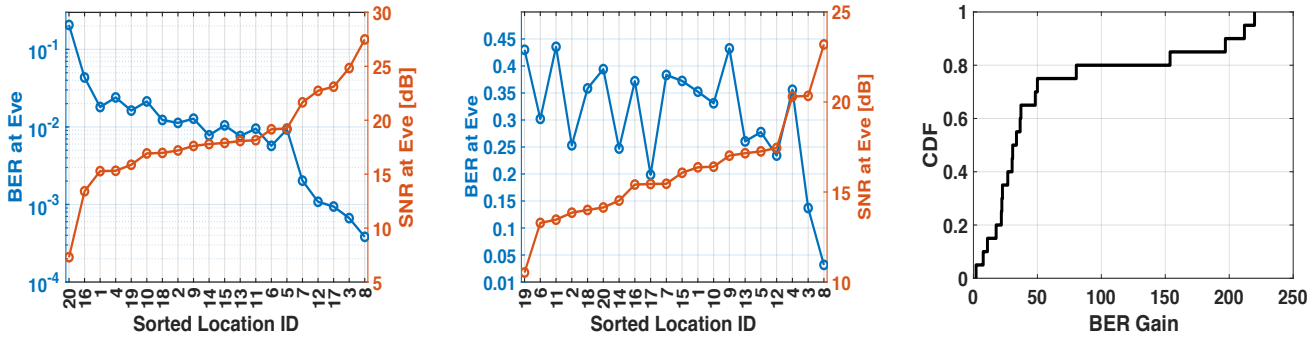
so that a greater BER improvement is characterized by a higher $\eta(x,s)$. We now introduce Eve into our system, which is implemented using the same hardware as Bob, and is configured using following steps. First, to ensure Eve's reception time covers the signals of interest, she synchronizes her frame time boundaries with Alice's frame by detecting a broadcasted beacon sequence (within the B slot in Fig. 3(c)), by which she then captures the signals belonging to downlink transmission slots (the D slots). Second, to ensure Eve's reception *frequency* window covers the spectrum occupied by the signals of interest, the carrier frequency and sampling rate are both set to be the same as Bob's, so that Eve can adjust the filtering response as needed. Finally, to equalize the channel effect, Eve finds her CSIR per subcarrier by comparing the received downlink pilot symbol carried by the first D slot to the expected one (§4.1.2).

During this experiment, Eve directs her antenna broadside towards Alice for enhancing the signal reception[5]. We record Eve's BER values while changing her location from 1 to 20 sequentially, in order to evaluate M3A's resilience across various locations. Meanwhile, Bob is fixed at location 8 for our measurement convenience. When Eve arrives at location 8, Bob and Eve's enclosures physically touch each other, meaning they cannot be placed any closer to one another. There, the resultant antenna spacing is measured to be 10.4 cm, equivalent to 1.24 units of carrier wavelength.

Vulnerability of Beamforming. The results when Alice employs BF are illustrated in Fig. 6(a), where the x-axis shows location IDs sorted in ascending order of receive SNR. Eve's respective values of average BER and SNR are on the left and right side of the y-axis, and the BER achieved *at Bob* is found to be 3.10×10^{-4}. We observe that BF provides a modest level of security, since Eve's BER is higher than Bob's at every location measured. This is because BF can actively focus transmit energy at Bob's antenna, lowering receive SNR elsewhere. Nevertheless, numerous locations exist where an eavesdropper can correctly decode the vast majority of information bits: Eve's BER remains around 10^{-4} to 10^{-2} for ten out of 20 locations. The reason is that BF in practice still suffers from the generation of strong sidelobes: on our testbed, an outdoor field showed that sidelobe levels can only be 10-20 dB lower than the mainlobe. When this effect is combined with multipath, the result is high SNR at locations that can either be close to, or far away from Bob. Notably, observe that Eve's BER is largely decreasing with respect to her SNR, according to Fig. 6(a). Thus, for BF, Eve's decoding ability is effectively determined by her receive SNR, yielding insufficiency of applying BF as a standalone defense against eavesdropping in an indoor environment. For instance, by exploiting a higher gain antenna, Eve is able to acquire moderate to high SNR more easily.

