Metasurface-in-the-Middle Attack: From Theory to Experiment

Zhambyl Shaikhanov
Rice University
zs16@rice.edu

Fahid Hassan
Rice University
fh16@rice.edu

Hichem Guerboukha
Brown University
hichem_guerboukha@brown.edu

Daniel Mittleman
Brown University
daniel_mittleman@brown.edu

Edward Knightly
Rice University
knightly@rice.edu

ABSTRACT

Metasurfaces enable controllable manipulation of electromagnetic waves and have been shown to improve wireless communications in many diverse ways. In this paper, we define and experimentally demonstrate for the first time a "MetaSurface-in-the-Middle" (MSITM) attack. In this attack, the adversary Eve places a metasurface in the path of a directive transmission between Alice and Bob and targets to re-direct a portion of the signal towards herself, without being detected. In particular, we show how Eve can design a metasurface that induces abrupt phase changes at the interface of the metasurface to controllably diffract directional links and establish furtive eavesdropping links. We explore the theoretical foundations of the MSITM attack and demonstrate that an effective metasurface can be prototyped in under 5 min at the cost of several cents. We experimentally demonstrate the attack in a THz time-domain system and perform a set of over-the-air experiments. Our results indicate that the MSITM attack yields an acute vulnerability that can significantly reduce empirical secrecy capacity while leaving a minimal energy footprint, making the attack challenging to detect.

CCS CONCEPTS

• **Security and privacy → Mobile and wireless security**.

KEYWORDS

Adversarial Metasurfaces, Physical Layer Security, Terahertz

ACM Reference Format:
Zhambyl Shaikhanov, Fahid Hassan, Hichem Guerboukha, Daniel Mittleman, and Edward Knightly. 2022. Metasurface-in-the-Middle Attack: From Theory to Experiment . In *Proceedings of the 15th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec '22), May 16–19, 2022, San Antonio, TX, USA*. ACM, New York, NY, USA, 11 pages. https://doi.org/10.1145/3507657.3528549

WiSec '22, May 16–19, 2022, San Antonio, TX, USA

ACM ISBN 978-1-4503-9216-7/22/05…$15.00
https://doi.org/10.1145/3507657.3528549

1 INTRODUCTION

Metasurfaces are artificially engineered structures that exhibit customizable electromagnetic properties, even beyond what is available in nature [1]. Metasurfaces have been used to enhance wireless communication performance in numerous ways, e.g., relaying signals via transparent metasurfaces embedded in windows [2], mitigating antenna polarization mismatch with wall-integrated metasurfaces [3], and extending signal coverage through metamorphic surfaces on curtains and blinds [4]. Moreover, metasurfaces have been used to realize new security features [5, 6], e.g., generating physical layer keys [5] and radio-frequency fingerprints [6]. With the advancement towards 6G networks, metasurfaces are envisioned to become an even ubiquitous part of the environment [7–9], providing highly controllable steering capability of high data rate (Tb/sec), high directional, and high-frequency (0.1 to 1 THz) wireless links. Moreover, the Federal Communications Commission (FCC) has adopted regulations in 2019 to expedite the development of new services in the spectrum above 95 GHz [10] and high data rate THz transmission over a distance of more than 1 km have already been demonstrated [11, 12].

In this paper, we, for the first time, consider that the *adversary* employs a metasurface and demonstrate a new acute vulnerability to a diffractive *MetaSurface-in-the-Middle* (*MSITM*) attack. In particular, we make the following three contributions. First, we explore the strategy of the MSITM attacker and analyze the theoretical foundation of the attack. We show how the eavesdropper (Eve) can design and deploy a diffractive metasurface that can be hidden in the environment as a "bug," e.g., disguised as a part of the decoration or concealed among other objects in the area. Positioning it between the transmitter (Alice) and receiver (Bob), Eve intercepts the transmission and manipulates the electromagnetic waves of that transmission. Specifically, she alters the radiation pattern between Alice and Bob to simultaneously *(i)* establish a diffracted link directed towards Eve so that Eve can be located away from Alice and Bob and *(ii)* maintain Alice and Bob's legitimate communication link so that Eve can avoid detection. Eve's engineered radiation pattern beyond the surface enables her to control the angular direction of the eavesdropping link. To understand the attack, we study how Eve exploits the metasurface via analysis based on generalized Snell's law [13], which incorporates surface effects such as phase discontinuities introduced at the interface. We further employ Huygens' principle [14] to characterize the metasurface-induced radiation pattern. To evaluate the severity of the attack, we define the empirical secrecy capacity of the link in the presence of Eve's metasurface.

Second, we explore the design space of the attacker. In particular, we show that Eve has a wide range of design possibilities and investigate her key principles in realizing MSITM attack. Specifically, she first engineers subwavelength scale metallic resonators referred to as meta-atoms. They enable Eve to control the amplitude and phase of the transmission according to geometrical configurations and orientations of the meta-atoms. Eve then strategically arranges a group of meta-atoms to form a supercell and induce artificial and position-dependent phase discontinuity at the surface interface. By doing so, Eve can controllably scatter Alice's transmission and generate her targeted diffraction radiation pattern to herself and Bob. To demonstrate MSITM attack, we employ C-shape split-ring-resonator meta-atoms [15]. In this design, Eve controls the outgoing phase via the meta-atom's orientation β, and she controls amplitude via the radius r and slit opening α. We construct a supercell composed of eight different meta-atoms arranged to realize a position-dependent interfacial phase discontinuity that covers 2π across spatial period Γ. Subsequently, we show how Eve can successfully generate a diffraction peak as an eavesdropping link. To characterize MSITM attack, we perform finite element method simulations of the constituent meta-atoms and supercells. Specifically, we numerically simulate Maxwell's equations and analyze the amplitude and phase responses of the aforementioned elements. We demonstrate the existence of design choices that make the attack especially challenging to detect. Particularly, she employs a THz-transparent material as a metasurface substrate to intentionally let most of Alice's transmission energy pass through the metasurface and leave a minimal energy footprint at Bob. Last, we demonstrate the cross-polarization property of MSITM attack and show how Eve sets her polarization to intercept signals with high SNR.

Finally, we fabricate a suite of metasurfaces and perform extensive over-the-air experiments with a THz system. For that, we first demonstrate how Eve can leverage [16] to employ standard office supplies such as a printer, laminator, foil sheet, and glossy paper to quickly (under 5 min) and cheaply (several cents) fabricate the MSITM. We then experimentally characterize the prototyped metasurfaces and analyze the model that guides Eve's design. Our results reveal that Eve can diminish the empirical secrecy capacity of the Alice-Bob link by as much as 80%. Moreover, Eve can acquire significant signal power not only at her targeted frequencies but also across a wide range of communications bands, generating a large insecure zone induced by metasurface diffraction radiation patterns. Further, the MSITM attacker is robust to mispositioning as Eve can be even 10° away from her ideal eavesdropping location and still successfully carry out the attack. Despite being such a strong threat, we demonstrate that the MSITM leaves a minimal energy footprint at Bob, with only a few dB power loss. Because such a loss is not on the order associated with blockages, but rather with typical wireless channel variations due to, for example, a slight distance change between transmitter and receiver or a small-scale antenna orientation change, it is unlikely to trigger Alice and Bob's beam adaptation to steer away from the threat. Finally, our findings reveal that Eve is robust to metasurface tilting, even to large-scale angular changes such as 40°. She is also largely unaffected by moderate-scale surface rotation. However, large-scale rotations influence the attacker's eavesdropping location, yet the effect observed in practice is milder than the model prediction, yielding robustness to rotational angular changes. Thus, we consider the MSITM as a strong adversary that is difficult to detect and circumvent.

2 SYSTEM AND ADVERSARY MODEL

In this section, we first describe the threat model and discuss the attacker's eavesdropping topology. Next, we describe the malicious metasurface model and study how Eve's surface induces diffraction radiation to create eavesdropping links. Then, we define a security metric to quantify the severity of damage from the MSITM attack.

