MetaFly: Wireless Backhaul Interception via Aerial Wavefront Manipulation

Zhambyl Shaikhanov
Electrical and Computer Engineering
Rice University

Sherif Badran
Electrical and Computer Engineering
Northeastern University

Hichem Guerboukha
School of Engineering
Brown University

Josep M. Jornet
Electrical and Computer Engineering
Northeastern University

Daniel M. Mittleman
School of Engineering
Brown University

Edward W. Knightly
Electrical and Computer Engineering
Rice University

***Abstract*—Wireless backhaul links, already ubiquitous and expanding further with 5G and beyond, are employed for many critical functions, such as financial trading on Wall Street. In this work, we demonstrate for the first time that such links are acutely vulnerable to a new class of aerial metasurface attacks. In particular, we show how an adversary Eve designs and employs *MetaFly* to covertly manipulate the electromagnetic wavefront of the signals and remotely eavesdrop on highly directional backhaul links. Exploring the foundation of the attack, we demonstrate Eve's strategy for generating eavesdropping diffraction beams by inducing pre-defined phase profiles at the aerial metasurface interface. We also show how Eve's flight navigation approach can dynamically shape radiation patterns based on drone mobility via a wavefront-tailored flight refinement principle. We prototype MetaFly and demonstrate Eve's lightweight, low-cost, transmissive, and power-free aerial metasurface. We implement the attack and perform a suite of over-the-air experiments in both a large indoor atrium and outdoor rooftops in a large metropolitan area. The results reveal that armed with MetaFly, Eve can intercept backhaul transmissions with nearly zero bit error rate while maintaining minimal impact on legitimate communication.**

1. Introduction

Wireless backhaul links are ubiquitous, with the wireless backhaul equipment industry valued at more than $30 billion in 2021 and projected to reach $105 billion by 2031 with the advancement towards 5G and beyond [1]. Such backhaul links are widely employed for many critical functions, including financial trading on Wall Street [2], medical record exchange in hospitals [3], and 5G base station interconnectivity [4], and can cover distances in the range of kilometers [5]. Wireless backhaul antennas are generally positioned in elevated regions such as towers and rooftops and commonly exploit mmWave and sub-THz frequency bands (30-300 GHz) with large bandwidths for high-date rate and low-latency communication [6], [7].

Since wireless backhaul links employ highly directive beams in hard-to-reach areas, they are assumed to be highly secure, as even the interception of these "pencil-beams" would seemingly disrupt or obstruct the transmission, exposing any potential attacks. However, in this paper, we show for the first time how a strong adversary, Eve, designs and employs *MetaFly* to secretly manipulate backhaul transmission at the fundamental electromagnetic (EM) wavefront level and realizes remote eavesdropping without disruption of legitimate links. We perform a theoretical and experimental investigation of the attack and make the following contributions.

First, we study the foundations of the attack and investigate Eve's aerial wavefront manipulation principles. Specifically, we show how Eve leverages the publicly available Federal Communications Commission (FCC) database [8] to acquire necessary information about the targeted wireless backhaul link, e.g., its frequency bands and antenna locations. She employs an off-the-shelf drone platform and standard office supplies to develop MetaFly, designing a transmissive on-drone metasurface that enables stealthy backhaul transmission wavefront manipulation. Armed with MetaFly, Eve remotely accesses the hard-to-reach backhaul link and covertly induces an additional 3D diffractive eavesdropping link on-the-fly, steering it from the metasurface towards her remote position, while letting the Alice-Bob link pass through. We explore the fundamentals of aerial metasurface-induced diffraction radiation patterns via the analysis of generalized Snell's law in 3D [9]. We show how Eve imparts targeted phase discontinuities at sub-wavelength scale resolution and generates over-the-air diffraction beams, repurposing them for eavesdropping.

Second, we explore Eve's design strategy in realizing MetaFly and discuss her wavefront-tailored flight refinement approach. In particular, she constructs artificial meta-atom elements with controllable electromagnetic properties, obtaining capabilities beyond natural materials. She then strategically arranges a group of unique meta-atoms to induce distinct phase and amplitude profiles and generate eavesdropping diffraction radiation patterns. We demonstrate the attack with a split ring resonator meta-atoms and perform finite element multiphysics simulation analysis to study the attacker's capabilities. We show how Eve purposefully

designs the elements on mmWave and sub-THz transmissive (and nearly transparent) substrates to facilitate the unobstructed transmission of the legitimate link. Unlike traditional metasurfaces that are non-mobile and electronically reconfigurable (e.g., metasurfaces incorporated into walls with externally powered active elements [10], [11], [12], [13], [14]), Eve employs a non-electronically reconfigurable metasurface so that it does not require a power source or a bulky controller. Instead, Eve realizes a reconfigurable EM response by controlling MetaFly's motion. That is, she constructs the aerial metasurface from passive meta-atoms that derive their EM properties from geometrical configurations, i.e., Eve can control phase shifts and amplitude transmissions of the impinging EM waves based on the dimensions and orientations of the meta-atoms. She then exploits MetaFly motion to dynamically modify the spatial phase profile and thereby steer the eavesdropping diffraction beam on-the-fly, refining MetaFly flight pattern in the attack for improved eavesdropping SNR. As we fabricate and demonstrate, the aerial metasurface weighs only several grams and requires no power source, which is especially convenient for the attacker using drones with limited battery life and minimal payload-carrying capability. We also show that Eve can fabricate such aerial metasurface in minutes at the cost of several cents, employing only standard office supplies, which brings the cost of the devastating attack to a minimum.

Third, we implement the attack and perform a suite of over-the-air experiments. For that, we set up a state-of-the-art sub-THz communication testbed and establish a 130 GHz link between transmitter Alice and receiver Bob, which resembles those now commercially available in D-Band ($110 - 175$ GHz) spectrum [7], [15]. To begin, we perform a set of controllable experiments in a large atrium to explore the impact of multiple aerial factors such as the effect of MetaFly vibration, orientation offset, and placement on Eve's eavesdropping performance. The results reveal that Eve's observed signal-to-noise ratio (SNR) of the diffracted link is robust to orientation offsets from her ideal yaw and pitch. In contrast, Eve's performance is significantly more sensitive to the drone's roll offset, with even 2° rotation of the metasurface along the roll axis reducing her SNR by as much as 5 dB. This is because roll offset has the pronounced effect of steering the beam whereas yaw and pitch induce relatively less spatial phase changes at corresponding offset angles. The results further show that Eve should position MetaFly as close to Bob as possible to minimize her bit error rate (BER) due to the superior beamforming efficiency of Alice's high-gain horn antenna compared to Eve's metasurface. However, the midway location between Alice and Bob might be preferable for Eve to avoid exposing the attack while only moderately increasing her BER. In general, the experiments indicate that with MetaFly, Eve can successfully establish an eavesdropping link, obtaining BER below the scale of 10^{-4} with Alice transmitting modulation orders up to 16-QAM. Yet, we also show that her performance is marginally sensitive to MetaFly stability as small-scale vibration can alter diffraction radiation patterns. Measurements at Bob indicate that MetaFly will be challenging to detect, as it leaves a minimal attack footprint, similar to small channel variations due to weather conditions such as snow and rain [16] and variable antenna alignment from building swaying.

Moreover, we demonstrate the attack between two outdoor rooftops in a large metropolitan area, overcoming numerous regulatory and logistical challenges. We set up a highly directive backhaul link at 30 m height and fly MetaFly in between the buildings. We show that MetaFly can consistently generate an eavesdropping diffraction beam on-the-fly while Eve successfully intercepts the link with 40 dB gain, even during moderately windy weather.

In general, in this paper, we explore the foundational physical layer security of wireless backhaul links and expose their acute vulnerability to aerial metasurface attacks. Then, intercepted backhaul links resulting from the attack could be either encrypted or non-encrypted (e.g., to avoid computation and latency overhead). In fact, encryption is a significant area of research with a corresponding set of challenges, including quantum computing attacks [17] and security misconfigurations [18]. Yet, we emphasize that the aerial metasurface attack yields an acute vulnerability, even when wireless encryption is in place and not broken. That is, the attack leaves some multi-layer control information exposed as standards do not encrypt all components of control information such as packet headers, channel state feedback, and addresses [19]. Moreover, under the aerial attack, associated timing information would also be exposed and thus yield vulnerable side channel information exploitable by strong adversaries [20], [21].

The remainder of this paper is organized as follows: Sec. 2 describes the threat model and Sec. 3 presents the attacker's challenges and design strategy. Sec. 4 introduces the attack implementation. Sec. 5 and Sec. 6 describe the over-the-air experimental results. Finally, Sec. 7 reviews related work and Sec. 8 concludes this paper.

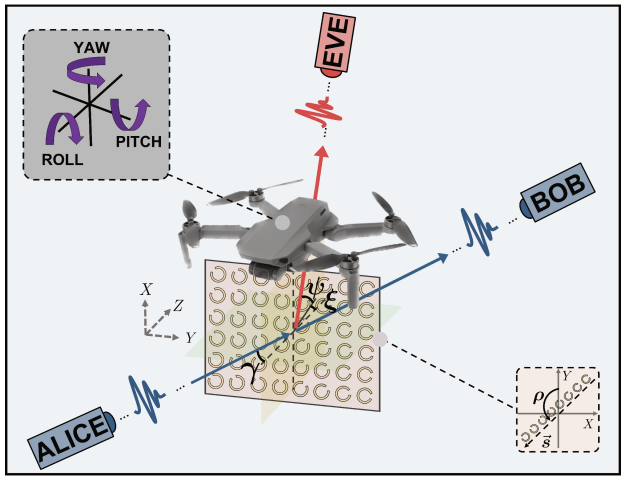


Figure 1: Overview of the aerial metasurface attack.