Security Improvement by M3A. Next, we aim to explore how much BER gain M3A can achieve in comparison with BF. Fig. 6(b) shows the empirical results when Alice employs M3A, from which we make three key observations. First, the irregular variation of BER as SNR increases indicates that Eve's BER is no longer a function of SNR only. Recall that M3A leverages a fundamentally different mechanism to thwart eavesdropping: rather than suppressing signal strength escaping through the sidelobe, M3A moves Eve's symbols to random locations that do not match those of the training symbols sent by Alice at the beginning of the frame. Second, when Alice uses M3A rather than BF, Eve

[5]Dual-polarized receive antennas provides 6 dBi of gain.



(a) Eve's BER and SNR under BF. (b) Eve's BER and SNR under M3A. (c) CDF of BER gain over all locations.

Figure 6: Comparison of Eve's average BER versus locations sorted in ascending order of SNR, when Alice employs different approaches. In 6(b), Eve's BER is in linear scale to better visualize its irregular variation.

experiences higher BER at every location measured while maintaining reliability at Bob (whose BER is 8.00×10^{-4}). In particular, with M3A, the minimum, median, and maximum BER at Eve are 3.17%, 34.1%, and 43.6% respectively. Third, inline with the intended user Bob, at four eavesdropping locations 3 (Eve is approximately 1/3 closer to Alice), 8, 13, and 18, Fig. 6(b) indicates that M3A provides much better security than the baseline, evidenced by BER gain values ranging from 32.5 to 233.3. In contrast, free-space DM schemes are known to be incapable of thwarting any Eve located along the same direction as Bob (e.g., [22, 26, 27, 29]). Remarkably, at location 8, where Bob and Eve are separated by only 1.24 wavelengths, M3A still yields a BER gain of $\eta(8, M3A) = 133$. To further ensure that Eve's high BER at location 8 is not due to her hardware discrepancies relative to Bob's, we perform a separate experiment by swapping the two nodes' positions and interchanging their role as being Bob or Eve. A pair of similar BER was observed.

We aggregate all BER measurements and present a CDF plot of BER gains in Fig. 6(c). Notice that the median is approximately 40×, with achieved BER gain values up to over 200×. Additionally, compared with prior designs that only introduce phase noise (e.g., [21, 29]), M3A achieves BER greater than 33.3% [6] at 11 out of 20 locations.

Findings: When using conjugate beamforming, an eavesdropper located angularly away from Bob can still decode signals with high probability due to compound effects from sidelobe leakages and multipath propagation. In contrast, M3A thwarts Eve to have a median BER of 34.1% across all tested locations, providing a median BER gain greater than 40× *compared to conjugate beamforming.*

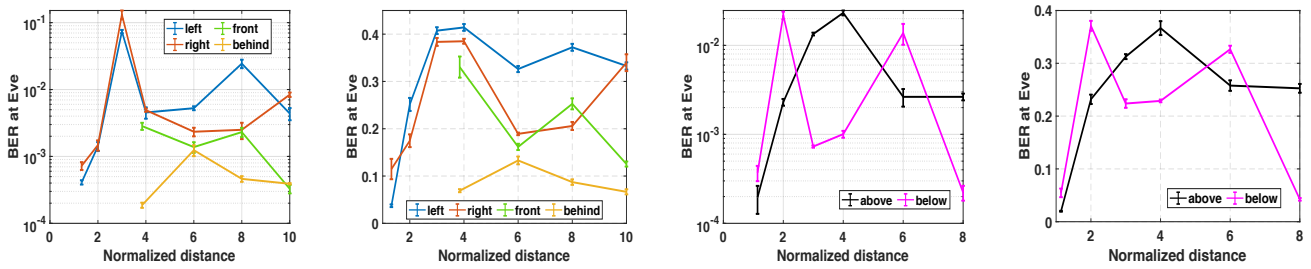
[6]The BER of Gray-coded 16-QAM with uniformly distributed phase noise.