2.1 Threat Model and Topology

We consider that transmitter Alice sends her signal to receiver Bob that she wants to keep secret from an eavesdropper Eve. For that, Alice and Bob establish a highly directional line-of-sight link in frequencies from 100 GHz to 1 THz, which we broadly refer to as THz. Meanwhile, Eve aims to intercept Alice and Bob's secret information. While doing so, she also aims to avoid substantially obstructing, blocking, or otherwise hindering Alice and Bob's communication as it will make her presence easier to detect. For ease of demonstrating the attack principles, we consider a single Alice, Bob, and Eve in the network, and all communication parties are positioned at a similar elevation and employ similar hardware, abstracting the transmit and receive capabilities as a single point in space. We also consider that Eve knows the locations of the communicating parties, their center frequency f_c and bandwidth B, and if necessary, can rotate her antenna as needed to improve her signal reception.

To carry out the attack, Eve develops a metasurface that can diffract THz transmission, and positions it between Alice and Bob, possibly disguising it as a part of the environment. As shown in Figure 1, Alice's signal propagates in the medium and passes through the metasurface before reaching Bob. We designate the center of the surface as the origin of the coordinate system and θ corresponds to Eve's angle relative to Bob. Notice that, the metasurface does not need to be normal to the ray between Alice and Bob to carry out the attack and γ represents the incidence angle of the transmission. In general, the dimensions of the metasurface and the beam are considered to be in the appropriate scale such that Eve can capture sufficient energy for wavefront manipulation.

The adversary could carry out MSITM attack in a broad set of attack scenarios and across different contexts. For example, it

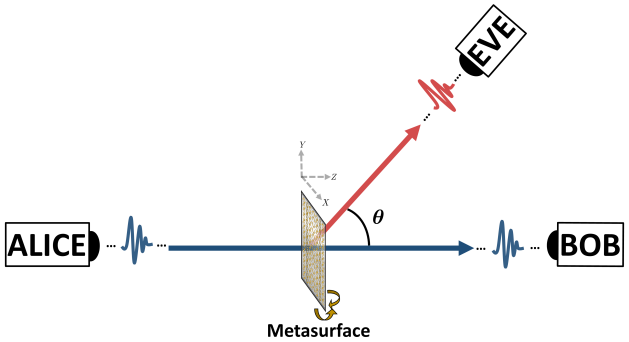


Figure 1: Overview of the MSITM attack

could be a WLAN scenario where Alice is an access point and Bob is a laptop or mobile client. Hiding the surface between THz transmissive objects, e.g., paper posters or plastic souvenirs, the attacker could be eavesdropping on sensitive data such as emails, financial, and other personal information. Similarly, the attacker could be eavesdropping on a point-to-point rooftop backhaul link, either a person standing in between buildings and positioning the metasurface accordingly to intercept transmission or an adversary drone carrying the metasurface and assisting the attack.

2.2 Malicious Metasurface Model

There is a broad class of metasurface designs available in the literature [9], which opens many possibilities for Eve. To demonstrate the MSITM attack, we model these surfaces as manipulating waves according to Huygens' principle [17]. This method provides perhaps the most comprehensive description of complex radiation patterns induced by most metasurfaces, although few types of surfaces, e.g., [18], might require an extension of the model or a different approach.

Building upon Maxwell's equations, we can express wavefront propagation as a propagation of an array of infinitesimal spherical waves. The radiation pattern emerging from the metasurface can then be described as a complex interaction of these waves passing through the structure. Considering the metasurface positioned orthogonally to the z-axis, we can derive the radiation pattern at any point (x', y', z') beyond the surface as [19]:

$$E(x', y', z') = \frac{z'}{j\lambda} \iint_{\Sigma} E(x, y, 0) \frac{e^{jkr}}{r^2} dxdy \tag{1}$$

where λ represents the wavelength and $E(x, y, 0)$ denotes the impinging plane wave $ae^{j\phi}$ with amplitude a and phase ϕ. Also, $r = \sqrt{(x - x')^2 + (y - y')^2 + (z')^2}$ designates the distance between the observation point and the point on the surface while k represents the wavenumber in the relevant medium. The expression $\frac{e^{jkr}}{r}$ describes the propagation of each spherical wave with radius r and $\frac{z'}{r}$ represents angular relation between the line connecting $(x, y, 0)$ and (x', y', z') and the z-axis. The factor $\frac{1}{j\lambda}$ in front of the integral ensures the right phase and field strength [20].

Notice that the integral in Equation (1) is computed as a Riemann sum and accounts for the field distribution across the metasurface. Then, the radiation pattern that Bob and Eve observe can be characterized as the aggregate impact of all individual spherical waves interacting with the surface and propagating towards their locations. To maintain coordinate system consistency across the paper, we further convert Cartesian form in Equation (1) to Polar form. Specifically, we designate radiation pattern at Bob as E^{Bob} and at Eve located at θ as $E^{Eve}(\theta)$. We further express their power intensities as the modular square of their radiation.

The MSITM attacker establishes an eavesdropping link by deflecting a portion of Alice and Bob's transmission towards herself. For that, Eve designs a metasurface that introduces a phase discontinuity at the surface interface. Specifically, she purposefully induces abrupt and position-dependent phase changes at metasurface. With a suitable phase discontinuity, Eve can deflect part of the outgoing transmission to potentially any direction [13]. For ease of exposition, we consider a surface that is periodic in the x-axis with spatial periodicity Γ and designate the phase discontinuity as $\Phi(x)$. We model the attacker's eavesdropping angle based on generalized Snell's law [13] as:

$$\theta = \sin^{-1}\left(\frac{\frac{c}{2\pi f_c}\frac{d\Phi(x)}{dx} + n_\gamma \sin(\gamma)}{n_\theta}\right) \tag{2}$$

where $\frac{d\Phi(x)}{dx}$ is the gradient of phase discontinuity, γ denotes the angle of incidence relative to the surface norm, and c is the speed of light. Also, n_γ and n_θ are refractive index the propagation medium, which we approximated by 1 due to the over-the-air transmission.

Observe that with zero phase discontinuity, $\Phi(x) = 0$, Equation (2) reduces to the standard Snell's law. In fact, the basic form $n_\theta \sin(\theta) = n_\gamma \sin(\gamma)$ describes the change in the direction of the incident wave due to different medium. However, a non-zero phase profile at the surface interface enables Eve to deflect outgoing transmission and generate an eavesdropping link. Identified as anomalous diffraction or anomalous deflection, this capability is unique to MSITM as other ordinary materials such as gratings and lenses can only acquire gradual phase changes and do not provide that degree of control over the wavefront [21]. To demonstrate Eve establishing an eavesdropping link, we investigate a malicious metasurface with linear phase profile along the x-axis with the phase gradient $\frac{d\Phi(x)}{dx} = \frac{2\pi}{\Gamma}$ and uniform amplitude [15]. We design the metasurface and perform finite element method simulation-based analysis in Section 3, fabricate the surface in Section 4, and perform experimental characterization in Section 5.

In general, we consider that Eve can have a programmable metasurface, changing Equation (1) dynamically in time as she chooses. This enables her to tune the eavesdropping angle in Equation (2) for her location. Moreover, Eve could instead have a static metasurface. Although not as versatile as a programmable one, for Eve, it is simpler to design and fabricate as it does not require switching components, and it is also easy to maintain since no power supply is required. Then, she will have to position herself correctly according to the geometry of her designed metasurface to receive a signal with high SNR. In this work, we will demonstrate the latter design.

2.3 Security Metric

To evaluate the MSITM attack, we quantify the security degradation Eve causes in the network. A common metric for the security of wireless channels is the secrecy capacity of the links [22]. It represents the signal quality advantage of Bob over the signal quality of Eve that can be used to securely encode a transmission.

We designate the signal-to-noise ratio at Bob and Eve as SNR^{Bob} and SNR^{Eve}, respectively. In our threat model, both Bob and Eve have a directional line-of-sight channel and experience similar channel gain. For ease of exposition, we consider that they are a similar distance away from the surface and thus have equal path loss. Obviously, if Eve is closer to the metasurface than Bob, then she will experience less path loss and thus higher SNR^{Eve}, giving her an advantage in the attack. However, this is a well-known effect described in the Friis transmission formula and we do not address it further.