2. Threat Model

We consider a wireless backhaul network in which the antennas of communicating parties, transmitter (Alice) and receiver (Bob), are deployed at fixed locations above the treeline, typically on towers or rooftops. Targeting secure high data rate transmission, Alice sends her signal to Bob over a highly directional line-of-sight mmWave and sub-THz link. Meanwhile, the attacker (Eve) is positioned distantly from Alice and Bob (possibly at a nearby building) and aims to eavesdrop on the transmission. She also targets to sustain high SNR at Bob in order to avoid substantial distortion of Bob's signal as it might alert him of a possible attack.

The geographical coordinates of the communications parties are designated as C^{Alice}, $\mathbf{C}^{\text{Bob}}$ and $\mathbf{C}^{\text{Eve}}$ where $\mathbf{C}^{\text{Alice}} = (x^{\text{Alice}}, y^{\text{Alice}}, z^{\text{Alice}})$. The center frequency and bandwidth of the transmission are denoted as f_c and B, respectively. Eve has knowledge of the aforementioned information, which she readily acquires from the publicly available FCC database [8]. In fact, this federal agency database is created and made publicly available with the intention to facilitate the deployment and co-existence of wireless services in a region. However, Eve in this attack exploits such information for malicious purposes.

Given the elevated hard-to-access backhaul link environment, Eve takes advantage of a drone to remotely approach the vicinity of the link. She also designs a lightweight on-drone metasurface that enables advanced EM wavefront manipulation on-the-fly. We consider a rectangular planar metasurface rigidly fixated to the bottom of the drone frame and refer to Eve's aerially positioning metasurface system as MetaFly. The location and orientation of the metasurface at time t is designated as $\mathbf{C}_t^{\text{MetaFly}}$ and $\boldsymbol{\theta}_t^{\text{MetaFly}}$, respectively. We define the orientation of the MetaFly as $\boldsymbol{\theta}_t^{\text{MetaFly}} = (\theta_{t,\,yaw}^{\text{MetaFly}}, \theta_{t,\,pitch}^{\text{MetaFly}}, \theta_{t,\,roll}^{\text{MetaFly}})$ in which yaw, pitch, and roll rotations are relative to the vertical axis, lateral axis, and longitudinal axis, respectively as shown in Fig. 1. We discuss Eve's aerial metasurface design and wavefront-tailored flight refinement approach in Sec. 3.

3. Attacker Challenges and Design Strategies

In this section, we explore Eve's key challenges and design strategies in realizing the aerial metasurface attack.

3.1. Inducing an Eavesdropping Beam

Eve modifies the transmission wavefront to establish an eavesdropping beam. A naive approach is to design MetaFly to reflect some transmission signal towards Eve, possibly intercepting the backhaul link via a reflecting surface positioned at a tilted angle. However, such an approach is not quite viable, as any slight positioning imperfections of the surface in the air (subtle swaying and drifting motions) are likely to redirect the reflected beam (specularly) away from Eve and even block the highly directive legitimate transmission, revealing the attack.

Instead, the attacker induces transmissive diffraction in the air. Specifically, she generates a cross-polarized diffracted beam by introducing abrupt and specific phase changes at the aerial metasurface interface, altering the impinging transmission as they pass through the structure. This strategy enables Eve to create a cross-polarized eavesdropping diffraction link from $\mathbf{C}^{\text{MetaFly}}$ to $\mathbf{C}^{\text{Eve}}$, while concurrently allowing the original beam to pass through with its original polarization for reception by Bob.

To demonstrate the principles, consider Fig. 1 in which Alice and Bob are in the yz-plane and Eve's aerial metasurface is in the xz-plane. Eve intercepts Alice's transmission with angle γ relative to the z-axis. Then, she generates a transmissive diffraction beam directed toward herself at angle ψ and ξ in which

$$\begin{aligned} \psi &= \sin^{-1}\left(\left(\frac{c}{2\pi f_c}\frac{d\Phi}{dy} + n_\gamma \sin(\gamma)\right)\frac{1}{n_\psi}\right) \text{ and} \\ \xi &= \sin^{-1}\left(\frac{c}{2\pi f_c}\frac{d\Phi}{dx}\frac{1}{\cos(\psi)}\frac{1}{n_\psi}\right) \end{aligned} \tag{1}$$

by exploiting the generalized Snell's law in 3D [9]. ψ designates the angle between the diffraction ray and its projection on the xz-plane and ξ is the angle between that projection and the z-axis. c is the speed of light, and $n_\gamma(n_\psi)$ is the refractive index of the propagation medium, approximated as one given the over-the-air transmission.

Importantly, Eve can impart an intended $\nabla\Phi$ phase gradient on the backhaul transmission, introducing $d\Phi/dx$ and $d\Phi/dy$ abrupt changes along the x-axis and y-axis as shown in Eq. (1). This allows her to stimulate constructive interference patterns of the electromagnetic waves passing through the aerial metasurface, generating a diffraction peak towards herself at ψ and ξ. Conversely, in its absence, i.e., $d\Phi/dx = 0$ and $d\Phi/dy = 0$, Eq.1 reduces to the standard Snell's law, which describes the change in transmission direction due to a different medium. However, Eve purposefully introduces a spatially periodic phase gradient at the aerial metasurface to induce diffraction radiation patterns in 3D and control the eavesdropping diffracted beam direction.

In the paper, we use the notation $\vec{s}$ to indicate the direction of the imposed linear phase gradient, which forms an angle ρ with the y-axis as shown in Fig. 1. As such, $|\nabla\Phi|$ and ρ denote the magnitude and orientation of the phase gradient.

3.2. Meta-Atom and Unit-Cell Design

Once the phase profile is determined based on the specified eavesdropping angle discussed in Sec. 3.1, the subsequent issue is its physical realization, which is non-trivial due to the involved minuscule wavelengths at such high frequencies. For that, Eve constructs artificial structures, meta-atoms, that enable controllable manipulation of electromagnetic waves, going beyond the capabilities of natural materials [22]. Sub-wavelength in scale, meta-atoms provide a wide range of amplitude and phase responses and

can be configured based on geometrical features. Eve further assembles an array of such unique meta-atoms, forming a unit-cell, to collectively generate the $\nabla\Phi$ phase profile across spatially periodic structures.

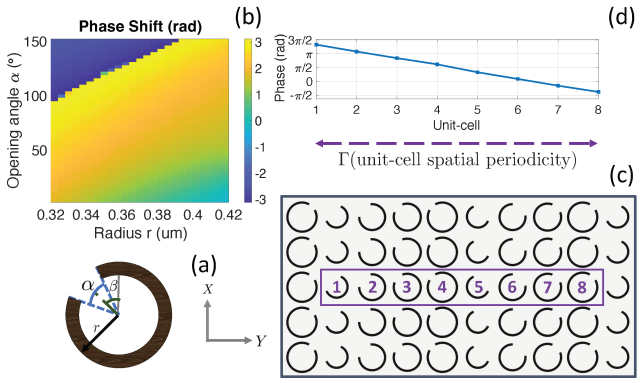


Figure 2: Eve designs (a) C-shaped split ring resonator meta-atoms whose electromagnetic response is controlled via their radius r, slit opening α, and orientation β. (b) With this structure, Eve can achieve the entire 2π phase shift. (c) She arranges a group of unique meta-atoms to form a unit-cell that induces an eavesdropping diffraction beam, (d) with each meta-atom generating a specified $\pi/4$ phase shift concerning neighboring meta-atoms.

We demonstrate the attack with C-shaped split ring resonator meta-atoms since they exhibit a strong EM response at targeted mmWave and sub-THz frequencies [23]. Composed of metallic rings shown in Fig. 2(a), these meta-atoms resonate at specified frequencies. The inductive response is caused by the split in the ring, and the capacitance arises from the gap between the slit ends. This combination leads to tunable resonant responses, allowing for adjustment of both the amplitude and phase response of the impinging wave. Thus, the meta-atom geometries, specifically its radius r, slit opening α, and orientation β, enable accurate control over the electromagnetic properties.

To understand the attacker's capabilities, we model the meta-atoms with varying r, α, and β parameters on COMSOL multiphysics and perform finite element analysis. The results are remarkable as Eve can obtain the entire 2π phase shift by selectively choosing radius r and opening angle α values as shown in Fig. 2(b). We also observe that with a simple rotation of the meta-atom by $\beta = 90°$, she can induce a π phase shift and achieve a symmetrical amplitude response that follows the $|\sin 2\beta|$ function. In fact, she can generate amplitude transmission and phase shift heatmaps, similar to one in Fig. 2(b), and select parameter values corresponding to potentially any targeted response.

Then, to yield a diffraction radiation pattern, Eve assembles a group of distinct meta-atoms to form a unit cell, which she then repeats periodically across a surface. Specifically, the meta-atoms are arranged over the spatial period Γ, and together, they collectively create a 2π phase shift across Γ while maintaining uniform amplitude transmission. These meta-atoms induce specified phase shifts, resulting in superposition and interference effects that cumulatively generate a diffraction radiation pattern in the far field.

Importantly, Eve can control the angle of the diffraction beam in the metasurface design. Specifically, by adjusting the spatial period Γ, she can create distinct phase shifts across the y and x-axis, namely $\frac{d\Phi}{dy} = \frac{2\pi}{\Gamma \cos\rho}$ and $\frac{d\Phi}{dx} = \frac{2\pi}{\Gamma \sin\rho}$, and direct the eavesdropping beam to different angles as formulated in Eq. (1). For instance, decreasing the values of Γ allows Eve to increase diffraction peak angles, potentially eavesdropping from afar. She can achieve such reduced spatial period Γ values by either decreasing the number of meta-atoms in the unit-cell or reducing the dimensions of the corresponding meta-atoms.

We demonstrate the attack with an exemplary unit-cell consisting of eight different meta-atoms and Γ of 6.11mm. Specifically, these meta-atoms have the following parameters $[r(\mu\text{m}), \alpha, \beta]$: $[240, 136°, -45°]$, $[284, 82°, -45°]$, $[296, 32°, -45°]$, $[320, 12°, -45°]$, and their $90°$ rotated counterparts. Each meta-atom produces $\pi/4$ phase shift relative to neighboring ones while maintaining approximately identical amplitude transmission. With an exemplary backhaul transmission at $f_c = 130$ GHz, Eve then establishes an eavesdropping diffraction peak at $\psi = 22°$, as described in Eq. (1) with ρ set to zero in the default state.