6.3 Eavesdropper Proximity in Wavelength-Scale

Research Question. In §6.2, we observed one location where the passive eavesdropper Eve is still thwarted, even being separated by only 1.24 units of carrier wavelength away from intended user Bob. In this section, we further explore whether the robustness of M3A's security performance is indeed achieved *in three-dimension*, against the effect of Eve's multiple positions to Bob in wavelength-scale.

Setup. Reusing the same transmitter and receiver setup in §6.2, and to quantify the effect of Eve's proximity on M3A, we fix Bob at the same location 8. Verifying Eve's proximity effect at other locations is left as a future work. Next, we introduce a new set of spatial locations by varying Eve's distances to Bob. As shown in Fig. 8, for both left and right direction (± x-axis), the distance ranges from 1.24λ (which is the closest we can physically get) to 10λ. Whereas in forward and backward direction, the closest antenna distance between Bob and Eve becomes approximately 3.80λ due to the different physical constraint. We stack Eve vertically above and below Bob's position using a tripod, and test the separation distances from 1.14λ up to 8λ.

Results. Fig. 7(a) depicts the mean and single standard deviation of Eve's BER at various locations in horizontal plane, when Alice employs BF. As similarly observed in §6.2, Eve decodes overheard signal from the BF transmission with relatively low BER values. In particular, there are only three out of 22 test locations where Eve has an BER above 1%. Additionally, Eve's BER varies quite unpredictably with respect to distances. For example, along right direction (+x-axis), moving Eve from 4λ to 3λ incurs a more than two orders of magnitude rise in BER due to 14.5 dB SNR drop at Eve. In this scenario, though Alice-Eve distance remains similar, the energy-focusing transmission combined with multipath



(a) BF, horizontal plane. (b) M3A, horizontal plane. (c) BF, vertical plane. (d) M3A, vertical plane.

Figure 7: Eve's BER as the function of normalized distance (with respect to carrier wavelength) in horizontal plane and vertical plane, when Alice employs different approaches.

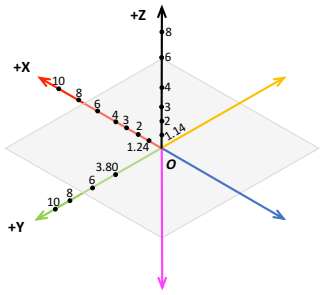
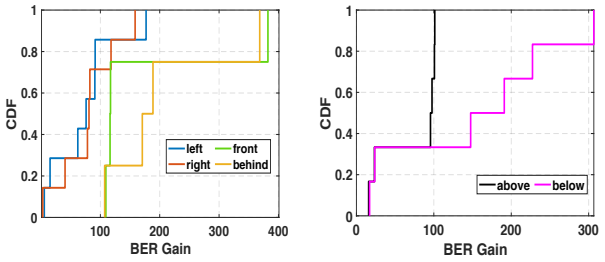


Figure 8: 3D view of experimental setup with distances normalized with respect to carrier wavelength λ. The origin represents Bob's antenna location, at which the positive x,y, and z points to the direction of right, front, and above, respectively.



(a) Horizontal plane. (b) Vertical plane.

Figure 9: CDF of BER gains achieved by M3A across all locations in horizontal plane and vertical plane.

channel are strong enough to occasionally null out Eve's SNR. Nonetheless, according to the BER statistics at other locations in Fig. 7(a), such nulling is accompanied by a highly irregular spatial response that can be quite favorable to Eve. On the other hand, results of Fig. 7(b) shows that M3A *consistently outperforms BF regardless of eavesdropper's proximity* by imposing higher absolute BER values. Specifically, we aggregate the measurements across all location IDs and provide a CDF plot of BER gains in Fig. 9(a). Compared to the baseline, along four different directions, the median BER gain achieved is approximately 80× (left, right), 110× (front), and 190× (behind) respectively.