As an empirical metric, we normalize secrecy capacity $B[\log(1+SNR^{Bob}) - \log(1+SNR^{Eve})]$ to the capacity without the MSITM attack. Specifically, we define the normalized secrecy capacity as:

$$\tilde{c} = \frac{\left[\log(1+SNR^{Bob}) - \log(1+SNR^{Eve})\right]^{+}}{\log(1+SNR^{Bob^{*}})} \tag{3}$$

where $SNR^{Bob^{*}}$ expresses the Bob's attack-free signal-to-noise ratio, and $[x]^{+} = max(x, 0)$. Observe that, the maximum value of $\tilde{c} = 1$ indicates that the link is secure and no transmission power was leaked to Eve. Conversely, decreasing $\tilde{c}$ is a sign of Eve successfully carrying out MSITM attack, with a minimum value of zero indicating that Eve has equal or more power compared to Bob and thus the secrecy capacity is zero.

3 ATTACKER DESIGN SPACE

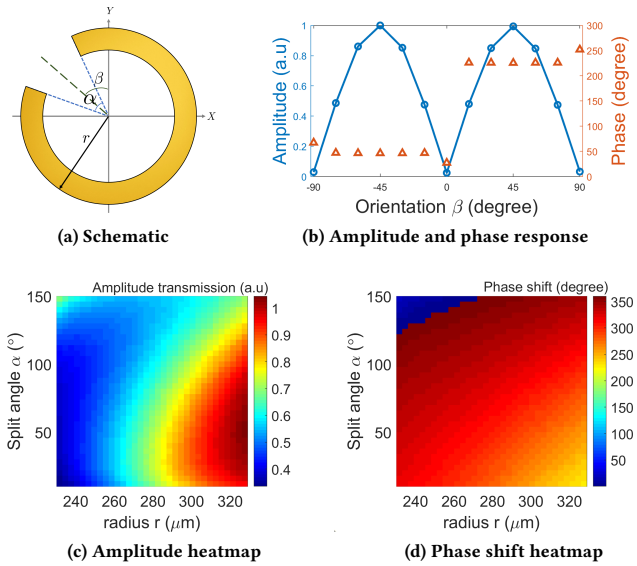
There are many design possibilities that Eve could exploit to realize MSITM attack. Yet, her key design principles are to (i) carefully construct subwavelength scale metallic structures, referred resonators or meta-atoms, and (ii) accurately arrange an array of these structures, referred supercells, to achieve interfacial phase discontinuities discussed in Section 2.2. Thereby, Eve can controllably scatter incident transmission and generate her targeted diffracting radiation pattern, establishing eavesdropping links.

To understand the attacker's design space, we discuss Eve's design choices and rationales. Demonstrating on C-shape [15] meta-atoms, we study Eve's strategy of manipulating phase and amplitude responses of meta-atoms based on their geometric configurations and orientations. We also explore how she generates supercells to create artificial abrupt phase shits at the surface interface. To analyze constituent elements of the metasurface, we perform finite element method simulations using multiphysics Comsol with varying geometric configurations and orientations. Without loss of generality, we consider Alice and Bob communicating at center frequency $f_c = 0.150$ THz with linearly y-polarized plane wave transmission and Eve's surface is normally incident to the transmission.

3.1 Meta-Atom Design

A meta-atom is a thin two-dimensional metallic resonator and a fundamental building unit of a metasurface. To realize MSITM attack, Eve first develops meta-atom resonators with proper geometrical configurations and orientations, each meta-atom contributing to the manipulation of the phase and amplitude of the outgoing transmission. For that, she could exploit a wide range of meta-atom structures with different shapes and sizes. For example, V-shape resonators, rectangular split-ring resonators, or rod-shaped resonators. To demonstrate the attack, we consider C-shape split-ring resonators that are known to have a stronger response at terahertz frequencies [15].

As shown in the schematic in Figure 2(a), the C-shape meta-atom comprises of radius r, opening angle α, and orientation angle β relative to y-axis. Having control over these parameters, Eve can simultaneously configure both the phase and the amplitude of the meta-atom for the targeted value. In particular, she configures the phase shift induced by the meta-atom by controlling geometrical parameters r and α, and she adjusts amplitude response by varying the



(a) Schematic (b) Amplitude and phase response

(c) Amplitude heatmap (d) Phase shift heatmap

Figure 2: Attacker exploits a C-shape meta-atom as a building unit of a malicious metasurface. (a) is a schematic view of the meta-atom and (b)-(d) are finite element method simulation results demonstrating controllable amplitude and phase responses.

orientation β. Importantly, C-shape meta-atoms have orthogonal-polarization characteristics [15]. That is, given, for instance, the y-polarized incident wave, the meta-atom significantly modulates the phase and amplitude of the wave in the x-direction. Therefore, Eve manipulates her radiation pattern in a cross-polarization regime and then orients her receiver to orthogonal polarization to that of incidence transmission to eavesdrop on the link.

To demonstrate how Eve adjusts the orientation of her meta-atoms and configures amplitude transmission, we compute the meta-atom electric field response with fixed r and α and varying β from -90° to 90°. We depict the results in Figure 2(b), showing orientation β in x-axis and the amplitude on the left side of y-axis. Shown in the blue line in Figure 2(b), observe that the amplitude profile has a symmetrical pattern as it follows the $|\sin(2\beta)|$ function. This is due to the excitation of symmetrical and anti-symmetrical modes in a C-shape resonator [15]. Specifically, scattered fields from both modes contribute to the orthogonally polarized output wave. Correspondingly, the amplitude reaches its maximum when the meta-atom is aligned along these mode axes at $\beta = -45^{\circ}$ and $\beta = 45^{\circ}$. It is also depicted as two spike peaks in Figure 2(b).

Another important feature of the meta-atom is that it induces π phase shift when rotated by 90°. That is, the outgoing orthogonal polarization changes by π when the meta-atom with fixed geometrical configurations r and α changes its orientation β by 90° along its central axis [15]. Meanwhile, the amplitude transmission of that meta-atom stays approximately the same. This is also depicted in Figure 2(b) in which the x-axis shows orientation β whereas the right y-axis depicts phase shift. In the orange scatter plot, notice that there is a phase jump of approximately π as β increases beyond zero. At the same time, the amplitude transmission stays the same

whenever the difference in β is approximately 90° as shown in the blue color line.

In general, Eve generates many meta-atoms and correctly arranges them as discussed in Section 3.2 to collectively induce phase discontinuity Φ in Equation (2). However, selecting the right geometrical configurations for each meta-atom such that they altogether produce the targeted response is a challenging as well as a cumbersome process. Strategic Eve is likely to produce a heatmap similar to one in Figure 2(c)-(d) to alleviate and expedite the procedure. Specifically, she generates the amplitude transmission (shown in Figure 2(c)) and phase shift (shown in Figure 2(d)) heatmap as a function of geometrical configurations of the meta-atom. Then, she can selectively choose appropriate geometrical configurations of the meta-atom for her targeted amplitude and phase shift response, leading to the supercell design in Section 3.2.

3.2 Supercell Design

The attacker constructs an array of meta-atoms and arranges them to induce the targeted phase discontinuity at the surface interface. Specifically, she generates a supercell that produces phase gradient $\frac{d\Phi}{dx} = \frac{2\pi}{\Gamma}$ and has uniform amplitude as discussed in Section 2.2. In other words, she aims to achieve a linear phase profile with 2π range across spatial period Γ while keeping similar transmission amplitude. Periodically organizing such supercells across the metasurface, Eve can diffract Alice's transmission and establish an eavesdropping link at θ degree angular location following Equation (2).

To realize such a supercell, Eve first generates and arranges four different meta-atoms. Specifically, each meta-atom is configured to produce $\pi/4$ phase shift relative to neighboring ones and have approximately identical amplitude. Eve can then rotate each structure by 90° to obtain an additional π phase shift as discussed in Section 3.1. She places them together with the former four along a line to form a supercell [15]. We demonstrate such a supercell design in Figure 3 and perform a finite element method simulation analysis of each constituent element. The results are illustrated in Figure 3 which depicts meta-atom structures on the x-axis and shows their respective amplitude transmission and phase shift on the left and right side of the y-axis. We designate amplitude in the blue curve and phase in the orange curve.