3.3. Realizing Lightweight, Power-Free, and Transmissive Aerial Metasurface

Traditionally in wireless networks, metasurfaces are designed as large, electrically tunable, reflecting metasurface infrastructures, that are statically positioned in the environment, e.g., integrated on walls [10], [11], [12], [13], [14]. Once installed, they are typically connected to an external power source, e.g., a wall outlet, to activate hundreds to thousands of reflecting elements on the metasurface. Then, wireless channels within the vicinity are reconfigured in real-time, e.g., supplying DC bias to varactor diodes, for different functionalities, such as extending signal coverage.

In contrast, the aerial nature of the attack necessitates a reconsideration of conventional principles and the development of a lightweight, transmissive, and dynamic metasurface with minimal power consumption.

For that, Eve designs a passive metasurface, in which she exploits the geometrical properties of the meta-atoms to manipulate the EM wavefront, rather than relying on an external power source. In particular, she induces selected amplitude transmission and phase shifts on the impinging EM waves solely based on the radius, slit opening, and orientation of the C-shaped meta-atoms as we describe in Sec. 3.2. As such, the aerial metasurface does not require any external power source and yet can successfully establish an eavesdropping diffraction link.

Such a design approach is complementarily advantageous to Eve in reducing MetaFly payload, e.g., no need for switching components, extra power supply, and FPGA controller units. In fact, not only are drones known to have very

limited payload lifting capabilities, but also a heavy payload can deplete the already limited drone battery significantly faster, potentially leading to a failed attack. However, we demonstrate in Sec. 4.1 that Eve's aerial metasurface is only several grams, making it a negligible addition to MetaFly.

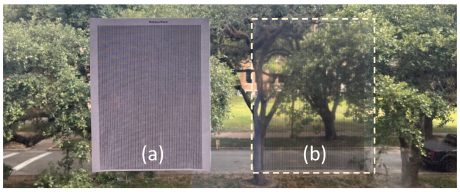


Figure 3: Demonstrating (a) paper substrate-based and (b) polymer (plastic) substrate-based aerial metasurfaces.

Importantly, the design facilitates the transmission of Alice to Bob's link and avoids obstructing that legitimate link. For that, Eve exploits mmWave and sub-THz transmissive materials as the aerial metasurface substrate. Specifically, she arranges periodic unit-cells discussed in Sec. 3.2 onto materials with a low refractive index (e.g., paper and polymer sheets) to reduce attenuation and improve penetration at these high frequencies. We demonstrate paper substrate-based and polymer (plastic) substrate-based aerial metasurfaces in Fig. 3. Our experiments reveal that both substrates indeed have minimal absorption loss, less than 1 dB.

Moreover, some substrates, like polymers, can provide additional transparency properties, as we demonstrate in Fig. 3(b). Eve could exploit that feature to carry out the attack with a concurrently transmissive and transparent aerial metasurface, essentially having a nearly invisible eavesdropping structure in the air.

3.4. Wavefront-Tailored Flight Refinement

Eve uses drone-aided metasurface mobility to overcome the physical constraints of hard-to-reach backhaul areas and improve the attack performance by dynamically adjusting the EM wavefront of the transmission based on the flight.

To execute the attack, she first acquires GPS locations of the backhaul antennas from the publicly available FCC database [8] and then remotely navigates the MetaFly to get the on-drone metasurface towards the path of directive backhaul transmission. Yet, approaching the link solely based on GPS coordinates might be insufficient for Eve as occasional positioning uncertainties, e.g., due to wind or GPS failure, likely set the MetaFly off the transmission beam or distort and re-direct generated diffraction beam. To address it, Eve performs wavefront-tailored flight refinement.

Specifically, she adjusts the flight pattern of the MetaFly, taking into account the fundamental characteristics of the on-drone metasurface, such as the phase profile $\nabla\Phi$, her targeted eavesdropping diffraction beam angles ψ and ξ, and her feedback on the observed eavesdropping SNR, as depicted in Fig. 4. MetaFly is then repositioned to the next location $\mathbf{C}_{t+1}^{*\text{MetaFly}}$ and orientation $\boldsymbol{\theta}_{t+1}^{*\text{MetaFly}}$ to improve the generated diffraction radiation patterns and increase eavesdropping SNR at Eve.

In the flight refinement process, Eve exploits the fundamental yaw, pitch, and roll movements of the MetaFly to dynamically and controllably modify the phase response of the aerial metasurface. For instance, she leverages the roll motion to adjust the orientation ρ. In turn, such motion stimulates distinct phase response along both the x-axis and y-axis, allowing her to modify the generated diffraction beam angle, as formulated in Eq. 1. By doing so, she can continually refine the eavesdropping diffraction angle on-the-fly, redirecting it towards her antenna.

In Fig. 5, we present analytical results demonstrating the impact of roll movement on the induced eavesdropping beam angles. We consider an exemplary center frequency of 130 GHz and the spatial periodicity $\Gamma = 3$ mm. Observe that Eve can have control over a wide range of azimuth ψ and elevation ξ angles of the eavesdropping diffraction beam governed by roll movement. Such a response is leveraged in the flight refinement to consistently redirect the beam to remote Eve's antenna and improve her SNR.

Eve can also exploit the wavefront-tailored MetaFly mobility approach to carry out the attack from various remote locations, such as from the rooftop, inside the building (with the beam passing through the window), or even at ground level. That is, even with a fixed aerial metasurface design, she can still generate a dynamic EM response governed by the MetaFly mobility, controllably steering the eavesdropping diffraction beam in 3D. For example, she can direct the beam anywhere from 0° to 50° in azimuth and elevation based on MetaFly roll motion, as shown in Fig. 5.

Likewise, she can take advantage of the yaw movement of MetaFly in dynamically shaping the wireless backhaul transmission. Specifically, she can initiate yaw rotation to deliberately intercept the transmission with different impinging γ angles. This allows her to further modify both the ψ and ξ components of the eavesdropping diffraction beam with non-linear relation as shown in Eq. 1.

In general, Eve could realize such wavefront-tailored flight in several ways. She could design an advanced on-drone control mechanism to automatically perform flight navigation. Alternatively, she can manually control MetaFly during the attack, adapting the flight pattern with a remote controller while monitoring her eavesdropping SNR in real-time. As we demonstrate in Sec. 6.1 and Sec. 6.3, Eve can be highly successful even with the latter simpler approach.

We also highlight that metasurfaces are traditionally considered to be either static or programmable based on their functionalities. A static metasurface generates one specific electromagnetic response while a programmable metasurface can change the response over time, e.g., via DC bias

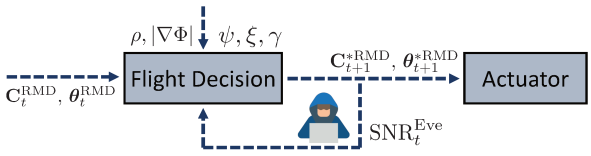


Figure 4: MetaFly wavefront-tailored flight refinement

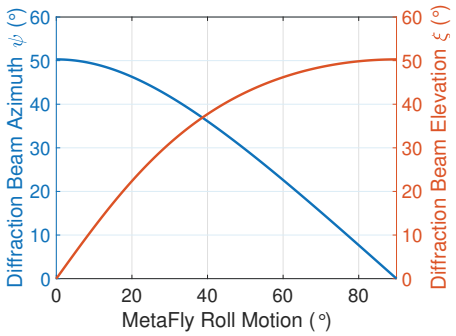


Figure 5: Eve exploits roll mobility of MetaFly to modify the diffraction radiation pattern on-the-fly and thereby controllably steer the eavesdropping diffraction beam in 3D.

excitation. In the context of wireless security, in this work, we demonstrate a first-of-its-kind static metasurface that can dynamically change its electromagnetic response governed by the mobility pattern of the drone.

4. Attack Implementation

In this section, we describe the implementation of the attack, introducing aerial metasurface fabrication, the state-of-the-art sub-THz testbed, and the experimental setup.

4.1. Aerial MetaSurface Fabrication

Traditionally, microfabrication techniques such as photolithography [24] are employed to fabricate metasurfaces, providing ultrahigh resolution ($\sim$ 100nm). However, these methods are also known for their high cost (reaching thousands of dollars) and slow processes, requiring sophisticated equipment and chemicals. Here, we demonstrate how Eve rapidly and inexpensively hot-stamps [25] an aerial metasurface using two simple steps.

First, she prints the aerial metasurface design pattern discussed in Sec. 3.2 using a standard toner printer. She employs mmWave and sub-THz transmissive substrates, such as off-the-shelf glossy paper [26] and transparent plastic sheet [27], to print the design. Then, she puts an off-the-shelf metallic foil [28] on top of the printed pattern and passes them through a laminator heated to a temperature of 290 °F, as shown in Fig. 7. As the foil and the substrate heat up, the metallic particles from the foil and the toner on the substrate bond together, metalizing the pattern. After peeling off the remaining foil and cleaning the pattern with standard tape, a fully functioning aerial metasurface is formed and its weight is only 10 grams.

In general, the fabrication process involves only standard office items such as paper, a laminator, and foil. It costs mere cents and takes only minutes to complete, minimizing the overall attack cost. Our fabricated metasurface is of letter paper size, and we mount it onto a lightweight plastic frame. We then integrate it onto an off-the-shelf DJI drone.

4.2. State-of-the-art Sub-THz Testbed

We demonstrate the attack with a state-of-the-art sub-THz testbed, transmitting ultra-broadband information-bearing framed signals. We establish a backhaul link at 130 GHz, which resembles those now commercially available and is similar to the 120 GHz-band wireless link used for live TV broadcasts (with a range of 400m) during the Beijing Olympics [29]. Additionally, our testbed employs hardware similar to that recently used in a 2-kilometer-range wireless backhaul link [5].

