RMDM: Using Random Meta-Atoms to Send Directional Misinformation to Eavesdroppers

Fahid Hassan*, Zhambyl Shaikhanov*, Hichem Guerboukha †,
Daniel M. Mittleman†, Kaushik Sengupta ‡, and Edward W. Knightly*
* Rice University, Houston, Texas, USA, Email: {FHassan, zs16, Knightly}@rice.edu
† Brown University, Providence, Rhode Island, USA, Email:{hichem_guerboukha, daniel_mittleman}@brown.edu
‡ Princeton University, Princeton, New Jersey, USA, Email: kaushiks@princeton.edu

***Abstract*—In this paper, we propose *RMDM*, Random Meta-atoms enabled Directional Misinformation, a novel system that enables a wireless transmitter to program a transmissive metasurface to send misinformation towards eavesdroppers while ensuring the correct information is received at the legitimate receiver. To do so, we design a metasurface with angular-dependent channel responses that alter the phase and amplitude of the transmitted symbol in different ways along different angular directions. We show how randomly selected groups of meta-atoms can be reconfigured so that the symbol constellation in the eavesdropper's direction is randomly transformed for each symbol. Moreover, our design includes a baseband correction, prior to transmission, to eliminate the metasurface's impact in the intended user's direction. Our experimental results show that the eavesdropper's error probability increases to almost 0.5 after an angular separation of only 4° away from the legitimate user's direction, forcing the eavesdropper to be very close to correctly intercept the information.**

I. Introduction

Millimeter wave (mmWave) to sub-THz spectrum provides plentiful bandwidth that allows unprecedented data rate and low latency, that together, will enable new applications for next generation 6G and beyond wireless networks [12], [20]. Because such frequency bands require directional beams to overcome the impact of high path loss [11], [16], mmWave and sub-THz wireless links are widely assumed to be more secure against eavesdropping attacks than legacy sub-6 GHz links. Unfortunately, recent studies have shown that directional links are not immune to eavesdroppers, and novel strategies can still enable successful interception by an attacker [15], [24].

In this paper, we introduce ***RMDM***, **R**andom **M**eta-atom enabled **D**irectional **M**isinformation, a novel security system that enables Alice to send time-variant misinformation (incorrect symbols) towards Eve provided she is sufficiently away from Bob. The key idea behind *RMDM* is to couple a reconfigurable transmissive metasurface with Alice's Access Point (AP) such that Alice randomly reconfigures the meta-atoms to transform the transmitted information symbol in the directions of eavesdroppers while ensuring that the metasurface is transparent only in Bob's direction. That is, Eve's location need not be known by Alice, but Eve must be sufficiently angularly away from Bob. In particular, we make the following contributions.

First, we show how Alice can realize directional misinformation by designing metasurface configurations that generate an *angular-dependent* transformation of the information symbol such that receivers at different angular directions relative to the metasurface receive different information symbols depending on their direction. Our design consists of groups of meta-atoms with randomly configured amplitude and phase responses such that the scattered signals from the meta-atoms constructively or destructively interfere at random directions, resulting in a change on the amplitude and phase of the information symbol that is unique for every angular direction. Because a single static transformation could be learned by Eve, we design *RMDM* to have many different configurations, each having a unique transformation, and one of which is randomly selected for each symbol. Next, *RMDM* must "undo" the impact of the metasurface for Bob to ensure that Bob gets the correct symbol. Hence, *RMDM* includes a transmitter-side *per-configuration correction* element. The objective of the correction process is to preserve the correct symbol in Bob's direction by adding a corrective phase and amplitude on the information symbol prior to transmission based on the selected metasurface response experienced at Bob's direction. Due to the angular-dependent property of the metasurface, the correction only eliminates the metasurface's impact in Bob's direction. In contrast, the (corrected) information symbol is corrupted at all other eavesdropper's directions that are angulary separated from Bob.

Second, we configure *RMDM* using the C-shaped split ring resonator (C-SRR) meta-atom as the building block for our metasurfaces [14], [25]. The C-SRR meta-atom has a simple structure that can be represented by a radius r, an opening angle α, and an orientation angle γ. We conduct finite element method simulations to characterize the amplitude and phase responses available to Alice by the C-SSR at our targeted center frequency of 150 GHz. Specifically, we simulate the meta-atom for various values of r, α, and γ and find that phase shifts spanning the range 0 to 2π are achievable by controlling r and α whereas amplitude can be controlled by changing the orientation angle γ. We show how Alice utilizes these design choices to compose a set of configurations with random amplitude and phase responses to confuse the eavesdropper.

Finally, We conduct over-the-air experiments using a high-

resolution time-domain-spectroscopy (TDS) system to evaluate *RMDM*. As a proof of concept, we fabricate a set of configurations, each composed of randomly selected groups of C-SSRs, using a rapid-prototyping metasurface fabrication technique [10]. First, we experimentally evaluate each configuration's capabilities of transforming the information in the eavesdropper's direction and find that Alice has full control over Eve's amplitude and phase. Finally, we evaluate the security performance of *RMDM* by studying the Bit Error Rate (BER) at the eavesdropper's directions. We measure the different metasurface configurations' responses at angular directions from -20° to 20° away from Bob. We use the channel measurements to drive a trace-driven-simulation and show that Eve's BER with *RMDM* is near the ideal target of 0.5, provided that Eve is not within 4° of angular separation from Bob's. If Eve is outside this region, her location-averaged BER is 0.464.

Thus, by transforming symbols in directions away from Bob, *RMDM* has two key application scenarios: First, *RMDM* provides a complimentary security enhancement for networks already employing wireless encryption (e.g., Wi-Fi can use AES-256 [1]), especially for the many headers and control information that are sent unencrypted and leak information to adversaries [1]. Second, for transmitters that are computationally-limited or energy-constrained and cannot perform classical encryption, an especially pressing concern at high frequencies [3], our method provides an alternative scheme for thwarting eavesdroppers.

The reminder of this paper is organized as follows: Section II presents the design of *RMDM* and its main components. Section III discusses the configuration of *RMDM* metasurfaces. Section IV describes our experimental platform and the evaluation results. Section V reviews the related work. And Section VI concludes the paper.