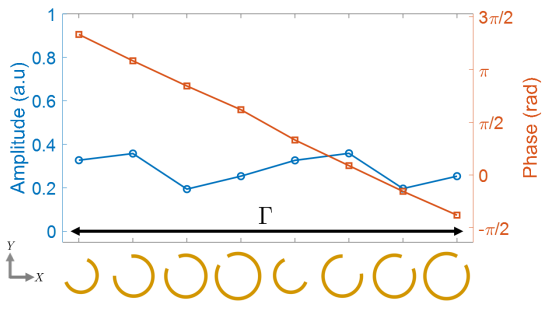


Figure 3: Eve constructs a supercell to induce a position-dependent and abrupt phase shift at the surface interface, thereby generating a diffraction radiation pattern.

Notice that transmission amplitude is approximately the same for each meta-atom while the phase shift has an increment of $\pi/4$ across neighboring meta-atoms and ranges between $\frac{-\pi}{2}$ and $\frac{3\pi}{2}$ across the entire supercell. Moreover, observe that the first four structures, from left to right, are oriented such that $\beta = 45°$ while the remaining four are rotated to 90° towards $\beta = -45°$. It demonstrates how Eve can achieve a linear phase profile of covering the range of 2π and maintain approximately similar amplitude. In general, Eve has many design choices. In the supercell in Figure 3, meta-atoms have geometrical parameters r = 240, 284, 296, and 320 μm with corresponding α = 136°, 82°, 32° and 12°, respectively, and Γ = 6.1 mm. However, she could equally achieve similar characteristics via different supercell structures by exploiting generic meta-atom features discussed in Section 3.1. Moreover, she could generate supercells for different central frequencies and eavesdropping angles configuring Γ and f_c accordingly to Equation (2).

To increase the overall efficiency of the MSITM attack, Eve jointly optimizes her design choices and subsequent fabrication process. In particular, she purposefully selects THz transparent materials, such as paper, as a substrate of her metasurface design in the fabrication. Doing so enables Eve to pass through most of Alice's transmission energy and leave a minimal energy footprint to make the attack more difficult to detect. Similarly, when selecting meta-atom geometrical configurations, Eve intentionally accounts for fabrication technique capabilities and limitations. For instance, given the achievable resolution of a fabrication technique, she might give preference to meta-atom structures with larger α and r to simplify the fabrication process as we describe in Section 4.

4 IMPLEMENTATION

In the following, we describe the low-cost and rapid metasurface fabrication technique that Eve employs in the MSITM attack. We then discuss the experimental setup we use to characterize and evaluate the attack in various settings.

4.1 Metasurface Fabrication

Traditionally, methods such as photolithography [23] are employed to fabricate metasurfaces. However, they are also costly and complex. Instead, we consider an adversary that exploits recent inexpensive and rapid fabrication alternatives such as the hot-stamping technique [16]. We explore Eve's fabrication methodology by characterizing the technique and prototyping the MSITM.

Convenient for Eve, the technique requires only standard office supplies, specifically, a toner-based printer, standard laminator, glossy paper, and inexpensive metallic foil. The adversary prints the design described in Section 3 on paper and then deposits metallization powder from the foil into the printed pattern. By doing so, Eve generates a metasurface with carefully arranged metallic structures on the THz transparent paper substrate as depicted in Figure 4(a). Consequently, she can controllably scatter an impinging transmission and establish diffracting eavesdropping links with that metasurface.

To prototype the MSITM, we first print the designed pattern using a Brother HL4150cdn printer and Hammermill glossy paper as shown in Figure 4(b). Next, we place an inexpensive iCraft Deco

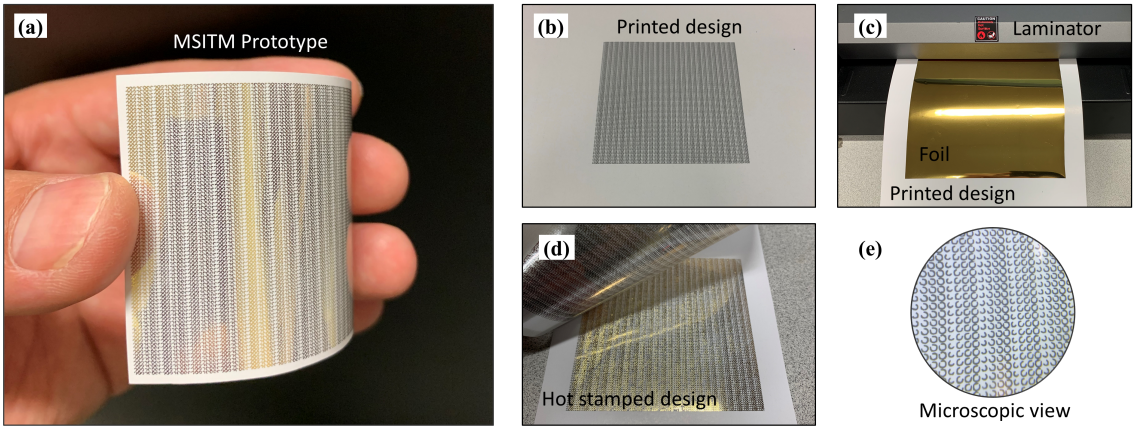


Figure 4: (a) is a prototype of the MSITM. Eve employs a low-cost and rapid fabrication method that involves (b) printing the designed pattern and (c) passing printed paper patterns along with metallic foil through a laminator. The surface (d) can also be cleaned with tape to remove excessive foil powder. (e) is a microscopic view of the fabricated metasurface.

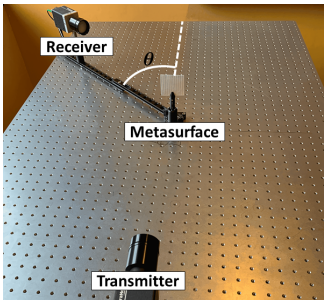


Figure 5: An experimental setup consists of a THz transmitter, receiver, and a metasurface in the middle

foil sheet on top of the printed pattern and pass it through a standard TruLam laminator at 263°F temperature, illustrating the process in Figure 4(c). With the foil containing a nearly 40μm thick layer of aluminum-based metallization powder, heat and pressure from the lamination allow the powder and toner to bond together. As a result, the metallic layer transfers on the printed pattern as shown in Figure 4(d). Several iterations of lamination could be performed to yield better bonding. Finally, the excess powder can be removed from the surface by cleaning it using tape.

Consequently, Eve can quickly fabricate the MSITM, spending less than 5 min per surface. She could even produce and deploy multiple metasurfaces in the environment, potentially making the attack even more sophisticated. Moreover, Eve can cheaply fabricate the metasurfaces as the process only involves standard office items. However, this technique also has its limitations such as the achievable resolution of printed design and non-perfect bonding between the powder and the toner. The impact of such fabrication artifacts is studied in Section 5.1.

4.2 Experimental Setup

We conduct the MSITM attack experiments using a TeraMetrix T-Ray 5000 TD-THz system [24]. The system has two fiber-coupled sensor heads acting as a transmitter and receiver. The terahertz transmitter generates wideband terahertz pulses that are received in real-time by the terahertz receiver. The system allows recording both the time-domain and frequency-domain signals. We place the transmitter and the receiver 1m apart from each other (due to the system's sub-μW transmit power) while positioning the fabricated metasurface 50cm from the transmitter. If not otherwise stated, the metasurface is placed such that transmitted beam has normal incidence to the surface as shown in Figure 5. Moving the receiver to $\theta = 0°$ designates Bob's reception whereas other locations are potential angular positions of Eve. We rotate the receiver 90° clockwise to set Eve's cross-polarized observation. In the experiment, we angularly move the receiver between $-90° < \theta < 90°$ with a resolution of 2° and collect both time-domain and frequency-domain data.