More specifically, our transmitter part consists of an analog programmable signal generator (PSG) employed for generating a local oscillator (LO) signal, an arbitrary waveform generator utilized to send an intermediate frequency signal, which is later mixed with the LO and upconverted to a higher RF signal through an upconverter frontend. The receiver part consists of a PSG which is used to generate the LO signal at the receiver side, a downconverter frontend, and a high-performance digital storage oscilloscope. We employ high-gain 40 dBi lens horn antennas. The transmit power just before the antenna is 13 dBm.

4.3. Experimental Setup

We conduct large-scale outdoor experiments, as discussed in Sec. 6.3, as well as controllable indoor atrium experiments to investigate the impact of different attack factors. As shown in Fig. 6, transmitter Alice and receiver Bob are positioned 10 m apart, with the aerial metasurface located midway (varied in corresponding experiments). Receiver Eve is angularly positioned ($\sim 22°$) away from Bob to observe the 130 GHz eavesdropping diffraction beam generated by the aerial metasurface. With Eve's cross-polarized aerial metasurface, we rotate her antenna to 90° relative to Bob to observe strongly modulated data in orthogonal polarization. Additionally, we utilize a motorized 3D stage (model Theta-Y-Theta-Z by IntelLiDrives) and a motorized vibrating stage (model VT007) in the experiments.

In the experiment, Alice transmits modulated data to Bob at 130 GHz carrier frequency using 10 GHz bandwidth, employing M-QAM modulation scheme. Our experiments include up to 1024-QAM, which are the same modulation used by LTE and Wi-Fi. The QAM frame structure consists of an 18-bit header, followed by $1500\log_2(M)$ pilot bits and $10000\log_2(M)$ data bits, concatenated together. The header (BPSK modulated high-autocorrelation sequence) is used for time synchronization at the receiver, and the pilot bits are employed as a training sequence for channel estimation. Channel estimation and equalization are performed using the minimum mean square error (MMSE) estimation. Received signals are processed, equalized, and demodulated to obtain performance evaluation parameters such as SNR, error vector magnitude (EVM), peak-to-average power ratio (PAPR), bitrates, and BER.

We conduct our experiments using an unencrypted link as there is not yet a standard for sub-THz backhaul encryption. Furthermore, the research question we address

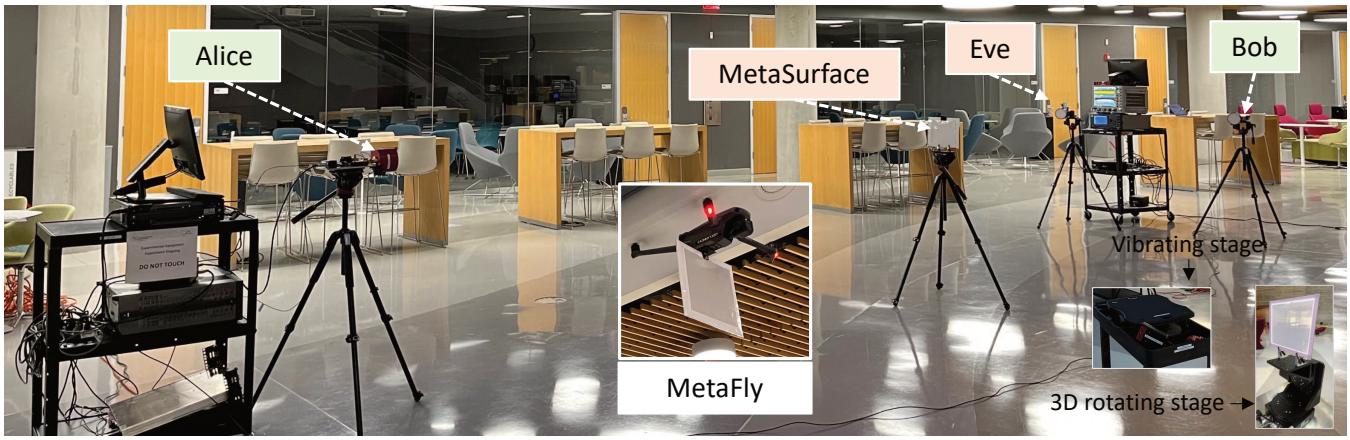


Figure 6: Large atrium experimental setup with state-of-the-art sub-THz communication testbed and MetaFly.

in this work is different from encryption, as we explore new vulnerabilities at the fundamental physical layer that arise despite the directionality and inaccessibility of wireless backhaul links. Nevertheless, our contribution is to demonstrate vulnerabilities of information leakage in either case, whether it involves the data itself (when unencrypted) or side information (when encrypted).

5. Aerial Attack Factors

In this section, we perform a suite of over-the-air experiments in which we explore various aerial attack factors such as metasurface vibration, orientation offset, and placement.

5.1. Orientation Offset

Eve targets to orient the metasurface to be perpendicular to a vector from Alice to Bob's aperture. Yet in practice, Eve is likely to be offset from her ideal due to both drone system imperfections such as inertial sensor errors, and external factors such as the wind impacting the control loop that stabilizes the drone. Here we controllably orient Eve's metasurface to different yaw, pitch, and roll angles, including both perfectly aligned and offset, and explore the impact of orientation angle offsets on her eavesdropping capabilities.

Adopting the setup discussed in Sec. 4.3, we integrate the metasurface into the motorized rotation stage and position it midway between Alice and Bob. In the experiment, Alice, Bob, and Eve are all on the same plane and the metasurface is within the vector from Alice to Bob. Eve is placed angularly away from Bob to observe the 130 GHz diffraction peak generated at the aerial metasurface at 22°. We change angular orientations in 2° increments while continually recording Eve's SNR and BER at her fixed remote location. For each configuration, we perform at least 50 instances of data captures, each capture containing at least 10 frames.

We depict the result in Fig. 8, showing a range of yaw, pitch, and roll angles on the x-axis and Eve's corresponding SNR on the y-axis. In the figure, we present the results for perfect orientation (0° offset) as well as moderate and high orientation offsets of 8° and 16° respectively.

First, the blue bar corresponds to the perfectly oriented scenario, in which Eve generates the best possible eavesdropping diffraction radiation pattern to obtain the maximum SNR, which is approximately 15 dB in this experiment. Moreover, observe that rotation of the metasurface across the different axes has a non-similar and non-uniform

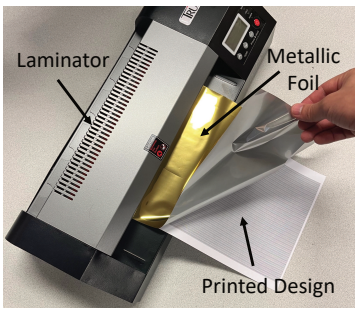


Figure 7: Fabricating the aerial metasurface using a standard office printer, laminator, and iCraft metallic foil.

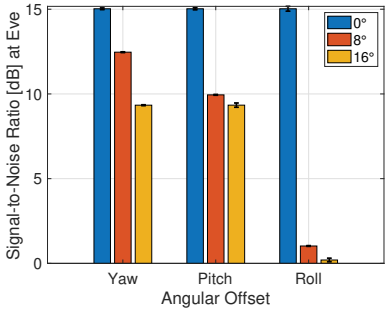


Figure 8: Impact of Eve's MetaSurface orientation offset on her remote eavesdropping SNR.

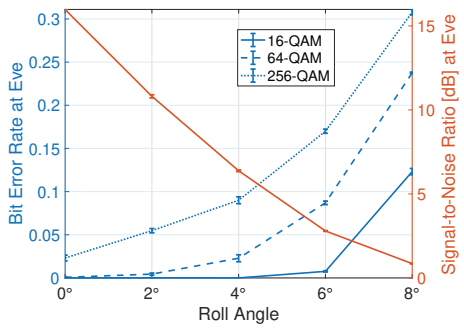


Figure 9: Effect of MetaSurface roll offset on Eve's SNR and BER.

impact on Eve's observed signal power. Specifically, the results in Fig. 8 reveal that Eve is less sensitive to yaw and pitch offsets when compared to roll. For example, an 8° offset in roll orientation drastically decreases Eve's SNR from 15 dB to 1 dB, whereas the same offset in yaw and pitch still enables Eve to maintain an SNR of 10 dB and above. This is because the orientation ρ (defined in Sec. 3.2) is directly governed by the roll offset. That is, the roll offset significantly modifies phase discontinuity response across x and y-axis of the metasurface, specifically to $\frac{d\Phi}{dy} = \frac{2\pi}{\Gamma \cos\rho}$ and $\frac{d\Phi}{dx} = \frac{2\pi}{\Gamma \sin\rho}$ as discussed in Sec. 3.4. As such, it diffracts the beam in a different direction other than Eve's location, following Eq. (1). In contrast, for pitch and yaw angular offsets, the impact at Eve is rather modest [30]. Particularly, yaw offset governs the incidence angle γ defined in Sec. 3.2 and has a negligible impact on the generated diffraction beam at these yaws offset below 20° due to only $\sin\gamma$ effect in Eq. (1).

For example, pitch offset does not directly affect the direction of the eavesdropping beam, instead but primarily impacts the total intercepted transmission beam area by the metasurface. Then, by employing a letter-size metasurface and positioning a midway Alice-Bob transmission beam (which is spreading out in space), Eve can obtain more than half of the SNR relative to the baseline case as shown in the experiment.

Given the high responsiveness of Eve's SNR to metasurface roll offset, we further investigate its impact on both Eve's SNR and (empirically measured) BER at a higher angular resolution. For that, we present the results in Fig. 9 and depict a range of angles from 0 to 8° at the step of 2° in the x-axis. On the right side of the y-axis, we show Eve's SNR (orange), and on the left side of the y-axis, we show Eve's BER (blue). We consider Alice's transmission with three different QAM modulation schemes, namely 16-QAM, 64-QAM, and 256-QAM, represented in blue solid, dashed, and dotted lines, respectively.