II. Metasurface Enabled Directional Misinformation

In this section, we first give an introduction on the concept of directional modulation followed by an overview of *RMDM*. Next we describe how *RMDM* generates time-variant random angular misinformation. We then discuss the correction process to eliminate the impact of the metasurface in Bob's direction. Finally we give an example of how *RMDM* can secure QAM.

A. Directional Modulation

Directional modulation (DM) provides a mechanism to counter eavesdropping attacks by transmitting misinformation towards directions other than the direction of the intended receiver. As shown in Figure 1, the goal of DM is to preserve the information symbol vector location in the I-Q space (desired symbol phase and amplitude) only towards the intended receiver's direction. In contrast, the symbol is moved to wrong locations in I-Q space in all other potential eavesdropper's directions. Ideally, the true symbol is mapped to a uniformly random symbol among all the possible symbols, such that

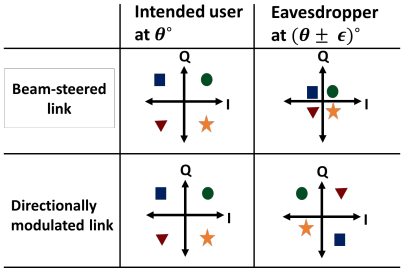


Fig. 1: Directional modulation vs. beam-steering

the received symbol in the eavesdropper's direction is equally likely to be any of the possible symbols. Moreover, DM ideally targets to update the transformation on the true symbol at the symbol transmission rate. In this way, an eavesdropper cannot know the instantaneous change of the true symbol, which leads her to decode the received symbol in error.

RMDM integrates a reconfigurable transmissive metasurface with the transmitter architecture to realize time-variant directional modulation. The goal of *RMDM* is to use the metasurface to change the symbol in the eavesdropper's (unknown) direction while ensuring that the metasurface is transparent in the direction of the intended user. To achieve this security feature, our solution is composed of two main parts, as shown in Figure 2.

B. Time-Varying Random Angular Misinformation

To achieve security with *RMDM*, the set of configurations that Alice uses must have two properties. First, for a fixed user location, the configurations must provide sufficient amplitude and phase changes to transform Eve's symbol to a different, wrong location in I-Q space. Second, each configuration must have an angular-dependent response so that the response for Bob and Eve is different.

To realize these properties, *RMDM* employs metasurface configurations with randomly encoded groups of meta-atoms. The idea is that every meta-atom will be randomly assigned an amplitude and phase shift from the set of available shifts that the meta-atom can produce. Because different meta-atoms will introduce different transformations, the signals scattered from the meta-atoms can either constructively or destructively interfere at random directions, resulting in a metasurface with a configurable random angular-dependent response. Accordingly, users at different angular directions relative to the metasurface will experience different responses from each configuration. Consequently, the information symbol vector moves to an unexpected location across the I-Q space which leads to misinformation in the eavesdropper's direction.

As one configuration can be learned by trial and error by Eve, Alice must use multiple configurations with different responses. Therefore, she pre-designs a set of configurations, each designed independently from the others following the random meta-atom selection procedure. This ensures that the responses experienced from different configurations at each location is different and depend on the randomly selected

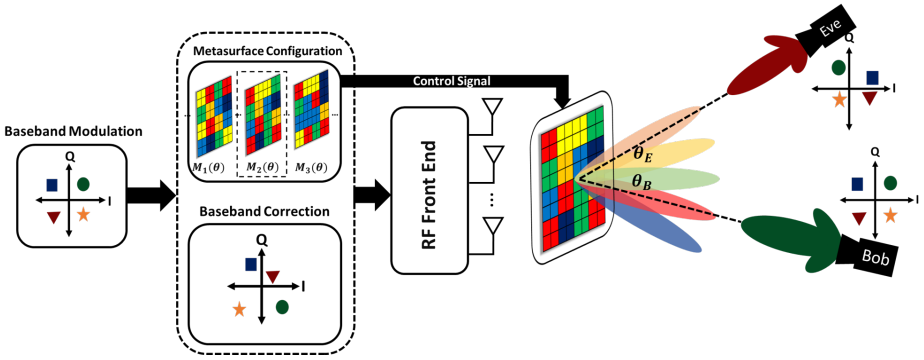


Fig. 2: *RMDM* system overview

meta-atoms composing the configuration. Ideally, Alice adopts a symbol-by-symbol random reconfiguration strategy. That is, prior to transmission of each symbol, Alice randomly selects one of the available configurations to create a new symbol transformation that is not predictable by Eve.

This design approach is general and can be realized with different types of meta-atoms. Different types of meta-atoms have different mechanisms of generating amplitude and phase shifts on the transmitted EM wave, e.g., by changing voltage biases across the meta-atom or by changing the geometrical parameters of the atom [25], [28]. Therefore, selecting a random phase shift for each meta-atom can be realized by randomly selecting a voltage bias or randomly selecting the geometrical parameters of the atom. Today's programmable metasurfaces can realize diverse responses: for example, in [17] up to 2^{16} responses per meta-atom are achievable.

C. Per-Configuration Baseband Correction

Because the metasurface changes the amplitude and phase of the transmitted symbol in *all* directions, it can also change the symbol in the direction of the intended receiver Bob. Therefore, in *RMDM*, to preserve the correct information symbol in Bob's direction, Alice modifies the information symbol at baseband according to the metasurface response experienced in Bob's direction. Therefore, the metasurface response of each configuration must be known by Alice for the covered range of angles. For this reason, Alice conducts *a priori* offline measurements to characterize the response of each configuration prior to establishing a link with Bob. In our model, we assume that both Bob and Eve are in the Line of Sight (LoS) of the metasurface. For this LoS scenario and a fixed transmitter set-up (the position and orientation of the metasurface with respect to Alice's antenna), the response of each configuration is deterministic. Therefore the measurements need to only be done once.