In Fig. 7(c), we plot the mean and single standard deviation of BER at Eve in vertical plane when Alice uses BF. Still, we observe that BF performs poorly in securing transmission in vertical direction: the BER values of all 12 locations ranged from an order of 10^{-4} to 10^{-2}. The root cause is that Eve can still receive pilot and data symbols with sufficiently high SNR, thereby decoding bits correctly.

With Alice using M3A, the improved BER results can be seen in Fig. 7(d): M3A *consistently outperforms BF regardless of eavesdropper's proximity, as well as in vertical direction.* This is because a linear MIMO array in complex multipath channel environment (e.g., WiFi or LTE femtocell) will leverage every reflection in the topology to ensure maximum constructive interference at Bob in a three-dimensional space. Even with the same coordinate in horizontal plane, channels $\boldsymbol{h}_{ab}(n,k)$ and $\boldsymbol{h}_{ae}(n,k)$ can still be de-correlated when being separated vertically. Thus, Alice may construct a wavelength-scale security zone in vertical direction with the help of M3A. Note that "vertical Eves" cannot be thwarted if linear array Alice uses beamsteering-based directional modulation techniques. Lastly, we aggregate measurements across all location IDs and a CDF plot of BER gain is shown in Fig. 9(b). It can be observed that along the ±z-axis tested, the median BER gain is about 100× (above) and 150× (below) respectively.

Findings: M3A still achieves better security performance than conjugate beamforming at wavelength-scale proximity distances. This is attained through the combination of the rich multipath propagation and the effect of random antenna switching. Furthermore, across all three dimensions, M3A provides approximately two orders of magnitude median BER gains both horizontally and vertically (115×, and 125×).

7 DISCUSSION AND FUTURE WORK

In this section, we discuss extensions of M3A beyond the threat model described in §3.

Uplink Transmission Security. M3A secures only downlink traffic. This limitation stems from the design principle of M3A, which relies on the transmitter having multiple transmit antennas to modulate the signals. Consequently, to secure uplink transmission via M3A, Bob would require multiple antennas (contrary to the single-antenna assumption we have in this work). The specific design and implementation of M3A for the uplink would require further research and development.

Distributed MIMO Attack. M3A has been designed and evaluated against single-antenna uncooperative Eves. While Eve having a phased array alone cannot reverse scrambled amplitudes and phases through beamforming gain, distributed MIMO eavesdropping has been identified as a means to reduce an adversary's BER [27, 34, 50]. E.g., [27] and [50] have proposed decoders based on two-layer neural networks or compressive sensing. Notably, their complexity and cost increases, as they require carefully designed eavesdropping locations, a large number of distributed chains (≥10), and offline time-domain synchronization. The potential threat posed by MIMO Eve to the security of M3A remains an open topic for future study.

Multi-user Downlink with Multiple Bobs. Currently, M3A does not cover the multi-user MIMO case (i.e., multiple spatial streams to multiple Bobs). However, M3A can leverage MIMO-OFDMA to transmit multiple secure streams to different Bobs concurrently based on the availability of Bobs' CSIT, the independence of binary masks in the time-frequency domain, and the orthogonality among subcarriers. We leave the OTA verification of this feature to future work.

8 CONCLUSION

We present our design, implementation, and evaluation of M3A, a multi-antenna multicarrier system against wireless eavesdropping at the wavelength scale. M3A achieves a security-reliability co-design using a novel digital baseband algorithm, exploiting rich multipath channels. Our experimental results show M3A not only moves the transmitted symbols to increase decoding errors at Eves, but also retains reliability at Bob.

APPENDIX A

Here, we re-state the proposition and provide a proof.