First, observe that even a 2° roll offset reduces Eve' SNR by as much as 5 dB. Additionally, her SNR continues to diminish rapidly with increasing offset, with Eve having only 1 dB SNR with her metasurface offset by 8°. Such a response is due to multiple factors. First, increasing roll angle correspondingly modifies the response due to $d\Phi/dx$ and $d\Phi/dy$ induced at the metasurface interface, thereby re-directing the eavesdropping beam away from Eve's targeted location as shown in Eq. (1). Moreover, Eve's metasurface demonstrated in the experiments is cross-polarized, and with roll movement, Eve's effective cross-polarized signal power re-directed towards herself also decreases. Jointly, these factors make Eve highly sensitive to metasurface roll offsets and force her to maintain an accurate roll position of the metasurface during the flight to carry out the attack efficiently.

Yet, in Fig. 9, we show that Eve's BER performance also depends on Alice's underlying transmission modulation order, which Alice will select according to the SNR of the Alice to Bob link. For example, if the Alice-Bob link employs 16-QAM, Eve's SNR is sufficient to obtain BER below 1% even at the roll offset of 6°. However, as the modulation order increases, Eve's corresponding BER degrades rapidly with increasing angular offset as shown in the blue dashed and dotted curves. This is particularly evident when Alice's transmission in 256-QAM and Eve's interception undergoes more than 30% BER with metasurface roll offset of 8°.

Findings: While Eve is minimally affected by pitch and yaw offsets of MetaFly, she is very sensitive to the roll offset as it modifies her phase gradients at the metasurface interface and thus diffracts the beam in a different direction other than Eve's location. In fact, even 2° rotation of Eve's metasurface along the roll axis can significantly decrease Eve's SNR, diminishing her SNR to 1 dB at 8° roll offset. Yet, Eve's attack performance from the BER perspective further depends on Alice's transmission modulation order, and Eve's BER can remain below 1% when Alice employs up to 16-QAM.

5.2. Impact of Vibration

Thus far, we have explored the impact of metasurface orientation offset. In addition to that, Eve's metasurface undergoes vibration during the flight as it is affixed to the drone platform. Here we investigate the impact of Eve's metasurface vibration on her ability to establish and maintain an eavesdropping diffraction radiation beam.

In the experiment, we use the same setup as previously and integrate the metasurface on a motorized vibration stage VT007, positioning it midway between the Alice-Bob link. We configure the vibration frequency to 40 Hz, corresponding to drone vibration characteristics reported in the prior work [31]. We record Eve's SNR continually for several minutes while the metasurface is vibrating at the configured frequency.

We depict the results in Fig. 10, showing time on the x-axis and Eve's SNR on the y-axis. As a baseline, we consider Eve without any metasurface and depict the results in the blue curve. Also, as a reference, we consider the scenario of Eve employing a metasurface without vibration and plot it in the orange curve. Lastly, Eve's response when the metasurface undergoes vibration is depicted in the

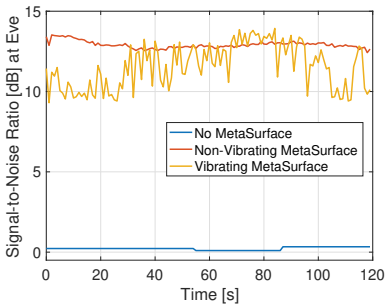


Figure 10: Temporal effect of MetaSurface vibration.

yellow curve. We report time-averaged results of the aforementioned experiments in Table 1, presenting the mean and standard deviation of Eve's observed SNR for corresponding metasurface configurations.

First, notice that without the metasurface, Eve is unable to intercept the highly directional sub-THz transmission, and thus her SNR is in the 0 dB range. However, the non-vibrating metasurface allows Eve to induce consistent and targeted phase discontinuities. Thus, she is able to establish an eavesdropping link and obtain a 12.9 dB mean SNR.

Moreover, the results reveal that Eve still obtains more than 11 dB mean SNR compared to the baseline even when the metasurface is vibrating. That is, the vibration motion of the metasurface does not inhibit it from creating targeted abrupt phase changes at the metasurface interface and generating diffraction radiation patterns. However, vibration generates random and minor orientation offset and mm-scale mobility, which in turn affects radiation pattern and impacts Eve's observed SNR in the form of 1.3 dB fluctuations as shown in Fig. 10. In general, note that the exact vibration patterns and their consequences on Eve's attack performance largely depend on the quality of her drone platform and its calibration status. The more Eve is willing to invest in her drone system and perform necessary internal and external sensor calibrations, the more efficient she will be in the attack.

Findings: When compared to idealistically static metasurface, vibration motion in MetaFly only reduces Eve's mean SNR performance from 12.9 *dB to* 11.6 *dB. However, random mm-scale mobility and minor orientation offset due to vibration still minimally distorts diffraction radiation pattern and impact Eve's observed SNR in the form of* 1.3 *dB fluctuations.*

TABLE 1: Time-Averaged Performance

Eve	Mean SNR	σ_{SNR}
No MetaSurface	0.2 dB	0.08 dB
Vibrating MetaSurface	11.6 dB	1.3 dB
Non-Vibrating MetaSurface	12.9 dB	0.2 dB

5.3. Eve's Placement of MetaSurface

To intercept signals, Eve will position MetaFly along the line-of-sight vector between Alice and Bob. Yet, within this vector, she can choose to place MetaFly at any point spanning from close to Alice, mid-way, or close to Bob. Here, we explore how Eve should best position MetaFly along this vector based on her eavesdropping performance as well as her risk of being detected by Alice or Bob.

We consider the same setup described in Sec. 4.3, with Alice and Bob at 10 m apart and at the same elevation. In the experiment, we controllably reposition the metasurface away from Alice from 1 m to 9 m at 2 m step while always maintaining it perpendicular to a vector from Alice to Bob's aperture. Moreover, we adjust Eve's location correspondingly to ensure that she always observes her targeted $f_c = 130$ GHz diffraction peak at 22° and maintains approximately 10 m of the total distance (the effective ray length from Alice's aperture to the metasurface and from metasurface to Eve's aperture). This setup allows us to largely eliminate the difference in Eve's observation due to path loss (a known effect described in the Friis transmission formula) and instead focus on the metasurface-induced wavefront factors.

We depict the results in Fig. 11, showing Eve's placement of the metasurface within the Alice-Bob link on the x-axis and her eavesdropping BER in log-scale on the y-axis. In the experiment, we configure Alice-Bob transmission with different QAM modulation schemes, ranging from 16-QAM up to 1024-QAM. Also, some data points in the 16-QAM (blue) are omitted in the log-scale plot, which corresponds to 0 measured bit errors.

To begin with, observe that Eve can reduce her BER as she positions the metasurface further away from Alice. For instance, with Alice's transmission in 64-QAM (orange), Eve decreases the BER from 1.9×10^{-2} to 9.3×10^{-4} by having the metasurface move from 1 m to 9 m. Additionally, such a pattern is consistent across different modulation schemes. Thus, from the perspective of minimizing BER, Eve should have the metasurface as close to Bob as possible in the attack, and there are two primary factors that motivate her to do so.

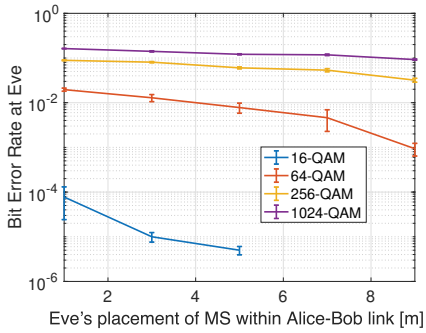


Figure 11: Impact of Eve's MetaSurface placement.

First, by placing the metasurface closer to Bob, Eve increases the beam spot efficiency on the metasurface. Specifically, because Alice's transmission (emitted by a 40 dBi directional antenna in the experiment) is spreading out in space, a larger area of the metasurface is illuminated if the metasurface is further away from Alice. As such, Eve can intercept more transmission beam energy and re-purpose it for eavesdropping. Conversely, when the metasurface is located very close to Alice, only a limited portion of its area is illuminated and Eve gets higher BER due to low intercepted signal power.

In general, the effective beam spot efficiency of the metasurface depends on the beamwidth of Alice's transmission and the metasurface size. Observe that, in this experiment, the (letter-size) metasurface is already fully illuminated when it is midway between Alice and Bob. Nevertheless, Eve's BER (across different modulation schemes) still continues to decrease as MetaFly moves closer to Bob beyond the mid-way point. This phenomenon highlights the second additional major factor regarding the beam spot efficiency at Eve. Particularly, because the metasurface array (with many meta-atom elements) is a less effective beamformer than the employed highly directive 2° half-power beamwidth horn antenna, Eve aims to position her metasurface as close to Bob as possible. In general, the efficiency of the metasurface depends on many factors, including the EM properties of the constituent meta-atoms (such as amplitude transmission and polarization) and the resolution of the fabrication technique.

On the other hand, Eve might purposefully avoid very close locations to either Bob or Alice to not expose the attack, e.g., if there are rooftop security cameras that might detect a drone. Thus, Eve might determine that, with MetaFly positioned midway between the communicating parties, she performs nearly as well, especially when Alice employs modulation orders above 256-QAM. For example, Eve increases her BER from 0.09 to only 0.12 when repositioning from 9 m to midway with Alice transmitting in 1024-QAM. This is also indicated by the pink curve flattening in Fig. 11.

Findings: Due to beam spot efficiency on the metasurface and superior beamforming efficiency of Alice's antenna vs. Eve's metasurface, Eve aims to position MetaFly as close to Bob as possible for minimizing her BER. Nevertheless, the midway locations between Alice and Bob may be preferable to Eve to avoid exposing the attack while minimally trading off BER.

6. MetaFly Attack Experiments

Thus far, we have performed a suite of controllable experiments with a stand-alone metasurface to individually investigate various aerial attack factors such as orientation offset, vibration, and metasurface placement. In this section, we integrate the metasurface with a drone, constructing MetaFly, and demonstrate the attack both in an indoor atrium and outdoor rooftop environments.