The information is used in a per configuration baseband correction procedure. The objective of the procedure is to eliminate the metasurface response in Bob's direction by adding a corrective gain and phase to the information symbol at Alice's baseband based on the metasurface response in Bob's direction. Due to the angular-dependent response of the metasurface, the correction and the metasurface response cancel each other only in Bob's direction. In contrast, an eavesdropper at a different angle will receive a different symbol, i.e., misinformation, due to both the metasurface's response in her direction and Alice's correction, as illustrated in Figure 2. Our approach in *RMDM* can be illustrated as follows: Let $M_i(\theta) = E_{M_i}(\theta)\ e^{j\phi_{M_i}(\theta)}$ denote the response of the i^{th} metasurface configuration at angle θ, where θ is the angular position of the receiver relative to the metasurface, $E_{M_i}(\theta)$ and $\phi_{M_i}(\theta)$ are the amplitude and phase response due to the metasurface at location θ, respectively. The symbol received at angle θ at discrete time k is given by:

$$y(k,\theta) = h(k,\theta)\ M_i(\theta)\ x(k) + n(k), \tag{1}$$

where $h(k,\theta)$ is the LoS channel gain between the metasurface and the receiver antenna. The transmitted information symbol at time k is denoted by $x(k) = E_s(k)e^{j\phi_s(k)}$, where E_s and ϕ_s are the amplitude and phase of the information symbol, respectively, and $n(k)$ is Additive White Gaussian Noise (AWGN) samples with variance σ^2. We assume that both Bob's angular position θ_B and Bob's channel $h(\theta_B)$ are estimated and known by both Alice and Bob. Moreover, we assume that Eve's channel $h(\theta_E)$ is known by Eve, but not Alice or Bob.

Once Bob's angle θ_B is known to Alice, she can securely transmit to Bob as follows. For each symbol, she first selects one of the pre-designed metasurface configurations uniformly at random. Next, she adds a corrective amplitude and phase to the information symbol based on the measured amplitude and phase changes occur in Bob's direction from the selected configuration. That is, for a selected configuration with response $M_i(\theta)$, instead of transmitting the information symbol $x(k) = E_s(k)e^{j\phi_s(k)}$, she transmits:

$$\begin{aligned}\tilde{x}(k) &= \frac{x(k)}{M_i(\theta_B)} \\ &= \frac{E_s(k)}{E_{M_i}(\theta_B)} e^{j(\phi_s(k) - \phi_{M_i}(\theta_B))},\end{aligned} \tag{2}$$

where, $\phi_{M_i}(\theta_B)$ and $E_{M_i}(\theta_B)$ are the phase and amplitude induced by the i^{th} metasurface configuration in Bob's direc-

tion. Accordingly, the received symbol at angle θ can now be written as:

$$y(k,\theta) = h(k,\theta)\ \tilde{M}_i(\theta)\ x(k) + n(k), \tag{3}$$

where $\tilde{M}_i(\theta))$ is the *effective* misinformation received at location (θ) due both the metasurface and Alice's modification to correct for the metasurface response at Bob's location. Consequently, it can be written as:

$$\tilde{M}_i(\theta) = \begin{cases} 1, & \theta = \theta_B \\ \frac{E_{M_i}(\theta)}{E_{M_i}(\theta_B)} e^{j(\phi_{M_i}(\theta) - \phi_{M_i}(\theta_B))}, & \theta \neq \theta_B \end{cases}.$$

We can see that in directions different than Bob's direction θ_B, Eve observes a transformation in both the amplitude and the phase of the information symbol. Therefore, the total misinformation Eve receives depends on how different the selected configuration response between Bob and Eve is.

D. Threat Model

The security achieved by *RMDM* is attributed to the transmitter's ability to dynamically transform the symbol vector to wrong locations across the I-Q space. Therefore the eavesdropper's symbol error rate (SER) can be used as a metric to quantify the error resulting from DM. However, SER does not necessary capture the error in the information since multiple bits can still be correct even if the symbol is in error. Therefore we use the eavesdropper's BER to evaluate the performance of *RMDM*. Specifically, we consider a certain location θ secure under a given modulation scheme, if an eavesdropper at that location decodes the information with an average BER of 0.5 since a BER of 0.5 means that the eavesdropper can not do better than a random guess between bit 0 and bit 1. In our threat model, we assume that both Bob and Eve are stationary and in the LoS of the metausrface. In addition the receivers decode the received symbol via maximum likelihood detection. Under maximum likelihood detection, the receiver divides the I-Q space between the constellation points into decision regions. The received symbol is mapped to a certain constellation point if it falls inside the boundaries of the corresponding decision region [18]. Thus, in our threat model, Eve does not attempt to learn which metasurface configuration is used (although if she does, this can be overcome by not repeating configurations;). Moreover, we consider only a single Eve and leave the case of multiple colluding Eves and a strong learning Eve to future work.

To achieve BER of 0.5, Alice must change Eve's symbol to a uniform random distribution across the I-Q space. For instance, to secure M-QAM, the distribution of phase shifts available must cover the 0 to 2π range with a resolution of $\frac{2\pi}{M}$, where M is the modulation order. In addition, a set of amplitude changes similar to the amplitude levels defined by the modulation order must be available. Thus, one symbol will equally likely appear in the decision regions of all the other symbols, resulting in an average BER of 0.5.

Example. Here we describe an example of how Alice can use *RMDM* to secure QPSK. Using QPSK modulation, there are 4 symbols that Alice can transmit. Each symbol represents one of the 4 possible bits combinations; 00, 01, 10, and 11. Under maximum likelihood, the decision region of each symbol is one of the 4 quadrants of the I-Q space. Hence, Alice needs to design a set of configurations that can move each symbol to the other 3 quadrants. For instance let the set of configurations have the following effective phase shifts at Eve's location: $\{90°, 180°, 270°\}$. In addition she can also switch the metasurface off, to realize a $0°$ phase shift. For each symbol transmitted Alice selects one of these 4 shifts uniformly at random. i.e., she selects one of the configurations with probability 1/4. Consequently, each symbol will equally likely appear in all 4 quadrants and is equally likely be decoded into the 4 possible bits combination. Table I shows Eve's estimation and the corresponding BER for the 16 different combinations of sent symbols and selected configurations. Moreover, the last column shows the average BER of each symbol. Notice that the resultant average BER of each symbol is 0.5. Moreover, Assuming that each information symbol is equally likely to be transmitted by Alice, then the average bit error probability at Eve reaches 0.5. Similarly, this analysis can be applied to any QAM or PSK modulation order.