Proposition. *Consider vector* $\boldsymbol{h}_{ab}(k) = [h_0, \ldots, h_{N_t-1}]$, *ordered such that* $|h_0| \geq |h_1| \geq \cdots \geq |h_{N_t-1}|$. *In a TDD frame containing* N_{sl} *downlink slots, Alice lets each subcarrier virtually selects* M_t *out of* N_t *antennas, resulting in the raw effective channel* $h_{ab}^{eff}(n,k)$ *for each slot n. Both M3A and M3A*$_{lc}$ *yield a time-invariant effective Alice-Bob channel, particularly*

- *in M3A*$_{lc}$, *we have* $h_{ab}^{eff}(k)^{lc} = M_t|h_{N_t-1}|$;
- *in M3A, we have* $h_{ab}^{eff}(k) = \min_{n=1,\ldots,N_{sl}} h_{ab}^{eff}(n,k)$, *where a diversity gain of* M_t *can be achieved.*

Proof. In M3A$_{\text{lc}}$, denote $\mathcal{A}$ as the set that contains indices of the M_t active antennas. Similar to Eq. (14), the effective Alice-Bob channel in each slot is derived as:

$$\begin{aligned} h_{ab}^{\text{eff}}(n,k)^{lc} &= \left\langle \boldsymbol{h}_{ab}(n,k), \widetilde{\boldsymbol{w}}_a^{lc}(n,k) \right\rangle \\ &= \alpha^{lc}(k) \cdot \left\langle \boldsymbol{h}_{ab}(k), \boldsymbol{h}_{ab}(k) \circ \boldsymbol{b}(n,k) \circ \boldsymbol{c}(k) \right\rangle \\ &\overset{(1)}{=} \alpha^{lc}(k) \cdot \sum_{i \in \mathcal{A}} |h_i|^2 / |h_i|^2 = M_t |h_{N_t-1}|, \end{aligned} \tag{17}$$

where (1) is by the construction of $\alpha^{lc}(k)$ and $\boldsymbol{c}(k)$ introduced in Eq.(12).

In M3A, similar to Eq. (11), $h_{ab}^{\text{eff}}(n,k)^{\text{mrt}}$ can be written as:

$$\begin{aligned} h_{ab}^{\text{eff}}(n,k)^{\text{mrt}} &= \left\langle \boldsymbol{h}_{ab}(n,k), \widetilde{\boldsymbol{w}}_a^{mrt}(n,k) \right\rangle \\ &= \left(\min_{n=1,\ldots,N_{sl}} h_{ab}^{\text{eff}}(n,k) / h_{ab}^{\text{eff}}(n,k) \right) \cdot \alpha(k) \cdot \\ &\quad \cdot \left\langle \boldsymbol{h}_{ab}(k), \boldsymbol{h}_{ab}(k) \circ \boldsymbol{b}(n,k) \right\rangle \\ &\overset{(2)}{=} \left(\min_{n=1,\ldots,N_{sl}} h_{ab}^{\text{eff}}(n,k) / h_{ab}^{\text{eff}}(n,k) \right) \cdot h_{ab}^{\text{eff}}(n,k) \\ &= \min_{n=1,\ldots,N_{sl}} h_{ab}^{\text{eff}}(n,k), \end{aligned} \tag{18}$$

where (2) is by the relation defined in Eq. (10). This shows the effective Alice-Bob channel in M3A is time-invariant. Next, to show the diversity gain of M3A, letting $\mathring{\mathcal{A}} = \{a_0, \ldots, a_{M_t-1}\}$ be the set of active antenna indices that leads to $\min_n h_{ab}^{\text{eff}}(n,k)$ in the given frame. By Eq. (10), we obtain

$$\begin{aligned} &\min_{n=1,\ldots,N_{sl}} h_{ab}^{\text{eff}}(n,k) = \min_{n=1,\ldots,N_{sl}} \left(\alpha(k) \cdot \|\boldsymbol{h}_{ab}(k) \circ \boldsymbol{b}(n,k)\|^2 \right) \\ &= \alpha(k) \cdot \min_{n=1,\ldots,N_{sl}} \left(\|\boldsymbol{h}_{ab}(k) \circ \boldsymbol{b}(n,k)\|^2 \right) \\ &= \frac{1}{|h_0|} \cdot \left(|h_{a_0}|^2 + \cdots + |h_{a_{M_t-1}}|^2 \right), \end{aligned} \tag{19}$$

from which a diversity gain of M_t can be achieved. □

ACKNOWLEDGEMENTS

The authors sincerely thank the anonymous shepherd and reviewers for their insightful comments and suggestions. This research was supported by Cisco, Intel, NSF grants CNS-2148132, CNS-2211618, CNS-1955075, and DOD: Army Research Laboratory grant W911NF-19-2-0269.