5 EVALUATION

In this section, we first experimentally characterize the MSITM and show how Eve configures her eavesdropping location in the attack. Next, we explore the secrecy degradation of Alice-Bob's link in the presence of MSITM attack and describe her robustness to mispositioning. Then, we analyze the impact of the attack on Bob and demonstrate the energy footprint that he observes. Finally, we investigate Eve's robustness to the metasurface orientation and analyze the impact of small to large-scale MSITM tilting and rotation at Eve.

5.1 Experimental Characterization of the Malicious Metasurface

Here, we analyze the first principles model in Equation (2) that Eve uses to guide her metasurface design and compute her eavesdropping location. We also experimentally characterize the malicious metasurface that she employs in the attack.

We consider the metasurface design presented in Section 3. Specifically, the surface is composed of periodic arrangements meta-atom with following (r, α, β) configurations: $(240\mu m, 136°, -45°)$,

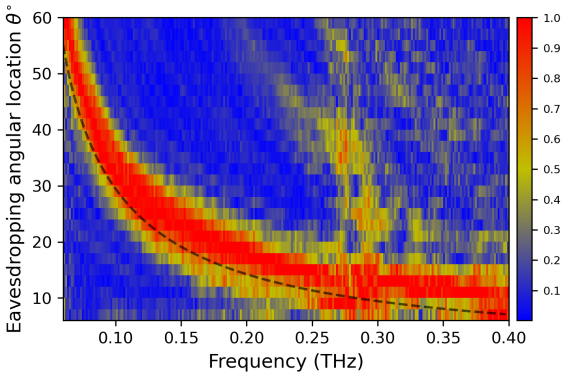


Figure 6: Experimental characterization of the MSITM (heatmap) and the first principles model (black dashed line)

$(284\mu m, 82^\circ, -45^\circ)$, $(296\mu m, 32^\circ, -45^\circ)$, $(320\mu m, 12^\circ, -45^\circ)$ and their 90° rotated counterparts. Accordingly, the spatial periodicity Γ is configured to $6.1mm$. We use the metasurface fabrication process described in Section 4 and the experimental setup in Section 4.2. In the experiment, we analyze the spatial and temporal characteristics of the radiation pattern emitting from the surface.

Figure 6 depicts the heatmap of the THz electric field amplitude with frequency on the x-axis and angle θ on the y-axis. We display θ values from 6° to 60° at an angular resolution of 2° and frequencies from 0.06 THz to 0.40 THz with a resolution of 1.43 GHz. We normalize the amplitude to a maximum value for each angular location θ. The color intensities from blue to red indicate increasing amplitude values. In the same Figure 6, we also plot the result of the first principal model derived from Equation (2), depicting it with the black dashed line.

Recall that Eve fundamentally exploits the model in Equation (2) to design her metasurface. That is, for the targeted center frequency, she configures metasurface parameters to eavesdrop on her desired location relative to Alice and Bob. For instance, Eve could decrease the radius r of the meta-atoms and the spatial period Γ of supercells in Section 3.1 to ultimately increase her eavesdropping angular location θ in Equation (2). Similarly, she could use the model to compute the ideal eavesdropping position given she employs a designed metasurface. Specifically, she can use f_c and θ relation in Equation (2) to compute her eavesdropping location for the metasurface design with configured Γ parameter. For example, she would ideally position at 19.1° to eavesdrop at f_c = 150 GHz as shown in the black dashed line in Figure 6. Thus, Eve employs the first principles model to design MSITM for her location and to compute her ideal eavesdropping location in the attack.

Eve can also experimentally pre-characterize her device before launching an attack to predict her performance and find her optimum angle. We demonstrate such a characterization in Figure 6. First, observe that Eve's fabricated metasurface design shares the trend of the angle-frequency coupled propagation pattern described in the model. That is, different center frequencies generally emit from the different angles exiting the metasurface as shown in red. This is also depicted as the black line, which is in the general area of the greatest intensities (red) in the figure. Moreover, Eve could choose her eavesdropping angle based on her experimental characterization of the metasurface. For instance, if she modeled and designed a device for 19.1° (black dashed line), but the true peak is at 22° (red), a few degrees off of her target, she can adjust her attack with an empirical characterization of the device. Thus, Eve can either pre-characterize the device and find the true peak or, if she hasn't done so, she can follow the model since Eve is generally robust to that scale of angular differences as we demonstrate in Section 5.2.

The experimental characterization also reveals differences between the model and experiments as well as irregularities. Specifically, the experimental results contain some randomly scattered peaks significantly farther away from those predicted by the model. These effects are mainly due to the fabrication imperfections described in Section 4.1. In particular, observe that the surface design has many meta-atoms with a small opening angle, e.g., $\alpha = 12^\circ$. However, precisely fabricating such elements with such small gaps is non-trivial with our rapid and low-cost fabrication technique. That is, hot stamping and transferring metallic dust from the foil to such a printed pattern with a small opening can result in bonding imperfections. In general, the fabrication quality will depend on many factors such as the quality of the printed pattern, the temperature of the laminator, and human effort. Observed irregularities in the heatmap are the cumulative impact of such factors.

In addition, notice that the experimental evaluation describes not only a peak frequency propagation emitting from the metasurface, but also provides additional details regarding peak-neighboring frequencies and their spatial radiation pattern. As we discuss later in the paper, such broad spectral and spatial characterization of the system is instrumental in analyzing MSITM attack features as well as understanding Eve's capabilities and strategies.

Finally, we discover that the observed intensity of the experimental diffraction peak pattern is non-uniform. That is, the shape of the pattern widens while the peak intensities slightly decrease at higher frequencies as shown in Figure 6. The reason is that in the employed THz system, higher frequency components are weaker compared to lower frequencies as described in Section 4.2. Hence, the signal level at these frequencies is more sensitive to measurement error and noise. This also explains the reason behind many irregularities mainly concentrated in higher frequency regions as observed in Figure 6.

5.2 MSITM Compromising Link Secrecy

Next, we investigate the secrecy degradation of the Alice-Bob link when Eve carries out the MSITM attack. Using the same experimental setup as previously, we consider Alice transmitting at f_c = 150 GHz with bandwidth B = 30 GHz. Meanwhile, Eve knows f_c and B and placed a metasurface between Alice and Bob. She aims to eavesdrop on the transmission.

Eve's Reception. First, we study how much signal power Eve obtains by diffracting Alice and Bob's transmission. For that, we consider Eve positions herself at the empirically optimal angular location 22° and present the results in Figure 7. We explore a broad range of frequencies in the x-axis, up to 500 GHz, and show her corresponding normalized signal power in the y-axis. As a baseline,

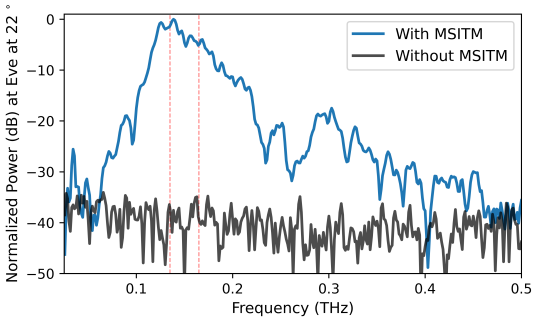


Figure 7: Eve with MSITM alters the legitimate directional transmission to receive more than 30 dB signal power relative to the baseline

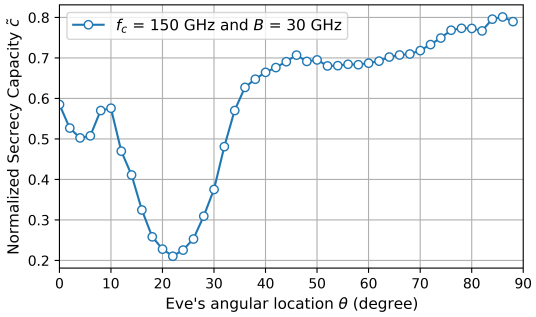


Figure 8: MSITM attacker diminishes up to 80% of the link security at her accurate eavesdropping location and she is also robust to moderate mispositioning

we consider the case when she does not launch the MSITM attack, presenting it in a black color line.