TABLE I: Eve's average BER for different symbols transmitted and configurations selection.

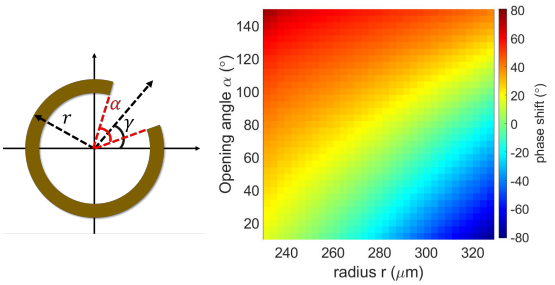
Sent symbol	Configuration selected (phase shift)				Avg. BER
	1 (0°)	2 (90°)	3 (180°)	4 (270°)	
00	00: 0	01: 0.5	10: 0.5	11: 1	0.5
01	01: 0	10: 1	11: 0.5	00: 0.5	0.5
10	10: 0	11: 0.5	00: 0.5	01: 1	0.5
11	11: 0	00: 1	01: 0.5	10: 0.5	0.5

III. Configuring *RMDM*

In this section we describe the process of designing metasurface configurations with groups of random meta-atoms. We first introduce the meta-atom structure we used to build the metasurface. Next, we describe the design steps that Alice follows to construct each configuration.

A. Meta-atom Structure

Meta-atoms can be realized with different structures and sizes depending on the targeted functionality and frequency of operation. Here, we adopt the C-SRR meta-atom, shown in Figure 3(a), as a building block for the metasurface. Although it has a simple structure, the C-SRR has a strong response to high frequencies and it has been used in many applications for mmwave and sub-THz frequencies [30]. Specifically , Alice can simultaneously control both the phase and amplitude of the transmitted wave by changing the geometry and the orientation of the C-SRR. The phase response of the meta-atom can be controlled by changing its radius r and its opening angle α, while the amplitude response can be adjusted by controlling the orientation angle γ [14], [30]. Provided by these design options, Alice can construct complex metasurface configurations with various responses to transform both the phase and amplitude of the EM signal in Eve's direction.



(a) Schematic of the C-SRR (b) Phase shifts

Fig. 3: C-SRR meta-atom and corresponding phase shifts

In order to characterize the phase and amplitude response of the C-SRR for a targeted frequency, Alice runs numerical simulations that compute the electric field response of the meta-atom for a set of geometrical parameters. For example, Figure 3(b) illustrates the phase response of the C-SRR meta-atom for a range of r and α values and for a fixed γ. The simulation is done in frequency domain using the commercial software COMSOL MultiPhysics for a wavelength $\lambda = 2$ mm (frequency $f = 150$ GHz). As can be seen from the figure, phase shift values spanning the range from 0 to π are achievable, allowing Alice a range of options to corrupt the phase of the symbol at Eve's direction. We note that the C-SRR can manipulate both the cross and co-polarized transmitted signals. However, here we focus on the former case due to the greater degrees of freedom that can be achieved [14].

B. RMDM Design Procedure

Here we apply *RMDM* to design a set of static metasurface configurations with random phase profiles. Figure 4 shows the steps followed to design each of the configurations. First, the metasurface is divided into a periodic square grid with sub-wavelength period l, in which a single meta-atom is positioned in each $l \times l$ cell.

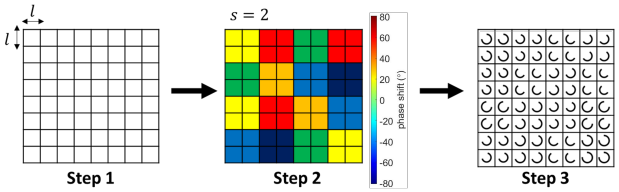


Fig. 4: Design steps of a random metasurface configuration

According to *RMDM*, for each cell, one phase shift value, and the corresponding C-SRR parameters r and α, are randomly selected from the available phase shift values provided by the phase map shown in Figure 3(b). However, placing meta-atoms with random sizes near each other may change the actual phase shift produced by each individual element [9]. This is due to the fact that the effective phase shift provided by each meta-atom is a result of both the resonance of each element along with the near-field coupling from neighboring elements. Therefore, placing meta-atoms with neighboring elements of different sizes can change the near-field coupling and accordingly the effective phase produced by each atom.

Hence, to minimize the error in the phase shift produced by each atom, instead of randomly selecting a phase shift value for each cell, one phase shift value is selected for a group of neighboring cells. That is, in step 2, first, each $s \times s$ cells are grouped into one group, where s denotes the group size. Next, one amplitude and phase shift value is randomly selected for each group, in contrast to each cell. Finally, in step 3 the metasurface configuration is built from meta-atoms with the corresponding r and α values obtained from the phase map.

IV. Experimental Evaluation

In practice, programmable C-SRR Meta-atoms have been fabricated via CMOS switches that can be shorted and opened to realize different combinations of the geometrical parameters (α and γ) to yield a range of phase and amplitude responses [25]. Specifically, in [25], 86 unique responses, corresponding to combinations of phase and amplitude changes are achieved per meta-atom. Moreover, real-time reconfiguration at gigahertz speed is also provided to yield sufficient symbol-rate switching for our purposes. Nonetheless, here, as a proof of concept, we utilize an easy-to-fabricate method to emulate a programmable metasurface with a sequence of static metasurface configurations. In this section, we first describe the metasurface fabrication technique and experimental set-up. Next, we present results from over-the-air experiments to evaluate the performance of *RMDM*.

A. Metasurface Fabrication

We employ the hot stamping technique, first introduced in [10], to fabricate the metasurface configurations. This inexpensive and rapid technique allow us to fabricate a set of different configurations such that we emulate a programmable metasurface that can be reconfigured into different configurations. To fabricate each configuration, first, the desired configuration pattern obtained from step 3 of the design procedure discussed in Section III-B is printed using a toner-based laser office printer. The pattern is printed on commercial glossy paper (Hammermill Papers) which we measured to have a refractive index of 1.8. Next, we place a thin aluminium-based foil sheet (iCraft Deco foil) that has a thickness of 40 μm on top of the printed pattern and the pair of sheets are passed through a laminator. Due to the high temperature of the laminator, the metallic powder of the foil is bonded with the toner, resulting in a metal pattern on top of the paper substrate. A picture of one fabricated configuration is shown in Figure 5.