REFERENCES

[1] Yulong Zou, Jia Zhu, Xianbin Wang, and Lajos Hanzo. A survey on wireless security: Technical challenges, recent advances, and future trends. *Proceedings of the IEEE*, 104(9):1727–1765, 2016.

[2] David Rupprecht, Katharina Kohls, Thorsten Holz, and Christina Pöpper. Call me maybe: Eavesdropping encrypted LTE calls with ReVoLTE. In *29th USENIX security symposium (USENIX security 20)*, pages 73–88, 2020.

[3] Martin Kotuliak, Simon Erni, Patrick Leu, Marc Roeschlin, and Srdjan Čapkun. LTrack: Stealthy tracking of mobile phones in LTE. In *31st USENIX Security Symposium (USENIX Security 22)*, pages 1291–1306, 2022.

[4] Baik Hoh, Marco Gruteser, Hui Xiong, and Ansaf Alrabady. Enhancing security and privacy in traffic-monitoring systems. *IEEE Pervasive Computing*, 5(4):38–46, 2006.

[5] Michael Rushanan, Aviel D Rubin, Denis Foo Kune, and Colleen M Swanson. Sok: Security and privacy in implantable medical devices and body area networks. In *2014 IEEE symposium on security and privacy*, pages 524–539. IEEE, 2014.

[6] Amitav Mukherjee. Physical-layer security in the internet of things: Sensing and communication confidentiality under resource constraints. *Proceedings of the IEEE*, 103(10):1747–1761, 2015.

[7] Jehad M Hamamreh, Haji M Furqan, and Huseyin Arslan. Classifications and applications of physical layer security techniques for confidentiality: A comprehensive survey. *IEEE Communications Surveys & Tutorials*, 21(2):1773–1828, 2018.

[8] H Vincent Poor and Rafael F Schaefer. Wireless physical layer security. *Proceedings of the National Academy of Sciences*, 114(1):19–26, 2017.

[9] Ertuğrul Güvenkaya, Jehad M Hamamreh, and Hüseyin Arslan. On physical-layer concepts and metrics in secure signal transmission. *Physical Communication*, 25:14–25, 2017.

[10] Muriel Médard and Ken R Duffy. Physical layer insecurity. In *2023 57th Annual Conference on Information Sciences and Systems (CISS)*. IEEE, 2023.

[11] Evgeny Khorov, Anton Kiryanov, Andrey Lyakhov, and Giuseppe Bianchi. A tutorial on IEEE 802.11ax high efficiency WLANs. *IEEE Communications Surveys & Tutorials*, 21(1):197–216, 2018.

[12] Erik Dahlman, Stefan Parkvall, and Johan Skold. *5G NR: The next generation wireless access technology*. Academic Press, 2020.

[13] Kanapathippillai Cumanan, Zhiguo Ding, Bayan Sharif, Gui Yun Tian, and Kin K Leung. Secrecy rate optimizations for a MIMO secrecy channel with a multiple-antenna eavesdropper. *IEEE Transactions on Vehicular Technology*, 63(4):1678–1690, 2013.

[14] Jong-Ho Lee, Jeongsik Choi, Woong-Hee Lee, and Jiho Song. Exploiting array pattern synthesis for physical layer security in millimeter wave channels. *Electronics*, 8(7):745, 2019.

[15] Yongpeng Wu, Chengshan Xiao, Zhi Ding, Xiqi Gao, and Shi Jin. Linear precoding for finite-alphabet signaling over MIMOME wiretap channels. *IEEE transactions on vehicular technology*, 61(6):2599–2612, 2012.

[16] Ying Ju, Hui-Ming Wang, Tong-Xing Zheng, and Qinye Yin. Secure transmissions in millimeter wave systems. *IEEE Transactions on Communications*, 65(5):2114–2127, 2017.