We discover that, without a metasurface to alter Alice's highly directional transmission, Eve largely observes noise fluctuating at around normalized power of −40 dB as illustrated in Figure 7. However, Eve can deflect a significant signal power to herself when she employs the MSITM in the attack. Indeed, observe that her metasurface enables her to receive over 30 dB more signal power relative to the baseline at her targeted center frequency. Thus, she can establish a diffraction peak eavesdropping link and compromises Alice and Bob's link secrecy that we demonstrate in the paper.

Our results also reveal that Eve receives non-negligible power at many other frequencies even though the device under test is specifically designed for her targeted $f_c = 150$. In particular, she acquires a very large range of communication bands spanning between $50-450$ GHz. Even at a further 450 GHz, she obtains a power increase of approximately 8 dB as shown in Figure 7. However, if, for instance, Alice and Bob were communicating at 450 GHz in the first place, Eve would not simply lose the remaining 22 dB, but would rather prefer to have the metasurface redesigned. Particularly she would employ Equation (2) and reconfigure meta-atoms and supercells to be optimized for the different f_c.

Secrecy Capacity. Next, we explore the secrecy capacity of the Alice-Bob link in the presence of the MSITM attack. For that, we compute the normalized secrecy capacity of the link given by Equation (3) and present the results in Figure 8. The x-axis depicts Eve's angular location θ and the y-axis shows normalized secrecy capacity $\tilde{c}$.

We find that Eve diminishes approximately 80% of the security of the link positioning at her true peak location, a large reduction in secrecy capacity, indicating that the MSITM attack is a highly effective attack and serious threat. Specifically, Eve decreases $\tilde{c}$ to approximately 0.2 by eavesdropping at 22°. Then, if Alice and Bob know that Eve is tampering with the transmission, they can still be secure through coding, but would lose 80% of the data rate. However, if they do not know the MSITM presence, then secrecy is severely compromised [22].

Moreover, our experiments reveal that Eve does not have to be positioned precisely to successfully eavesdrop on the link. Since she has significant receive power at many locations other than the peak shown in Figure 6, she is a threat across a wide range of θ. For example, she can be approximately 10° off from her peak position and still reduce the normalized secrecy capacity to below 0.5. This is particularly relevant when Eve's ideal location in the model does not exactly match the experimentally characterized best position, which can be off by several degrees as discussed in Section 5.1. Then, the results in Figure 8 indicate that Eve is indeed robust to moderate mispositioning and she can successfully carry out the attack even from off-peak locations. In general, Eve going beyond 35° results in $\tilde{c} > 0.6$ because θ is too far from the peak location and there is a significant signal power decrease at Eve at those locations. Similarly, normalized secrecy capacity remains above 0.5 in the region between $0° \leq \theta \leq 10°$ because Eve is eavesdropping on an orthogonally-polarized transmission to that of what Bob (who in contrast obtains much greater signal power at different polarization as described in Section 5.3).

Insecure Zone. Finally, we study the insecure zone induced by Eve carrying out the MSITM attack. In particular, we create a map with the normalized security threshold below which the Alice-Bob link is considered compromised. To do so, we employ the normalized secrecy capacity Equation (3) with an exemplary threshold value $\tilde{c} = 0.4$ (e.g., representing the threat level that Alice and Bob have encoded to protect against). We present the result in

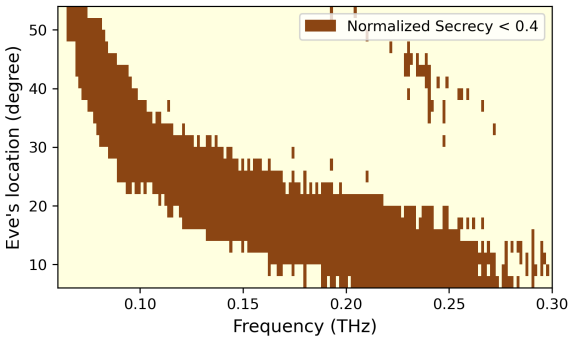


Figure 9: Malicious metasurface-induced insecure zone

Figure 9, showing frequency and eavesdropping angles in the x-axis and y-axis, respectively. The below-threshold insecure region is highlighted in brown whereas the above-threshold secure region is shown in yellow.

The figure illustrates that nearly 30% of the region is insecure. Expectedly, the insecure region follows the angle-frequency couple propagation pattern presented in Figure 6. Thus, any transmission configurations following in the brown area will result in compromised security of the Alice-Bob link. Notice that there are some arbitrarily scattered insecure areas in the map, which could potentially be exploited by Eve for eavesdropping opportunistically.

5.3 Impact at Bob

Here we explore the impact of the MSITM attack on Bob, as disruption to Bob's communication link could alert him to the attack. In particular, we analyze degradation of transmission power at Bob due to the presence of the MSITM in the path of the Alice-Bob link. Then, we study the implications of the attack for Alice and Bob's beam steering.

In this experiment, we consider the same setup as previously to study the energy footprint at Bob. We present the results in Figure 10, showing frequencies up to 1 THz in the x-axis and received signal power in the y-axis. We depict Bob's observed power in the presence of the MSITM in red and include two baseline references in the analysis: no intermediate surface with clear line-of-sight between Alice and Bob (green curve) and complete transmission blockage (black curve). To realize a completely blocked transmission, we place a plain metallic plate between Alice and Bob.

First, observe that higher frequency components, above 200 GHz, are weaker compared to the lower frequencies, both with and without the MSITM (red and green respectively). This is due to the characteristics of the THz illumination source. Also, notice the existence of several significant dips near 550 GHz, 750 GHz, and 1 THz. Those are the impact of atmospheric absorption, such as water vapor gases, that causes transmission attenuation at these frequencies. Unsurprisingly, a completely blocked link results in a significant power drop at the intended receiver, and its shown in the black curve in Figure 10.

Moreover, we discover that the power spectrum observed by Bob with MSITM is quite similar to the one when there is no MSITM, with a modest some downward shift. Indeed, the fluctuations of

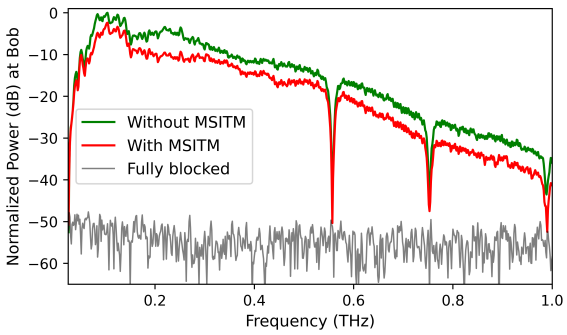


Figure 10: MSITM attack from perspective of Bob

the red curve closely resemble the changes in the original green one across different frequencies. Thus, at Bob, the MSITM induces only a few dB power reduction that is nearly uniform across the spectrum. This indicates that Eve's MSITM attack is quite efficient and effective in deflecting power to herself such that Bob experiences only a few dB (3 − 4 dB) signal power loss at his end and the dynamics of the power spectrum he observes with and without the metasurface is not easily distinguishable.

Unfortunately for Alice and Bob, a few dB power loss is characteristic of many wireless channels and would be unlikely to impact Alice and Bob's beam steering decision. In fact, slight distance change between communicating entities, such as minor mobility, also causes a similar few dB path-loss shift, which is especially common at these high THz frequencies. Similarly, antenna misalignment, e.g., small-scale orientation change, can yield similar effects. In such cases, the transmitter usually employs rate adaptation to adjust the data rate based on the newly available SNR, e.g, 802.11ay [25]. In more extreme SNR degradation cases, e.g., blockage and 10's of dB power loss, beam adaptation is triggered since Alice and Bob's link becomes exceedingly deteriorated and a new path is required [26]. Thus, in the MSITM attack, Eve intentionally leaves a minimal energy footprint to avoid triggering Alice and Bob to re-steer, yielding a challenging adversary to detect and circumvent. Moreover, Eve is also an efficient attacker. She re-directs only around 3dB of Bob's power relative to his attack-free case (shown in Figure 10) to acquire more than 30dB power relative to not having the MSITM, a case in which she largely observes noise (shown in Figure 7).