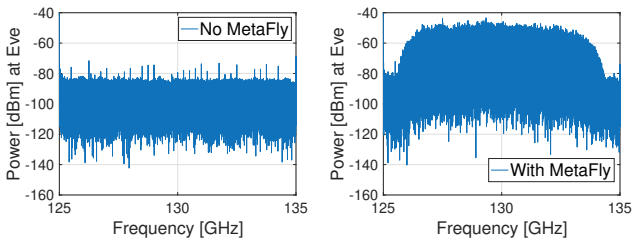
6.1. Attack Demonstration

We begin with an indoor atrium study to enable flight while still having a controlled flight environment (e.g., no wind or weather artifacts). We position Alice and Bob 10 m apart and at the same elevation in a large open atrium environment that has office windows, stair cases, ground-level seating and tables, etc. In the experiment, Eve remotely controls MetaFly and positions it midway between the communicating parties (based on the findings of Sec. 5.3), and hovers it at that location. Eve positions her receiver to intercept the $f_c = 130$ GHz eavesdropping diffraction peak at her design specification of 22° induced at the on-drone metasurface interface. As a baseline, we consider the case when Eve does not employ MetaFly in the attack. We start by studying the feasibility of the attack and depict Eve's power spectral profile observed in two different scenarios in Fig. 12.

Notice the significant difference between the power spectrum in Fig. 12(a) vs. Fig. 12(b). Specifically, Eve largely receives noise without MetaFly, with the blue curve mostly fluctuating below -80 dBm in Fig. 12(a). The reason is that Eve is unable to observe the highly directive transmission without MetaFly to manipulate the Alice-Bob link. In contrast, Eve's acquired signal power drastically changes as she employs MetaFly in the attack. On average, Eve obtains more than 25 dB above the noise floor signal power across her targeted 10 GHz bandwidth as depicted in Fig. 12(b). By remote positioning MetaFly and stealthy interception of the link, she induces her targeted abrupt phase changes $|\nabla\Phi| = 2\pi/6.11$ mm on the transmission wavefront. As such, she generates an eavesdropping diffracted beam steered toward her antenna.

Next, to investigate the effectiveness of the attack, we compute the total number of Alice's transmitted data bits and the portion that Eve can intercept without error, i.e., her empirical BER. In this experiment, we consider a range of modulation orders employed at Alice, spanning from 16-QAM to 1024-QAM. We present the results in Fig. 13, showing modulation orders on the x-axis and Eve's BER on the y-axis.

First, notice that Eve is highly effective at maintaining BER below the scale of 10^{-4} when Alice employs up to 32-QAM. That indicates that Eve acquires sufficient signal



(a) Eve Without MetaFly (b) Eve Employing MetaFly

Figure 12: Feasibility of the attack.

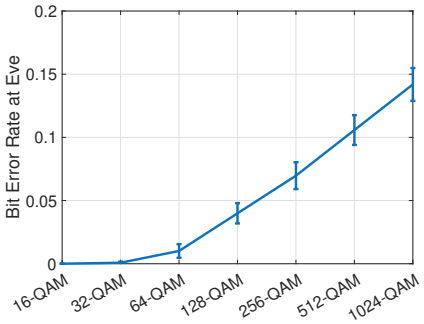


Figure 13: Effectiveness of the attack.

power in her eavesdropping link to accurately distinguish unique phases and amplitudes in each symbol and recover the data. Yet, expectedly, her mean BER decreases with increasing modulation order. More importantly, observe that the standard deviations are non-negligible and increasing, especially at above 64-QAM. This is because of the small-scale mobility and vibration effects of MetaFly studied in Sec. 5 that partially alter the spatial phase gradients $d\Phi/dy$ and $d\Phi/dx$. In turn, such a response alters the generated diffraction beam, resulting in fluctuations in received signal power. As such, Eve's achievable BER is sensitive to the stability of the MetaFly. Nevertheless, in this experiment, we demonstrate that Eve can still maintain, on average, below 15% BER even at such high modulation orders as 1024-QAM.

Lastly, we note that we have not used any error correction coding in this experiment. However, if Alice does use such redundancy to help Bob, Eve can also utilize it to more effectively decode, reducing her BER and ultimately, her frame error rate.

Findings: We experimentally demonstrate that Eve can remotely navigate MetaFly and successfully establish an eavesdropping diffraction link steered towards her receiver, maintaining BER below the scale of 10^{-4} *with Alice transmitting at up to* 32*-QAM. Yet, we also show that BER performance is also sensitive to MetaFly stability as the small-scale mobility and vibration characteristics of the MetaFly can alter the generated eavesdropping diffraction radiation patterns.*

6.2. Impact at Bob

Thus far, we have demonstrated the attack from the perspective of Eve, exploring her capabilities. Here, we study the impact of such an aerial threat on Bob, as disruption to Bob's communication link could alert him to the attack.

We employ a setup similar to that described in Sec. 6.1 and consider Bob's observation in the absence of MetaFly as a baseline, i.e., an unobstructed line-of-sight path between Alice and Bob. First, we investigate the energy footprint of the attack and depict Bob's power spectral profile in two different scenarios in Fig. 14.

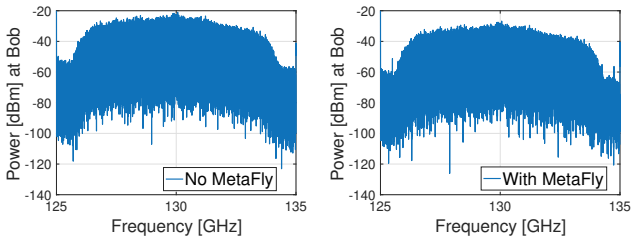
TABLE 2: Summary of Bob's Observation (1024-QAM)

Parameter	No Attack	With Attack
EVM	5.75%	7.10%
PAPR at Tx	9.64 dB	9.65 dB
Actual Bitrate	49.95 Gbps	49.95 Gbps
Max. Theoretical Bitrate	50 Gbps	50 Gbps
Number of Error Bits	6622	9069
BER	6.62×10^{-2}	9.07×10^{-2}

Observe that the power spectral profiles in the two scenarios are very similar, albeit with a few dBm power shifts. This is because Eve purposefully exploits the sub-THz transparent structure (paper in this experiment) as the on-drone metasurface substrate discussed in Sec. 4. In doing so, she intentionally allows Alice's transmission to pass through the aerial metasurface and reach Bob. As such, Eve not only establishes an eavesdropping link but also maintains the legitimate link, leaving a minimal energy footprint.

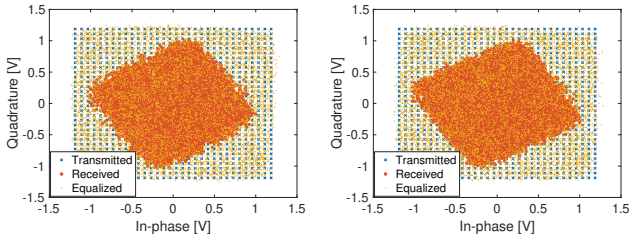
Additionally, recall that Eve manipulates the transmission in an orthogonal polarization to that of Alice, employing a cross-polarized aerial metasurface. On top of that, her metasurface has a wideband response as we observed in the experiments. As a result, there is no evident frequency-selective response of the metasurface at Bob, but rather a nearly uniform few dBm power decrease as shown in Fig. 14(b). Consequently, detecting such an energy footprint would be non-trivial for Bob. In addition, wireless backhaul channels can encounter similar channel variations even without MetaFly in between the Alice-Bob link. Specifically, backhaul infrastructure on towers and buildings are prone to swaying due to wind. As such, this leads to antenna misalignment and a decrease in the received power, which is particularly evident at these high frequencies.

Moreover, prior work has shown that weather conditions such as rain and snow introduce path loss increase at sub-THz frequencies. Specifically, scattering from snowflakes and rain and molecular absorption due to water vapor has been demonstrated to increase path loss from a few dB to tens of dB for different weather conditions [16]. Thus, considering the additional impact of weather in outdoor backhaul scenarios, detecting the attack by analyzing only the energy footprint would be challenging for Bob.



(a) No Attack (b) With Attack

Figure 14: Energy footprint of the attack viewed at Bob.



(a) No MetaFly (b) With MetaFly

Figure 15: Constellation diagrams as observed at Bob.

Next, to analyze the effect of the attack at a symbol level, we show the constellation diagrams observed at Bob for both scenarios, with and without MetaFly in between the Alice-Bob link. Since there is a higher probability of an error (including due to the effect of the attack) with increasing QAM order, we purposefully show the results for the highest modulation order from the experiments, as high as 1024-QAM, in Fig. 15. We also summarize the results in Table 2, highlighting Bob's observed EVM, PAPR, bitrates, and BER, among others, in both scenarios.

Fig. 15 depicts the transmitted, (raw) received, and equalized symbols in blue, orange, and yellow dots, respectively. First, notice that without MetaFly in Fig. 15(a), the raw received constellations are rotated (as well as shrunk) compared to the transmitted one. These are mainly the impact of the device and channel effects, such as oscillator phase noise, IQ imbalance, and multipath propagation, among others. Importantly, notice that even with MetaFly in Fig. 15(b), the overall pattern and rotation of the constellation that Bob observes remain largely similar. This indicates the low-profile nature of the attack as the on-drone metasurface (with low refractive-index substrate) induces minimal change to the amplitude and phase of the symbols.

Moreover, channel training with physical-layer preambles is a common standardized technique for estimating and equalizing the channel, with yellow dots in Fig. 15 depicting such equalized symbols. As MetaFly is positioned in between the Alice-Bob link, the training phase then also encompasses an on-drone metasurface, with the transmission passing through it. As such, the metasurface is then effectively perceived as a part of the channel. This makes the attack even more challenging to detect for Bob. Thus, EVM, PAPR, and BER characteristics for two different scenarios are very similar as shown in Table 2.

Lastly, we extend the experiments to different modulation orders and study the overall impact of the attack on Bob's observed BER, depicting the results in Fig. 17. The blue and orange curves in the figure represent the baseline and MetaFly scenario, respectively, while the missing data points in this log-scale figure correspond to zero BER. Following the aforementioned reasons, the results in Fig. 17 indeed demonstrate the negligible impact of the attack on Bob's overall BER. (Note that, a zero measured BER means that the actual BER is less than $1/N_{bits}$, where $N_{bits} = 10000 \log_2(M)$ is the number of data bits [32].)