B. Experimental Set-up

We use the TeraMetrix T-Ray 5000 TDS-THz system [8] to conduct our measurements. The system generates a picosecond time-domain THz pulse that is transmitted and received by two fiber-coupled sensor heads acting as a transmitter and a receiver as shown in Figure 5. The transmission power

is less than a micro-watt over the entire spectrum. Thus, with the extremely low transmit power, the maximum range is subsequently limited, and we set distances in our setup accordingly. A metal frame is used to mount the fabricated metasurfaces and they are positioned at a fixed distance 15 cm away from the transmitter. The metal frame and the transmitter are aligned such that the transmitted beam has normal incidence on the metasurface. The receiver is placed at a fixed distance of 45 cm in the LoS of the metasurface and can freely rotate to realize a range of angular directions.

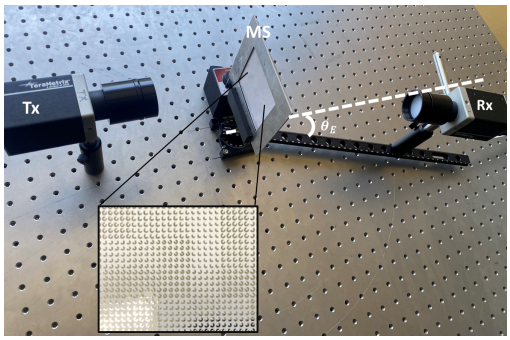


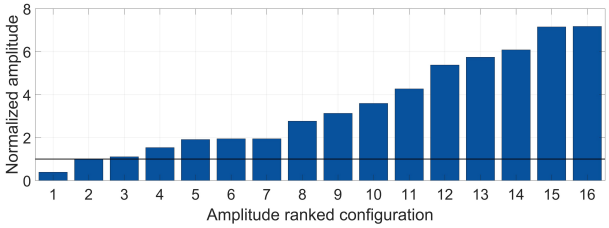
Fig. 5: Experimental setup used to evaluate the metasurfaces response in Eve's direction

C. Misinformation at Eve After Correcting for Bob

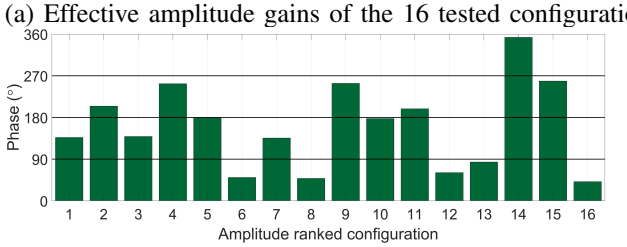
Here, we evaluate the effective symbol transformation at Eve due both the metasurface response and Alice's correction for the metasurface at Bob. Ideally, *RMDM* creates a random effective metasurface response at Eve for each configuration (to be changed per symbol), such that each symbol received by Eve is transformed to a random constellation point. In order to secure QAM, Alice needs to change both amplitude and phase at Eve, hence we analyze both amplitude and phase responses of the configurations at Eve's location. While *RMDM* ideally includes a large set of configurations that Alice uses to transform Eve's symbol, here as an example, we evaluate a set of 16 different metasurface configurations designed following the procedure discussed in Section III-B for a center frequency of 150 GHz. In particular, each metasurface is divided into a grid of 150×150 equally sized square cells. The length of the side of the cell l is chosen to be $\lambda/3 = 667\ \mu m$. The group size s is chosen to be 5 such that each 5×5 positions compose one group with atoms sharing the same C-SRR parameters. For each group, a pair of C-SRR parameters (α, r) is selected from the available values shown in the phase map shown in Figure 3(b). Recall that one pair (α, r) results in one phase and amplitude response. Next, the overall design is printed and fabricated following the hot stamping technique discussed above. We set Bob's location to have angle $\theta_B = 0°$ and Eve's location is angularly offset to $\theta_E = 8°$.

For each configuration, we measure the time signal at both Bob's and Eve's locations. The complex channel information, that is, both the phase and amplitude response for the targeted 150 GHz center frequency is extracted by performing fast-Fourier transform on the time signal. The process is repeated for all 16 metasurfaces. In order to decouple the channel response due to the metasurface from the static LoS channel, a reference signal is collected for the two locations without the metasurface. The collected measurements for the metasurfaces are normalized with respect to the channel information of the reference signal.

Furthermore, as discussed in II-C, since Alice corrects the basedband symbol according to the response at Bob's direction, the final effective symbol transformation seen at Eve is the ratio between the response at her location and the response at Bob's predetermined direction. Therefore, To evaluate the final response seen at Eve' location, for each configuration, the complex channel response measured at Eve's direction is divided by the value measured at Bob's direction.



(a) Effective amplitude gains of the 16 tested configurations



(b) Effective phase shifts of the 16 tested configurations

Fig. 6: Effective channel responses at $\theta_E = 8°$

The amplitude results are shown in Figure 6(a). The configurations are ranked according to the amplitude change induced by the configurations. As the values represent the ratio between the amplitude change at Bob's and Eve's locations, a value of 1 represents the same amplitude response at both locations.

Observe from the figure that different configurations have different effective amplitude changes between Eve and Bob. That is, even after correcting to cancel the metasurface response at Bob's location, Eve still experiences different amplitude changes across the configurations. The reason for this is twofold: First, as described in Section II-B, the configurations designed by *RMDM* have angular-dependent channel response. Thus, there is a difference between Bob and Eve's gain and phase even with the same configuration. Second, *RMDM* ensures that this difference in response varies across the different configurations because *RMDM* generates the configurations with random profiles, with each configuration generated independently from the others. Therefore, the 16 tested configurations create a range of effective amplitude changes ranging from 0.3 and up to 7. This behavior is critical for securing amplitude modulation schemes. Specifically, with this distribution, Alice can change the amplitude of a symbol

at Eve's location into different levels based on the modulation order used.