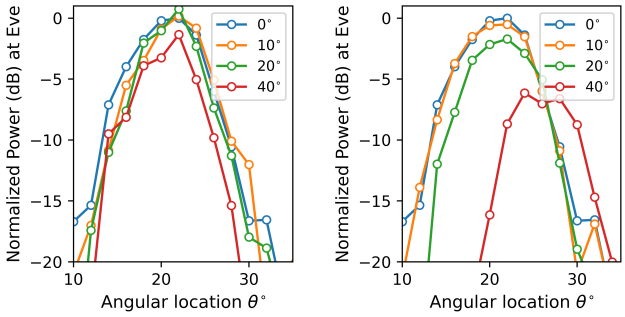
5.4 Eve's Robustness to Metasurface Orientation

Thu far, we investigated the case that the MSITM is positioned with normal incidence to Alice's transmission. However, in some attack scenarios, such accurate surface placement might be infeasible for Eve. Here, we study Eve's robustness to metasurface orientation by analyzing diffraction radiation patterns from oblique incidence.

Building upon the previous experimental setup, we rotate and tilt the metasurface, and record Eve's corresponding normalized signal power. In particular, we first tilt the surface around the x-axis in the counter-clockwise direction between 0° to 40°. We then rotate the surface around the y-axis in the counter-clockwise direction from 0° to 40°. Effectively, this is equivalent to changing the incident angle γ in Equation (2). Throughout the experiment, the metasurface encompasses the entire transmission beam.

We depict the result in Figure 11, showing Eve's angular location in the x-axis and her observed signal power in the y-axis. As a baseline reference, we consider a metasurface with normal incidence illustrated as 0° in the blue curve, while angular changes of 10°, 20°, and 40° are shown in orange, green, and red respectively. For convenience, we refer to them as small-scale, moderate-scale, and large-scale angular change, respectively.

First, we discover that the MSITM is robust to tilting, even with large-scale angular changes. In fact, despite orienting the metasurface to various tilting angles, all curves (orange, green, and red) reach their peak at Eve's true peak location at $\theta = 22°$ as shown in Figure 11(a). In addition, in all different tilting instances, Eve's signal power is similar to that of the baseline, albeit with a slight power



(a) Tilting the metasurface **(b) Rotating the metasurface**

Figure 11: Impact of MSITM orientation

decrease in 40°. Most likely, because the constituent meta-atoms are spatially periodic in the x-axis, the metasurface tilted around the x-axis is capable of accurately maintaining its original abrupt phase-shifting property and cross-polarized scattering power. Thus, Eve's cross-polarized eavesdropping link stays relatively similar to the baseline in terms of both diffracted angle and diffracted signal power.

Unlike tilting, rotation of the surface results in a non-negligible difference at Eve. Specifically, large-scale rotation of the surface results in a 4° shift of Eve's peak location towards the right relative to the baseline as depicted in Figure 11(b). The reason is that γ rotation of the metasurface induces additional $\sin(\gamma)$ deflection. However, because of the sinusoidal relationship, this effect becomes dominant only when the metasurface rotation undergoes large-scale angular change, and otherwise has minimal impact [27]. Our experimental results depicted in the yellow and green curves in Figure 11(b) also confirm this. In principle, if Eve knows γ (e.g., she purposefully positioned the MSITM in the attack), then she can predict the total expected diffraction angle because the $\sin(\gamma)$ effect is already incorporated in her metasurface model in Equation (2).

However, we also find that the model overestimates the impact of metasurface rotation compared to the experiment. In particular, with $\gamma = 40°$, the model predicts Eve's peak angular location to be 36° while in the experiments, it is approximately 26° as shown in the red curve in Figure 11(b). This model and experiment mismatch is likely due to multiple underlying idealistic assumptions in the model, such as perfectly fabricated metasurface design and perfectly collimated THz beams. In practice, however, metasurface fabrication incurs imperfections while beams are collimated only to a certain degree. Importantly, disagreement between the model and the experiment favors Eve in the MSITM attack. Specifically, if Eve does not know the metasurface rotation angle (e.g., it was changed externally), in practice, her peak eavesdropping location is less affected by the surface rotation and she is even within the robust mispositioning range discussed in Section 5.2.

6 RELATED WORK

Metasurfaces and Security. Due to their wavefront manipulation capabilities, metasurfaces have been extensively investigated in the literature to improve wireless networks performance and enable new security features [2–6, 28–32]. Yet, very few works consider the converse when the adversary designs and employs a metasurface to realize new advanced security threats. Related work explores intelligent surfaces capable of controllably reflecting spread out signals and studies reflection-induced jamming [33] and pilot spoofing [34] attacks with numerical simulations. In contrast, we investigate transmissive metasurfaces that can be in the line-of-sight path between Alice and Bob. In this context, we demonstrate the first adversarial metasurface attacking a highly directional link, and expose the acute eavesdropping vulnerability. We also provide the first theory to experimental work to study metasurface security features in THz links.

Man-in-the-Middle Attack. An adversary covertly inserted between legitimate communication parties is termed a Man-In-The-Middle (MITM) attack [35]. For example, impersonating a legitimate device, a MITM attacker targets to compromise the confidentiality and integrity of sensitive data. Recognized as one of the most devastating security threats in the literature, such attacks have been extensively explored in the prior work [36–39]. The name MSITM is inspired by that scenario. However, in contrast to a prior MITM attack, the adversary in the MSITM attack exploits advanced metasurface designs to secretly intercept high data rate directional links and artificially manipulates electromagnetic waves of the transmission for establishing diffractive eavesdropping links. Similar to the MITM attack, this yields a strong adversary capable of compromising the security of the legitimate links while leaving a minimal attack footprint.

7 CONCLUSION

In this paper, we define and experimentally demonstrate for the first time the MSITM attack. We explore the theoretical foundations for such an attack and show how Eve designs her metasurface to induce phase discontinuity at the surface interface and controllably generate diffraction radiation patterns, establishing diffraction eavesdropping links. We also demonstrate that Eve, unfortunately, can realize such a sophisticated attack rapidly and cheaply with common office supplies. Our experimental results reveal that Eve can severely reduce the empirical secrecy capacity of legitimate links while also leaving a minimal attack footprint, making the attack both devastating and challenging to detect.

8 ACKNOWLEDGEMENTS

This research was supported by Cisco, Intel, and by NSF grants CNS-1955075, CNS-1923782, CNS-1824529, CNS-1801857, NSF-1923733, NSF-1954780 and DOD: Army Research Laboratory grant W911NF-19-2-0269.

REFERENCES

[1] Alexander V Kildishev, Alexandra Boltasseva, and Vladimir M Shalaev. Planar photonics with metasurfaces. *Science*, 339(6125), 2013.
[2] Daisuke Kitayama, Yuto Hama, Kenta Goto, Kensuke Miyachi, Takeshi Motegi, and Osamu Kagaya. Transparent dynamic metasurface for a visually unaffected reconfigurable intelligent surface: controlling transmission/reflection and making a window into an rf lens. *Optics Express*, 29(18):29292–29307, 2021.
[3] Lili Chen, Wenjun Hu, Kyle Jamieson, Xiaojiang Chen, Dingyi Fang, and Jeremy Gummeson. Pushing the physical limits of iot devices with programmable metasurfaces. In *18th USENIX Symposium on Networked Systems Design and Implementation (NSDI 21)*, pages 425–438, 2021.

[4] R Ivan Zelaya, Ruichun Ma, and Wenjun Hu. Towards 6g and beyond: Smarten everything with metamorphic surfaces. In *Proceedings of the Twentieth ACM Workshop on Hot Topics in Networks*, pages 155–162, 2021.

[5] Long Jiao, Guohua Sun, Junqing Le, and Kai Zeng. Machine learning-assisted wireless phy key generation with reconfigurable intelligent surfaces. In *Proceedings of the 3rd ACM Workshop on Wireless Security and Machine Learning*, pages 61–66, 2021.