Findings: Detecting the attack is challenging for Bob as Eve purposefully exploits sub-THz transparent substrates in MetaFly design to leave a minimal energy footprint, only a few dB power shifts. Detecting such shifts is non-trivial for Bob because these changes are characteristic of ordinary wireless backhaul channels affected by weather conditions such as rain and snow and variable antenna alignment from buildings swaying. Overall, the attack minimally affects Bob's observed BER due to the low-profile nature of the on-drone metasurface that is perceived as a part of the channel during the channel training phase.

6.3. Rooftop Attack Demonstration

Thus far, we have demonstrated the attack in an indoor atrium environment. Here, we realize the attack on outdoor rooftops in a large metropolitan area and explore the ability of Eve to intercept the sub-THz transmitter.

To implement the attack in a large metropolitan area (between rooftops of an urban university campus) and fly MetaFly in the Federal Aviation Administration (FAA) regulated airspace region, a set of challenges had to be addressed. Those include completing the recreational Unmanned Aircraft System Safety Test (TRUST) to fly the drone in a controlled airspace zone, officially registering MetaFly in the FAA database (as it weighs more than 250 g) to be allowed to legally fly outdoors, and successfully passing a rooftop safety training course to gain access to the roofs, among others. Moreover, as the experiments were conducted on a university campus, we had to obtain authorization from both campus and local city police departments to be permitted to fly MetaFly over pedestrians, cars, and property.

The setup of the rooftop experiment is shown in Fig. 16. Bob and Eve are positioned on the roof of a 30-meter high library building while Alice is located on the engineering building roof, also at an elevation of 30 meters. Alice and Bob are approximately 30 m apart. The communicating parties are equipped with 40 dBi lens horn antennas, with such antennas placed on tripods to maintain the same elevation at Alice, Bob, and Eve. Eve's antenna is rotated 90° relative to Bob's to observe the cross-polarized eavesdropping signals. Since the backhaul link we set up for this experiment is not in the FCC database (thus no publicly available information on antenna locations), we flew MetaFly manually via the remote controller. Recall that our experiments in Sec. 5.3 indicated that Eve's best performance is obtained when MetaFly is closest to Bob, while placing MetaFly midway between Alice and Bob can serve as a compromise for Eve to avoid discovery with a minimal performance loss. Nonetheless, here Eve hovers MetaFly approximately 5 m from Alice for safety purposes, in case MetaFly has to be urgently landed on the roof and to avoid being directly above pedestrians walking on the ground level in between the buildings. In the experiment, Alice sends a sinusoidal tone at 130 GHz with transmit power of 13 dBm before the antenna, and her antenna is aimed directly at Bob.

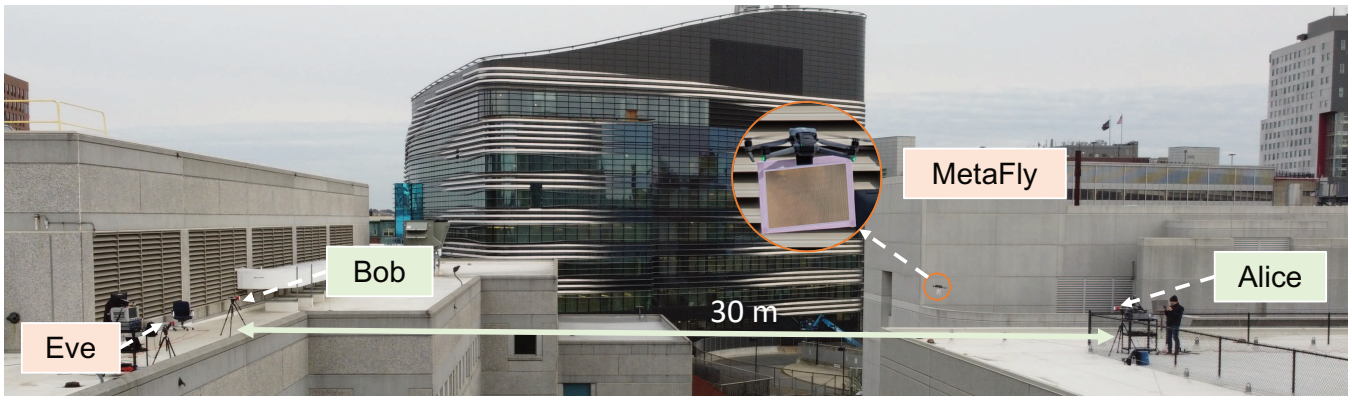


Figure 16: Eve armed with MetaFly intercepting a rooftop wireless backhaul link in a large metropolitan area.

Also, we conducted the metropolitan rooftop experiment using only the baseline continuous wave case. This is due to severe constraints on our experimental time, arising from legal and administrative challenges, as well as the requirement for supervised presence and police permissions. Nevertheless, in our future work, we plan to conduct additional rooftop experiments using modulated waves, similar to what we demonstrated in the atrium scenario in Sec. 5.

We depict the results in Fig. 18, showing frequency on the x-axis and power at Eve on the y-axis. As a baseline, we measure Eve's reception without MetaFly. Observe that the orange curve peaks at 130 GHz in Fig. 18(b) which indicates that with MetaFly, Eve can intercept the transmission with more than 40 dB relative to the baseline at that frequency. The weather during the experiment was moderately windy, with an average speed of approximately 10 mph and gusty variations due to turbulence between buildings. Nonetheless, MetaFly enabled sufficient flight stability (e.g., avoiding severe detrimental impacts of high roll variations as described in Sec. 5.1) to consistently generate an eavesdropping diffraction beam such that Eve can intercept that beam. Eve could improve her performance even further by realizing automatic flight control as discussed in Sec. 3.4.

Findings: Despite many regulatory and logistical challenges, we demonstrated the attack between two outdoor rooftops in a large metropolitan area. We showed that Eve can intercept a 130 GHz transmitter with 40 dB gain, even during moderately windy weather.

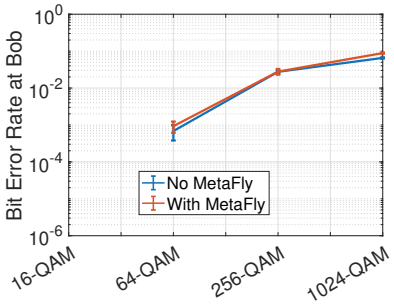
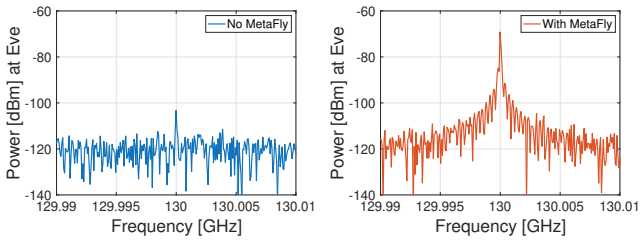


Figure 17: Attack impact across different QAM orders.



(a) No MetaFly (b) With MetaFly

Figure 18: Eve intercepting 130 GHz transmitter.

7. Related Work and Countermeasures

Metasurfaces and Wireless Security. Despite a large literature on metasurfaces [11], [13], [14], [33], [34], [35], [36], [37], [38], [39], only a few works focus on security, and those are limited to non-mobile metasurface structures. For instance, in [40], metasurfaces are hidden in the environment as a "bug" to carry out metasurface-in-the-middle attacks on WLANs, wall-integrated metasurfaces in [41] generate multi-lobe multi-frequency reflection patterns for concealed sideband eavesdropping, and meta-material tags in [42] launch wireless sensing attacks, imitating vanished objects (e.g., obstacles) and creating ghost effects. Conversely, [43] studies metasurface RF fingerprinting injection to enable secure authentication, while [12] proposes using reflecting metasurfaces to obfuscate wireless channels and protect wireless sensing. Unlike prior work, we study mobile aerial metasurfaces that can dynamically manipulate EM wavefront based on drone flight patterns and pose security threats to hard-to-reach wireless backhaul links.

Drones with Integrated Metasurfaces. A few recent works theoretically study drone systems with metasurfaces, mostly investigating communication performance enhancement applications. For example, reflective structures integrated on drones are considered in [44] to relay signals and assist terrestrial communication while [45] optimizes the number of on-drone reflecting elements and the drone height to numerically analyze outage probability and ergodic

capacity of the relaying system. In contrast, in this work, we theoretically investigate and experimentally demonstrate the first aerial transmissive metasurface and expose the security vulnerabilities of backhaul links to over-the-air attacks. Our workshop paper [46] outlines a similar roadmap but it neither has a full system design nor evaluation.

Defense Mechanisms. The attack we expose in this work is of low profile due to Eve's passive and transmissive metasurface. Yet, wireless backhauls could potentially be upgraded to continually and rigorously monitor the link for all relevant physical alterations, including the effects of different weather conditions, small-scale building motions, antenna misalignment, and aerial metasurfaces. Utilizing machine learning algorithms, the detection of any suspicious electromagnetic footprint could help in exposing the attack. Another possibility is to equip the backhaul infrastructures with advanced acoustic, visual, and infrared surveillance sensors and monitor the vicinity of the backhaul links for unauthorized drones. Such a defense mechanism could be highly effective for short and even mid-range backhaul links, but the performance is likely to diminish for kilometer-range links, in addition to adding extra cost overhead.

Lastly, it could be valuable to investigate the temporal aspect of aerial metasurface insertion. This involves examining situations where Alice and Bob deliberately seek out non-weather-signature SNR transitions to detect the attack. Yet, Eve can also control MetaFly to adjust patterns to better emulate different weather/misalignment effects. This presents a promising avenue for future research on countermeasures.