Figure 6(b) shows the phase responses of the configurations with the same ranking shown in Figure 6(a). The values represent the *difference* between phase responses at Bob's and Eve's location after Alice's correction. Therefore, 0° indicates that Bob and Eve experience the same phase shift as a result of using the metasurface configuration. Observe that even after the correction for the metasurface response at Bob's location, the random structures of the configurations result in different phase shifts added to the phase of the referenced signal. Moreover, the distribution of the effective phase shifts at Eve is spread across the 4 quadrants, covering the total constellation region from 0 to 2π.

Under the threat model presented in Section II-D, to secure a particular modulation order, Alice needs to be able to move each information symbol into all the decision regions of the other symbols at Eve. Hence for QAM and PSK schemes, the distribution of phase shifts at Eve's location must cover the 0 to 2π range, with a resolution that depends on the modulation order. For instance, Alice can use the above 16 tested configurations to secure 4-QPSK since she can move an information symbol at Eve to all four quadrants with multiple options in each quadrant. Note that while the 16 tested configurations can be used for QPSK, higher modulation orders will require Alice to generate more configurations to satisfy the resolution requirement as discussed in Section II-D.

Findings: *RMDM* ensures that even after correcting for Bob's direction, different configurations result in different channel responses at Eve's location compared to Bob's. In particular, *RMDM* provides multiple amplitude levels for Alice to change the symbol amplitude at Eve's location relative to Bob. Moreover, *RMDM* can generate relative phase shifts that cover 0 to 2π. Accordingly, Alice can use *RMDM* to both ensuring that Bob receives the correct symbol, while simultaneously ensuring that each configuration shifts Eve's response sufficiently to represent a different received symbol according to the modulation order and number of configurations.

D. BER Evaluation

Here, we study the security performance of *RMDM* by evaluating the BER of potential eavesdroppers at angular positions different than Bob. We consider that Eve determines the received signal by mapping the received gain and phase to the nearest constellation point via maximum likelihood detection [18]. We compare the performance of *RMDM* with the performance of a conventional beam steered towards Bob.

We use the same setup from the previous experiment shown in Figure 5. The distance between the transmitter and the receiver is 60 cm. A range of potential Eve's locations from -20° to 20° with a step size of 2° is considered. Bob's location is fixed at 0°. To study BER, we first measure the channel information of the metasurfaces at Eve's locations. Next, the measured channel information is used in a simulation of a pseudo-random symbol stream modulated at Alice and received and demodulated at Bob's and Eve's locations. The modulation order for the simulation is chosen based on Bob's measured SNR. That is, we select the modulation order such that Bob's BER does not exceed 10^{-4}. Moreover, the BER is calculated at each location as the ratio of the number of error bits to total bits.

First, as a baseline without the metasurface, we analyze the case of conventional beam steering towards Bob. Here, the transmitter shown in Figure 5 is aligned to achieve maximum gain towards Bob, located at 0° and the signal and noise power is measured at each location to characterize the beam directed towards Bob.

BER with and without RMDM: Next, we use the metasurface channel measurements to evaluate *RMDM*. Since the TDS platform used is incapable of transmitting modulated data, we use the channel measurements in a numerical evaluation to simulate PSK transmission between Alice and Bob. Specifically, a stream of 10^4 random 256-PSK symbols is generated at the transmitter. As described in Section II-C, Alice reconfigures the metasurface at the symbol transmission speed; therefore, for every symbol, one configuration from the available tested configurations is uniformly selected at random. The symbol is then modified based on the selected configuration's response measured at Bob's location. Next, for each Eve's location, the metasurface's response measured at the location is added to the modified symbol. Finally, white Gaussian noise with zero mean and variance equal to the noise power measured at the receiver location is added. This ensures that our measurement-based simulation is based on the signal and noise power measured at the receiver.

The same symbol stream is used for the conventional beamsteering case. However, in this case, only Gaussian noise is added to the transmitted symbol since no metasurface is used. At the receiver, the symbols are decoded and mapped to a set of binary bits following binary bit mapping. Finally, upon receiving the entire stream, the BER at each location is calculated as the ratio of the number of error bits to total bits.

The BER results are shown in Figure 7. We make the following observations: First, for conventional beamsteering, in the vicinity of Bob, the curve is flat and is near zero BER, indicating that Eve does nearly as well as Bob if she is within approximately $\pm 5^\circ$ of him. Moreover, even beyond this flat region, Eve's BER only slowly increases as her location becomes angularly farther away from Bob. This is because without the metasurface, Eve's BER depends solely on her SNR. Thus, since Eve's SNR decreases as her location becomes angularly farther from Bob, her BER increases.

In contrast, as targeted by Alice and Bob, with *RMDM*, Eve's BER sharply increases when she is located angularly away from Bob. For example, with *RMDM*, Eve's BER increases to greater than 0.3, only 2° away from Bob's location. On the other hand, with conventional beamsteering, Eve needs to be as far as 18° away from Bob for her BER to be greater than 0.3. The reason is that the dominant source of Eve's error in this case is the amplitude and phase change added to the symbol by the metasurface. Therefore, Eve's BER increase is

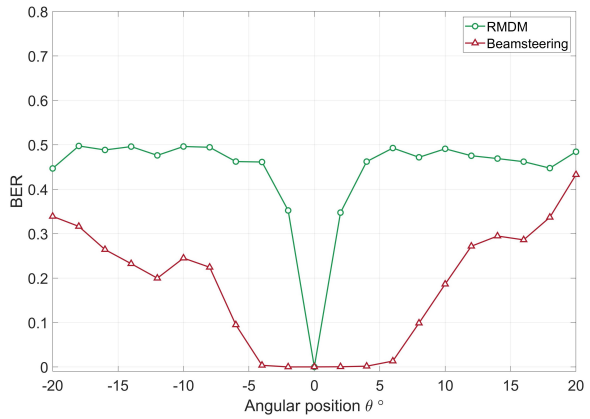


Fig. 7: BER for different Eve locations for Bob at $\theta_B = 0°$

dominated by the amplitude and phase transformations due to the metasurface rather than by Eve's reduced signal strength due to not being in the direction of the strongest signal.

