DEMO: Adversarial Metasurfaces: Metasurface-in-the-Middle Attack

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. Investigating adversarial metasurfaces, we define and experimentally demonstrate for the first time a "MetaSurface-in-the-Middle" (MSITM) attack in our paper [1]. In the 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. Here, we demonstrate the rapid fabrication of the MSITM employing only standard office supplies such as a printer, paper, foil, and laminator. We show that an effective metasurface can be prototyped in under 5 min at the cost of several cents. We also demo the attack implementation in the THz network, presenting a video of the MSITM attacker establishing a diffractive eavesdropping link while maintaining the legitimate Alice-Bob link. Our results indicate that the attack yields an acute eavesdropping vulnerability 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

1 INTRODUCTION
Metasurfaces are artificially engineered structures that exhibit customizable electromagnetic properties, even beyond what is available in nature [2]. Metasurfaces have been used to enhance wireless communication performance in numerous ways, e.g., relaying signals via transparent metasurfaces embedded in windows [3] and extending signal coverage through metamorphic surfaces on curtains and blinds [4]. With the advancement towards 6G networks, metasurfaces are envisioned to become an even ubiquitous part of the environment [5–7], 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 [8] and high data rate THz transmission over a distance of more than 1 km has already been demonstrated [9, 10].

In our paper [1], we consider for the first time that the adversary employs a metasurface and explore a new acute vulnerability to a diffractive MetaSurface-in-the-Middle (MSITM) attack. In particular, we show how Eve can design and deploy a diffractive metasurface to secretly intercept and manipulate EM waves of Alice’s transmission. Eve 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. In this work, we demonstrate key aspects of [1] including rapid fabrication of MSITM and a video of an experimental demonstration of the MSITM attack in the THz network (the THz equipment is on an optical table that is expensive to transport).

2 ATTACK OVERVIEW
To carry out the attack, Eve develops a metasurface that can diffract THz transmission and position it between Alice and Bob, possibly hiding it in the environment as a “bug,” e.g., disguising it as a part of...
the decoration or concealing it among other objects in the area. As depicted in Figure 1, Alice’s signal propagates in the medium and passes through the metasurface before reaching Bob. The center of the surface is designated as the origin of the coordinate system and $\theta$ corresponds to Eve’s angle relative to Bob and $\gamma$ represents the incidence angle of the transmission.

To deflect a portion of Alice and Bob’s transmission towards herself, Eve designs a metasurface that introduces a phase discontinuity at the surface interface. Specifically, she purposefully induces abrupt and position-dependent phase changes $\Phi(x)$ at the metasurface. Eve’s engineered radiation pattern beyond the surface enables her to control the angular direction of the eavesdropping link based on generalized Snell’s law as:

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

where $\frac{d\Phi(x)}{dx}$ is the gradient of phase discontinuity, $\gamma$ denotes the angle of incidence relative to the surface norm, $f_c$ is the center frequency and $c$ is the speed of light. Also, $n_y$ and $n_\theta$ are refractive index the propagation medium. In [1], we the discuss design space of the attacker in achieving her targeted phase discontinuity $\Phi(x)$ and describe how Eve constructs subwavelength scale metallic resonators (meta-atoms) to control the amplitude and phase of the transmission according to geometrical configurations and orientations of the meta-atoms.

3 MSITM FABRICATION

Traditionally, methods such as photolithography [11] 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 [12]. 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 patterns 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 2(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 2(b). Next, we place an inexpensive iCraft Deco 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 2(c). With the foil containing a nearly 40$\mu$m 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 2(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. Importantly, Eve can quickly and cheaply fabricate the MSITM, spending less than 5 min per surface and employing only standard office items.

4 EVALUATION

4.1 Experimental Setup

We conduct the MSITM attack experiments using a TeraMetrix T-Ray 5000 TD-THz system [13]. 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. We place the transmitter and the receiver 1m apart from each other (due to the system’s sub-$\mu$W transmit power) while positioning the fabricated metasurface 50cm from the transmitter. We consider Alice and Bob communication with $f_c = 150$ GHz and bandwidth $B = 30$ GHz, and Eve positions herself at the empirically optimal angular location $22^\circ$.

4.2 Eve’s Reception

Without a metasurface to alter Alice’s highly directional transmission, Eve largely observes noise fluctuating at around normalized
We explore the impact of the MSITM attack on Bob, as disruption to our analysis of the degradation of transmission power at Bob due to fluctuations of the red curve closely resemble the changes in the baseline at her targeted center frequency. Thus, she can establish a diffraction peak eavesdropping link and compromises Alice and Bob’s link secrecy.

Moreover, 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 3. 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 (1) and reconfigure meta-atoms to be optimized for the different $f_c$ as we describe in [1].

4.3 Impact on Bob

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 the degradation of transmission power at Bob due to the presence of the MSITM in the path of the Alice-Bob link.

We discover that the power spectrum observed by Bob with 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. Thereby, Eve leaves a minimal attack footprint, making the attack both devastating and challenging to detect.

5 ACKNOWLEDGEMENTS

This research was supported by Cisco, Intel, and by NSF grants CNS-1955075, CNS-192378, CNS-1824529, CNS-1801857, NSF-1923733, NSF-1954780 and DOD: Army Research Laboratory grant W911NF-19-2-0269.

REFERENCES