[17] Chen Chen, Yue Dong, Xiang Cheng, and Na Yi. An iterative FFT-based antenna subset modulation for secure millimeter wave communications. In *2017 International Conference on Computing, Networking and Communications (ICNC)*, pages 454–459. IEEE, 2017.

[18] Jixin Guo, Lorenzo Poli, Mohammad Abdul Hannan, Paolo Rocca, Shiwen Yang, and Andrea Massa. Time-modulated arrays for physical layer secure communications: optimization-based synthesis and experimental assessment. *IEEE Transactions on Antennas and Propagation*, 66(12):6939–6949, 2018.

[19] Yuan Ding and Vincent Fusco. Experiment of digital directional modulation transmitters. In *Forum for Electromagnetic Research Methods and Application Technologies (FERMAT)*, volume 11, 2015.

[20] Naga Sasikanth Mannem, Tzu-Yuan Huang, Elham Erfani, Sensen Li, David Munzer, Matthieu R Bloch, and Hua Wang. A 25–34-ghz eight-element MIMO transmitter for keyless high throughput directionally secure communication. *IEEE Journal of Solid-State Circuits*, 57(5):1244–1256, 2021.

[21] Kartik Patel, Nitin Jonathan Myers, and Robert W Heath. Circulant shift-based beamforming for secure communication with low-resolution phased arrays. *IEEE Transactions on Wireless Communications*, 2022.

[22] Nachiappan Valliappan, Angel Lozano, and Robert W Heath. Antenna subset modulation for secure millimeter-wave wireless communication. *IEEE Transactions on communications*, 61(8):3231–3245, 2013.

[23] Nafel N Alotaibi and Khairi Ashour Hamdi. Switched phased-array transmission architecture for secure millimeter-wave wireless communication. *IEEE Transactions on Communications*, 64(3):1303–1312, 2016.

[24] Mohammed E Eltayeb, Junil Choi, Tareq Y Al-Naffouri, and Robert W Heath. Enhancing secrecy with multiantenna transmission in millimeter wave vehicular communication systems. *IEEE Transactions on Vehicular Technology*, 66(9):8139–8151, 2017.

[25] Aydin Babakhani, David B Rutledge, and Ali Hajimiri. Transmitter architectures based on near-field direct antenna modulation. *IEEE Journal of Solid-State Circuits*, 43(12):2674–2692, 2008.

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

[27] Suresh Venkatesh, Xuyang Lu, Bingjun Tang, and Kaushik Sengupta. Secure space–time-modulated millimetre-wave wireless links that are resilient to distributed eavesdropper attacks. *Nature Electronics*, 4(11):827–836, 2021.

[28] Ying Ju, Yanzi Zhu, Hui-Ming Wang, Qingqi Pei, and Haitao Zheng. Artificial noise hopping: A practical secure transmission technique with experimental analysis for millimeter wave systems. *IEEE Systems Journal*, 14(4):5121–5132, 2020.

[29] Xinyi Li, Chao Feng, Fengyi Song, Chenghan Jiang, Yangfan Zhang, Ke Li, Xinyu Zhang, and Xiaojiang Chen. Protego: securing wireless communication via programmable metasurface. In *Proceedings of the 28th Annual International Conference on Mobile Computing And Networking*, pages 55–68, 2022.

[30] Chao Feng, Xinyi Li, Yangfan Zhang, Xiaojing Wang, Liqiong Chang, Fuwei Wang, Xinyu Zhang, and Xiaojiang Chen. Rflens: metasurface-enabled beamforming for iot communication and sensing. In *Proceedings of the 27th Annual International Conference on Mobile Computing and Networking*, pages 587–600, 2021.

[31] Suhas Mathur, Wade Trappe, Narayan Mandayam, Chunxuan Ye, and Alex Reznik. Radio-telepathy: extracting a secret key from an unauthenticated wireless channel. In *Proceedings of the 14th ACM international conference on Mobile computing and networking*, pages 128–139, 2008.

[32] Shyamnath Gollakota and Dina Katabi. Physical layer wireless security made fast and channel independent. In *2011 Proceedings IEEE INFOCOM*, pages 1125–1133. IEEE, 2011.