Second, with *RMDM*, the BER at Eve's locations with $4°$ or greater angular separation fluctuates near Alice's targeted maximum value of 0.5, with an average value of 0.464 across Eve's locations. In contrast, with conventional beamsteering, the average value across Eve's locations is only 0.192. Note that the highest BER value achieved without the metausrface is 0.434, observed at the furthest Eve's location with $20°$ separation from Bob. Since without the metasurface, Eve's BER depends only on her SNR, she must be far away from Bob for her BER to reach 0.5. Whereas with *RMDM*, a BER of 0.497 can be realized at an angular separation of only $8°$.

Finally, recall that under the conditions presented in the model of Section II-D, Alice can increase the BER at a particular location for Eve up to the theoretical maximum value of 0.5 by generating 256 configurations with phases that correspond to the possible 256 PSK symbols. Nonetheless, since the configurations generated by *RMDM* are randomly scattered across the I-Q space and for this high modulation order, Alice can still achieve high average BER value across Eve's locations using only 16 configurations.

Findings: Under conventional beamsteering, given Eve's high SNR values, Eve's BER is near zero within $\pm 5°$ of Bob and it increases slowly as she is farther away from Bob's location, with an average value of 0.196, averaged over angles from $-20°$ to $+20°$. Only when Eve is very far away from Bob and hence has very low SNR can Eve's BER increase to near 0.5. In contrast, with *RMDM*, Eve's BER increases towards near 0.5 after only $4°$ angular separation from Bob's location, with an average value of 0.464 across the considered Eve's locations, thus forcing Eve to be extremely close to Bob for a successful attack. Moreover, although the theoretical conditions to guarantee an average BER of 0.5 are not met here, the experiment shows that Alice can increase Eve's BER to very close to 0.5, with far fewer configurations than what the model requires, potentially enabling simpler designs of *RMDM* in practice.

V. Prior work

DM Implementation with Antenna Arrays. Phased array DM (first proposed in [6]) was experimentally demonstrated in [7]: By switching the phase shifts of the antenna elements, the desired symbol can be created at a particular direction with minimum BER, while the BER is maximized at the unintended directions. DM has also been implemented with time modulated arrays (TMAs) [19]. in which the radiation pattern of the antenna array is changed with time to enforce dynamic spectrum aliasing at directions other than the direction of the intended receiver.

In comparison with the above antenna-based schemes, in this work, we propose a reconfigurable metasurface-based method to realize DM. In our scheme, the directional links are created via an Alice-controlled metasurface comprising a large 2-D array of meta-atoms. Our approach can be used with existing transmitter architectures regardless of the type or number of antennas used.

Thus, *RMDM* can be implemented with a phased array transmitter and achieve secure links without imposing a trade-off between beamforming gain and security. In contrast, antenna array based DM techniques usually sacrifice beamforming gain to achieve randomness at eavesdroppers directions. Thus *RMDM* is suitable for mmWave and sub-THz frequencies links, in which beamforming gain is very important. In addition, the sub-wavelength size of meta-atoms allows higher resolution phase and amplitude control per unit area compared to a phased array. As a result, greater variation of amplitude and phase can be achieved at the eavesdropper's direction with a metasurface compared to a phased array.

Security with Metasurfaces. Recent work studied the theoretical features of Intelligent Reflective Surfaces (IRS)-based physical layer security, including an IRS-based artificial noise scheme [5] and positional modulation (PM) [29]; see also [2] and the references therein. Other works have studied potential security concerns when an attacker is using a malicious IRS [4], [26]. Although these works present an early analysis on IRS potential contribution to physical layer security, no implementation or experimental evaluation has been introduced.

Lastly, few works provide experimental evaluation of configurable surfaces for security applications. For example, in [22], the authors propose an IRS-based physical layer key generation system to generate secure keys in static propagation environments. In addition, in [23] a countermeasure against adversarial wireless sensing is proposed. Likewise, an adversarial metasurfaces that enables eavesdropping on highly directional sub-THz links was introduced in [21]. Recent related work implemented directional modulation with reflective metasurfaces for sub-6 GHz bands [13], [27]. In contrast, in this paper, we present the first design and experimental evaluation of directional modulation at sub-THz frequencies. Our transmissive metasurface has a low profile of $10cm \times 10cm$, which makes it practical to be coupled with mmWave and sub-THz transmitter architectures. In addition, we show how modulation orders

(both amplitude modulation and phase modulation schemes) with high orders can be secured. This is due to the fact that the C-SRR have high-resolution phase and amplitude manipulation capabilities, allowing Alice to generate a secure set of configurations for any modulation scheme.

VI. Conclusion and Future work

This paper presents *RMDM*, a novel security system that enables the transmitter Alice to send time-variant directional misinformation in the eavesdropper's direction using a transmissive metasurface while ensuring that the legitimate user is receiving the correct information. We demonstrated how Alice can randomly reconfigure the meta-atoms of the metasurface to transform both the amplitude and the phase of each information symbol to a random value in Eve's direction. We further showed how Alice can modify her baseband signal to make the metasurface transparent in Bob's direction while still transmitting misinformation to Eve. Our experimental findings show that *RMDM* increases Eve's BER to near 0.5 at all directions beyond 4° angular separation from Bob, forcing her to be very close to Bob to intercept the information. In future work, we plan to implement *RMDM* using programmable C-SRR meta-atoms, e.g., via the CMOS architecture in [25].

VII. Acknowledgements

FH, ZS, and EK's research was supported by Cisco, Intel, and by NSF grants CNS-2148132, CNS-2211618, CNS-1955075, DOD: Army Research Laboratory grant W911NF-19-2-0269, and DOD: Army Research Instrumentation grant W911NF-23-1-0340. HG and DM's research was supported by NSF grants CNS-1954780, CNS-2211616 and Air Force Office of Scientific Research grant FA9550-22–1-0412.

References

[1] IEEE 802.11 Working Group. 2017. Enhanced throughput for operation in license-exempt bands above 45 GHz, IEEE P802.11ay/D0.3 (2017).

[2] A. Almohamad, A. M. Tahir, A. Al-Kababji, H. M. Furqan, T. Khattab, M. O. Hasna, and H. Arslan. Smart and secure wireless communications via reflecting intelligent surfaces: A short survey. *IEEE Open Journal of the Communications Society*, 1:1442–1456, 2020.