[6] Sekhar Rajendran, Zhi Sun, Feng Lin, and Kui Ren. Injecting reliable radio frequency fingerprints using metasurface for the internet of things. *IEEE Transactions on Information Forensics and Security*, 16:1896–1911, 2020.

[7] Ian F Akyildiz, Ahan Kak, and Shuai Nie. 6g and beyond: The future of wireless communications systems. *IEEE Access*, 8:133995–134030, 2020.

[8] Yuanwei Liu, Xiao Liu, Xidong Mu, Tianwei Hou, Jiaqi Xu, Marco Di Renzo, and Naofal Al-Dhahir. Reconfigurable intelligent surfaces: Principles and opportunities. *IEEE Communications Surveys & Tutorials*, 2021.

[9] Marco Di Renzo, Alessio Zappone, Merouane Debbah, Mohamed-Slim Alouini, Chau Yuen, Julien De Rosny, and Sergei Tretyakov. Smart radio environments empowered by reconfigurable intelligent surfaces: How it works, state of research, and the road ahead. *IEEE Journal on Selected Areas in Communications*, 38(11):2450–2525, 2020.

[10] U.S. Federal Communications Commission. 2019. FCC Opens Spectrum Horizons for New Services and Technologies. . https://www.fcc.gov/document/fcc-opens-spectrum-horizons-new-services-technologies/.

[11] Akihiko Hirata, Toshihiko Kosugi, Hiroyuki Takahashi, Jun Takeuchi, Hiroyoshi Togo, Makoto Yaita, Naoya Kukutsu, Kimihisa Aihara, Koichi Murata, Yasuhiro Sato, et al. 120-ghz-band wireless link technologies for outdoor 10-gbit/s data transmission. *IEEE Transactions on Microwave Theory and Techniques*, 60(3):881–895, 2012.

[12] Thomas Kürner, Daniel M Mittleman, and Tadao Nagatsuma. Introduction to thz communications. In *THz Communications*, pages 1–12. Springer, 2022.

[13] Nanfang Yu, Patrice Genevet, Mikhail A Kats, Francesco Aieta, Jean-Philippe Tetienne, Federico Capasso, and Zeno Gaburro. Light propagation with phase discontinuities: generalized laws of reflection and refraction. *Science*, 334(6054):333–337, 2011.

[14] Eugene Hecht. *Optics, 5e*. Pearson Education, 2002.

[15] Xueqian Zhang, Zhen Tian, Weisheng Yue, Jianqiang Gu, Shuang Zhang, Jiaguang Han, and Weili Zhang. Broadband terahertz wave deflection based on c-shape complex metamaterials with phase discontinuities. *Advanced Materials*, 25(33):4567–4572, 2013.

[16] Hichem Guerboukha, Yasith Amarasinghe, Rabi Shrestha, Angela Pizzuto, and Daniel M Mittleman. High-volume rapid prototyping technique for terahertz metallic metasurfaces. *Optics Express*, 29(9):13806–13814, 2021.

[17] Justin Peatross and Michael Ware. Physics of light and optics. In *Laser Science*, page JWA64. Optical Society of America, 2010.

[18] Lei Zhang, Xiao Qing Chen, Shuo Liu, Qian Zhang, Jie Zhao, Jun Yan Dai, Guo Dong Bai, Xiang Wan, Qiang Cheng, Giuseppe Castaldi, et al. Space-time-coding digital metasurfaces. *Nature communications*, 9(1):1–11, 2018.

[19] Joseph W Goodman. Introduction to fourier optics, roberts & co. *Publishers, Englewood, Colorado*, 2005.

[20] Justin Peatross and Michael Ware. Physics of light and optics.

[21] Xiaoqiang Su, Chunmei Ouyang, Ningning Xu, Wei Cao, Xin Wei, Guofeng Song, Jianqiang Gu, Zhen Tian, John F O'Hara, Jiaguang Han, et al. Active metasurface terahertz deflector with phase discontinuities. *Optics express*, 23(21):27152–27158, 2015.

[22] Joao Barros and Miguel RD Rodrigues. Secrecy capacity of wireless channels. In *2006 IEEE international symposium on information theory*, pages 356–360. IEEE, 2006.

[23] Oleksandr Sushko, Melusine Pigeon, Robert S Donnan, Theo Kreouzis, Clive G Parini, and Rostyslav Dubrovka. Comparative study of sub-thz fss filters fabricated by inkjet printing, microprecision material printing, and photolithography. *IEEE Transactions on Terahertz Science and Technology*, 7(2):184–190, 2017.

[24] TeraMetrix T-Ray 5000 . https://lunainc.com/blog/terametrix-t-rayr-5000-series-intelligent-terahertz-control-unit.

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

[26] Shivang Aggarwal, Urjit Satish Sardesai, Viral Sinha, Deen Dayal Mohan, Moinak Ghoshal, and Dimitrios Koutsonikolas. Libra: learning-based link adaptation leveraging phy layer information in 60 ghz wlans. In *Proceedings of the 16th International Conference on emerging Networking EXperiments and Technologies*, pages 245–260, 2020.

[27] Yanqiang Xie, Chang Yang, Yun Wang, Yun Shen, Xiaohua Deng, Binbin Zhou, and Juncheng Cao. Anomalous refraction and reflection characteristics of bend v-shaped antenna metasurfaces. *Scientific reports*, 9(1):1–8, 2019.

[28] 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.

[29] Kun Woo Cho, Mohammad H Mazaheri, Jeremy Gummeson, Omid Abari, and Kyle Jamieson. mmwall: A reconfigurable metamaterial surface for mmwave networks. In *Proceedings of the 22nd International Workshop on Mobile Computing Systems and Applications*, pages 119–125, 2021.

[30] Manideep Dunna, Chi Zhang, Daniel Sievenpiper, and Dinesh Bharadia. Scattermimo: Enabling virtual mimo with smart surfaces. In *Proceedings of the 26th Annual International Conference on Mobile Computing and Networking*, pages 1–14, 2020.

[31] Philipp del Hougne, Mathias Fink, and Geoffroy Lerosey. Optimally diverse communication channels in disordered environments with tuned randomness. *Nature Electronics*, 2(1):36–41, 2019.

[32] Hanting Zhao, Ya Shuang, Menglin Wei, Tie Jun Cui, Philipp Del Hougne, and Lianlin Li. Metasurface-assisted massive backscatter wireless communication with commodity wi-fi signals. *Nature communications*, 11(1):1–10, 2020.

[33] Bin Lyu, Dinh Thai Hoang, Shimin Gong, Dusit Niyato, and Dong In Kim. Irs-based wireless jamming attacks: When jammers can attack without power. *IEEE Wireless Communications Letters*, 9(10):1663–1667, 2020.

[34] Jie Yang, Xinsheng Ji, Feihu Wang, Kaizhi Huang, and Lin Guo. A novel pilot spoofing scheme via intelligent reflecting surface based on statistical csi. *IEEE Transactions on Vehicular Technology*, 70(12):12847–12857, 2021.

[35] Jim Doherty. *Wireless and mobile device security*. Jones & Bartlett Learning, 2021.

[36] Daniel Steinmetzer, Yimin Yuan, and Matthias Hollick. Beam-stealing: Intercepting the sector sweep to launch man-in-the-middle attacks on wireless ieee 802.11 ad networks. In *Proceedings of the 11th ACM Conference on Security & Privacy in Wireless and Mobile Networks*, pages 12–22, 2018.

[37] Richard Mitev, Markus Miettinen, and Ahmad-Reza Sadeghi. Alexa lied to me: Skill-based man-in-the-middle attacks on virtual assistants. In *Proceedings of the 2019 ACM Asia Conference on Computer and Communications Security*, pages 465–478, 2019.

[38] Franco Callegati, Walter Cerroni, and Marco Ramilli. Man-in-the-middle attack to the https protocol. *IEEE Security & Privacy*, 7(1):78–81, 2009.

[39] Ulrike Meyer and Susanne Wetzel. A man-in-the-middle attack on umts. In *Proceedings of the 3rd ACM workshop on Wireless security*, pages 90–97, 2004.