[33] Narendra Anand, Sung-Ju Lee, and Edward W Knightly. Strobe: Actively securing wireless communications using zero-forcing beamforming. In *2012 Proceedings IEEE INFOCOM*, pages 720–728. IEEE, 2012.

[34] Haitham Hassanieh, Jue Wang, Dina Katabi, and Tadayoshi Kohno. Securing RFIDs by randomizing the modulation and channel. In *12th*

USENIX Symposium on Networked Systems Design and Implementation (NSDI 15), pages 235–249, 2015.

[35] Christina Garman, Matthew Green, Gabriel Kaptchuk, Ian Miers, and Michael Rushanan. Dancing on the lip of the volcano: Chosen ciphertext attacks on apple imessage. In *USENIX Security Symposium*, pages 655–672, 2016.

[36] Simon Erni, Martin Kotuliak, Patrick Leu, Marc Roeschlin, and Srdjan Capkun. Adaptover: adaptive overshadowing attacks in cellular networks. In *Proceedings of the 28th Annual International Conference on Mobile Computing And Networking*, pages 743–755, 2022.

[37] Xu Zhang and Edward W Knightly. CSIsnoop: Attacker inference of channel state information in multi-user WLANs. In *Proceedings of the 18th ACM International Symposium on Mobile Ad Hoc Networking and Computing*, 2017.

[38] Arunabha Ghosh, Jun Zhang, Jeffrey G Andrews, and Rias Muhamed. *Fundamentals of LTE*. Pearson Education, 2010.

[39] Xiufeng Xie, Xinyu Zhang, and Karthikeyan Sundaresan. Adaptive feedback compression for MIMO networks. In *Proceedings of the 19th annual international conference on Mobile computing & networking*, pages 477–488, 2013.

[40] Clayton Shepard, Hang Yu, Narendra Anand, Erran Li, Thomas Marzetta, Richard Yang, and Lin Zhong. Argos: Practical many-antenna base stations. In *Proceedings of the 18th annual international conference on Mobile computing and networking*, pages 53–64, 2012.

[41] Paul H Moose. A technique for orthogonal frequency division multiplexing frequency offset correction. *IEEE Transactions on communications*, 42(10):2908–2914, 1994.

[42] John Terry and Juha Heiskala. *OFDM wireless LANs: A theoretical and practical guide*. Sams publishing, 2002.

[43] Ehsan Aryafar, Narendra Anand, Theodoros Salonidis, and Edward W Knightly. Design and experimental evaluation of multi-user beamforming in wireless LANs. In *Proceedings of the sixteenth annual international conference on Mobile computing and networking*, pages 197–208, 2010.

[44] Renew wireless wikipage. https://wiki.renew-wireless.org/.

[45] Skylark wireless. https://skylarkwireless.com/products/infrastructure/.

[46] Clayton Shepard, Josh Blum, Ryan E Guerra, Rahman Doost-Mohammady, and Lin Zhong. Design and implementation of scalable massive-MIMO networks. In *Proceedings of the 1st International Workshop on Open Software Defined Wireless Networks*, 2020.

[47] Joao Vieira, Fredrik Rusek, Ove Edfors, Steffen Malkowsky, Liang Liu, and Fredrik Tufvesson. Reciprocity calibration for massive MIMO: Proposal, modeling, and validation. *IEEE Transactions on Wireless Communications*, 16(5):3042–3056, 2017.

[48] Jian Ding, Rahman Doost-Mohammady, Anuj Kalia, and Lin Zhong. Agora: Real-time massive MIMO baseband processing in software. In *Proceedings of the 16th International Conference on emerging Networking EXperiments and Technologies*, pages 232–244, 2020.

[49] Spdlog github repository. https://github.com/gabime/spdlog.

[50] Cristian Rusu, Nuria González-Prelcic, and Robert W Heath. An attack on antenna subset modulation for millimeter wave communication. In *2015 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, pages 2914–2918. IEEE, 2015.