[3] S. Bi, T. Hou, T. Wang, Y. Liu, Z. Lu, and Q. Pei. Dywcp: Dynamic and lightweight data-channel coupling towards confidentiality in iot security. WiSec '22, page 222–232. Association for Computing Machinery, 2022.

[4] H. Chen and Y. Ghasempour. Malicious mmwave reconfigurable surface: Eavesdropping through harmonic steering. HotMobile '22, New York, NY, USA, 2022. Association for Computing Machinery.

[5] J. Chen, Y. Xiao, X. Lei, H. Niu, and Y. Yuan. Artificial noise aided directional modulation via reconfigurable intelligent surface: Secrecy guarantee in range domain. *IET Communications*, 16(13):1558–1569, 2022.

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

[7] M. P. Daly, E. L. Daly, and J. T. Bernhard. Demonstration of directional modulation using a phased array. *IEEE Transactions on Antennas and Propagation*, 58(5):1545–1550, 2010.

[8] I. Duling and D. Zimdars. Revealing hidden defects. *Nature Photonics*, 3(11):630–632, 2009.

[9] M. Dupre and L. Hsu. On the design of random metasurface devices. *Scientific Reports*, 8, 05 2018.

[10] H. Guerboukha, Y. Amarasinghe, R. Shrestha, A. Pizzuto, and D. M. Mittleman. High-volume rapid prototyping technique for terahertz metallic metasurfaces. *Optics Express*, 29(9), 2021.

[11] J. Jornet, E. Knightly, and D. Mittleman. Wireless communications sensing and security above 100 ghz. *Nature communications*, 2023.

[12] T. Kürner, D. M. Mittleman, and T. Nagatsuma. Introduction to thz communications. In *THz Communications*. Springer, 2022.

[13] X. Li, C. Feng, F. Song, C. Jiang, Y. Zhang, K. Li, X. Zhang, and X. Chen. Protego: Securing wireless communication via programmable metasurface. In *Proceedings of the 28th Annual International Conference on Mobile Computing And Networking*, MobiCom '22, page 55–68, New York, NY, USA, 2022.

[14] L. Liu, X. Zhang, M. Kenney, X. Su, N. Xu, C. Ouyang, Y. Shi, J. Han, W. Zhang, and S. Zhang. Broadband metasurfaces with simultaneous control of phase and amplitude. *Advanced Materials*, 26(29):5031–5036, 2014.

[15] J. Ma, R. Shrestha, J. Adelberg, C.-Y. Yeh, Z. Hossain, E. Knightly, J. Jornet, and D. Mittleman. Security and eavesdropping in terahertz wireless links. *Nature*, 563, 11 2018.

[16] B. Peng, K. Guan, A. Kuter, S. Rey, M. Patzold, and T. Kuerner. Channel modeling and system concepts for future terahertz communications: Getting ready for advances beyond 5g. *IEEE Vehicular Technology Magazine*, 15(2):136–143, 2020.

[17] L. Petrou, K. Kossifos, M. Antoniades, and J. Georgiou. The first family of application-specific integrated circuits for programmable and reconfigurable metasurfaces. *Scientific Reports*, 2022.

[18] J. G. Proakis. *Digital Communications*. McGraw-Hill, 1995.

[19] C. Qu, K. Chen, W. Long, Y. Chen, S.-W. Qu, J. Hu, and S. Yang. A vector modulation approach for secure communications based on 4-d antenna arrays. *IEEE Transactions on Antennas and Propagation*, 70(5):3723–3732, 2022.

[20] P. Sen, J. V. Siles, N. Thawdar, and J. Jornet. Multi-kilometre and multi-gigabit-per-second sub-terahertz communications for wireless backhaul applications. *Nature Electronics*, 6:1–12, 12 2022.

[21] Z. Shaikhanov, F. Hassan, H. Guerboukha, D. Mittleman, and E. Knightly. Metasurface-in-the-middle attack: From theory to experiment. WiSec '22, page 257–267, New York, NY, USA, 2022. Association for Computing Machinery.

[22] P. Staat, H. Elders-Boll, M. Heinrichs, R. Kronberger, C. Zenger, and C. Paar. Intelligent reflecting surface-assisted wireless key generation for low-entropy environments. In *2021 IEEE 32nd Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*, pages 745–751, 2021.

[23] P. Staat, S. Mulzer, S. Roth, V. Moonsamy, M. Heinrichs, R. Kronberger, A. Sezgin, and C. Paar. Irshield: A countermeasure against adversarial physical-layer wireless sensing. In *2022 IEEE Symposium on Security and Privacy (SP)*, 2022.

[24] D. Steinmetzer, J. Chen, J. Classen, E. Knightly, and M. Hollick. Eavesdropping with periscopes: Experimental security analysis of highly directional millimeter waves. In *2015 IEEE Conference on Communications and Network Security (CNS)*, 2015.

[25] S. Venkatesh, X. lu, H. Saeidi, and K. Sengupta. A high-speed programmable and scalable terahertz holographic metasurface based on tiled cmos chips. *Nature Electronics*, 3:1–9, 12 2020.

[26] Y. Wang, H. Lu, D. Zhao, Y. Deng, and A. Nallanathan. Wireless communication in the presence of illegal reconfigurable intelligent surface: Signal leakage and interference attack. *IEEE Wireless Communications*, 29(3):131–138, 2022.

[27] M. Wei, H. Zhao, Y. Chen, Z. Wang, T. J. Cui, and L. Li. Physical-level secure wireless communication using random-signal-excited reprogrammable metasurface. *Applied Physics Letters*, 122(5):051704, 2023.

[28] Z. Yaxin, Z. Hongxin, K. Wei, W. Lan, D. M. Mittleman, and Y. Ziqiang. Terahertz smart dynamic and active functional electromagnetic metasurfaces and their applications. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 378(2182):20190609, 2020.

[29] B. Zhang, W. Liu, Q. Li, Y. Li, X. Zhao, C. Zhang, and C. Wang. Metasurface based positional modulation design. *IEEE Access*, 8:113807–113813, 2020.

[30] X. Zhang, Z. Tian, W. Yue, J. Gu, S. Zhang, J. Han, and W. Zhang. Broadband terahertz wave deflection based on c-shape complex metamaterials with phase discontinuities. *Advanced Materials*, 25(33):4567–4572, 2013.