8. Conclusion

In this paper, we demonstrate for the first time the security vulnerabilities of wireless backhaul links to aerial metasurface attacks. We perform a theoretical and experimental investigation of the attack and show how Eve designs and deploys MetaFly to stealthily manipulate the EM wavefront of the backhaul signals.We study the strategy of the attacker and show her (meta)atom-by-atom design approach as well as the EM wavefront-tailored flight refinement principle. We fabricate the low-cost, lightweight, transmissive, and power-free aerial metasurface and implement the attack. We experimentally demonstrate the attack in an indoor atrium and outdoor rooftops and show that Eve can obtain nearly zero BER while having a minimal impact on legitimate communication.

References

[1] Allied Market Research. Wireless backhaul equipment market to reach 104.8 billion us dollars globally by 2031. Available: https://www.prnewswire.com/news-releases/wireless-backhaul-equipment-market-to-reach-104-8-billion-globally-by-2031-at-12-9-cagr-allied-market-research-301760705.html, [Accessed: July 31, 2023].

[2] Anova Financial Networks. Low latency financial connectivity. Available: https://anovanetworks.com/, [Accessed: July 31, 2023].

[3] Alpha Omega Wireless. Hospital gigabit wireless backhaul link. Available: https://www.aowireless.com/technology/case-studies/case-studies-downloads/hospital-gigabit-wireless-backhaul-link, [Accessed: July 31, 2023].

[4] Xiaohu Ge, Hui Cheng, Mohsen Guizani, and Tao Han. 5G wireless backhaul networks: challenges and research advances. *IEEE Network*, 28(6):6–11, 2014.

[5] Priyangshu Sen, Jose V Siles, Ngwe Thawdar, and Josep M Jornet. Multi-kilometre and multi-gigabit-per-second sub-terahertz communications for wireless backhaul applications. *Nature Electronics*, 6(2):164–175, 2023.

[6] George R MacCartney and Theodore S Rappaport. 73 GHz millimeter wave propagation measurements for outdoor urban mobile and backhaul communications in New York City. In *IEEE International Conference on Communications (IEEE ICC)*, pages 4862–4867. IEEE, 2014.

[7] A. Singh et al. A D-band radio-on-glass module for spectrally-efficient and low-cost wireless backhaul. In *2020 IEEE Radio Frequency Integrated Circuits Symposium (RFIC)*, pages 99–102. IEEE, 2020.

[8] Federal Communications Commission (FCC). Universal licensing system. Available: https://wireless2.fcc.gov/UlsApp/UlsSearch/searchAdvanced.jsp, [Accessed: July 31, 2023].

[9] Francesco Aieta, Patrice Genevet, Nanfang Yu, Mikhail A Kats, Zeno Gaburro, and Federico Capasso. Out-of-plane reflection and refraction of light by anisotropic optical antenna metasurfaces with phase discontinuities. *Nano Letters*, 12(3):1702–1706, 2012.

[10] Paul Staat, Harald Elders-Boll, Markus Heinrichs, Christian Zenger, and Christof Paar. Mirror, Mirror on the Wall: Wireless environment reconfiguration attacks based on fast software-controlled surfaces. In *Proceedings of the 2022 ACM on Asia Conference on Computer and Communications Security (ACM ASIA-CCS)*, pages 208–221, 2022.

[11] Kun Woo Cho, Mohammad H Mazaheri, Jeremy Gummeson, Omid Abari, and Kyle Jamieson. mmWall: A steerable, transflective metamaterial surface for NextG mmWave networks. In *20th USENIX Symposium on Networked Systems Design and Implementation (NSDI)*, pages 1647–1665, 2023.

[12] Paul Staat, Simon Mulzer, Stefan Roth, Veelasha Moonsamy, Markus Heinrichs, Rainer Kronberger, Aydin Sezgin, and Christof Paar. IRShield: A countermeasure against adversarial physical-layer wireless sensing. In *IEEE Symposium on Security and Privacy (IEEE S&P)*, pages 1705–1721. IEEE, 2022.

[13] 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):3926, 2020.

[14] Lili Chen, Wenjun Hu, Kyle Jamieson, Xiaojiang Chen, Dingyi Fang, and Jeremy Gummeson. Pushing the physical limits of IoT devices with programmable metasurfaces. In *USENIX Symposium on Networked Systems Design and Implementation (USENIX NSDI)*, 2021.

[15] Anova Financial Networks. Nokia demonstrates live D-Band microwave backhaul connection. Available:https://www.nokia.com/about-us/news/releases/2022/04/13/nokia-demonstrates-live-d-band-microwave-backhaul-connection/, [Accessed: July 31, 2023].

[16] Priyangshu Sen, Jacob Hall, Michele Polese, Vitaly Petrov, Duschia Bodet, Francesco Restuccia, Tommaso Melodia, and Josep M Jornet. Terahertz communications can work in rain and snow: impact of adverse weather conditions on channels at 140 GHz. In *Proceedings of the 6th ACM Workshop on Millimeter-Wave and Terahertz Networks and Sensing Systems (ACM mmNets)*, pages 13–18, 2022.

[17] Vasileios Mavroeidis, Kamer Vishi, Mateusz D. Zych, and Audun Jøsang. The impact of quantum computing on present cryptography. *International Journal of Advanced Computer Science and Applications*, 9(3), 2018.

[18] Constanze Dietrich, Katharina Krombholz, Kevin Borgolte, and Tobias Fiebig. Investigating system operators' perspective on security misconfigurations. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security (ACM CCS)*, pages 1272–1289, 2018.

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

[20] Paul C Kocher. Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems. In *Annual International Cryptology Conference*, pages 104–113. Springer, 1996.

[21] David Brumley and Dan Boneh. Remote timing attacks are practical. *Computer Networks*, 48(5):701–716, 2005.

[22] Alexander V Kildishev, Alexandra Boltasseva, and Vladimir M Shalaev. Planar photonics with metasurfaces. *Science*, 339(6125):1232009, 2013.

[23] 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.

[24] 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.

[25] H. Guerboukha et al. High-volume rapid prototyping technique for terahertz metallic metasurfaces. *Optics Express*, 29(9):13806–13814, 2021.

[26] Amazon. Glossy everyday printer paper, 8.5 x 11 inches. https://www.amazon.com/Hammermill-10263-0-PREMIUM-BRIGHT-500-Sheets/dp/B01FDD8PGO/ref=sr_1_5?keywords=hammermill+premium+color+copy&qid=1691030260&sprefix=hammermill+prem%2Caps%2C151&sr=8-5. Accessed [July 31, 2023].

[27] Amazon. Overhead project transparency printing sheet. https://www.amazon.com/Overhead-Project-Transparency-Printing-Definition/dp/B08139J4JR/ref=sr_1_5?crid=3BCXEO9999DZ1&keywords=plastic+printing+sheet&qid=1690646277&sprefix=plastic+printing+shee%2Caps%2C165&sr=8-5. Accessed [July 31, 2023].

[28] Amazon. iCraft Deco foil value pack, 6 x 12 inches, 20 sheets. https://www.amazon.com/iCraft-Deco-Foil-Value-inches/dp/B075TJ6S1L/ref=sr_1_1?crid=3QJG2GF5HKW7E&keywords=deco%2Bfoil%2Bicraft&qid=1678386275&sprefix=%2Caps%2C134&sr=8-1&th=1. Accessed [July 31, 2023].

[29] Akihiko Hirata. Transmission trial of television broadcast materials using 120-GHz-band wireless link. *NTT Tech. Rev.*, 7(3), 2009.

[30] 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.

[31] Phuc Nguyen, Hoang Truong, Mahesh Ravindranathan, Anh Nguyen, Richard Han, and Tam Vu. Matthan: Drone presence detection by identifying physical signatures in the drone's RF communication. In *Proceedings of the 15th Annual International Conference on Mobile Systems, Applications, and Services (ACM MobiSys)*, pages 211–224, 2017.

[32] Dragan Mitić, Aleksandar Lebl, and Žarko Markov. Calculating the required number of bits in the function of confidence level and error probability estimation. *Serbian Journal of Electrical Engineering*, 9(3):361–375, 2012.

[33] 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):4334, 2018.

[34] Antonio Albanese, Francesco Devoti, Vincenzo Sciancalepore, Marco Di Renzo, and Xavier Costa-Pérez. MARISA: a self-configuring metasurfaces absorption and reflection solution towards 6G. In *IEEE Conference on Computer Communications (IEEE INFOCOM)*, pages 250–259. IEEE, 2022.

[35] 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 (ACM MobiCom)*, pages 587–600, 2021.

[36] Venkat Arun and Hari Balakrishnan. RFocus: Beamforming using thousands of passive antennas. In *17th USENIX Symposium on Networked Systems Design and Implementation (USENIX NSDI)*, pages 1047–1061, 2020.

[37] Weihan Li, Qian Ma, Che Liu, Yunfeng Zhang, Xianning Wu, Jiawei Wang, Shizhao Gao, Tianshuo Qiu, Tonghao Liu, Qiang Xiao, et al. Intelligent metasurface system for automatic tracking of moving targets and wireless communications based on computer vision. *Nature Communications*, 14(1):989, 2023.

[38] Kun Qian, Lulu Yao, Xinyu Zhang, and Tse Nga Ng. MilliMirror: 3D printed reflecting surface for millimeter-wave coverage expansion. In *Proceedings of the 28th Annual International Conference on Mobile Computing And Networking (ACM MobiCom)*, pages 15–28, 2022.

[39] Dianhan Xie, Xudong Wang, and Aimin Tang. MetaSight: localizing blocked RFID objects by modulating NLOS signals via metasurfaces. In *Proceedings of the 20th Annual International Conference on Mobile Systems, Applications and Services (ACM MobiSys)*, pages 504–516, 2022.

[40] Z. Shaikhanov et al. 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 (ACM WiSec)*, 2022.

[41] Haoze Chen, Hooman Saeidi, Suresh Venkatesh, Kaushik Sengupta, and Yasaman Ghasempour. Wavefront manipulation attack via programmable mmWave metasurfaces: from theory to experiments. In *Proceedings of the 16th ACM Conference on Security and Privacy in Wireless and Mobile Networks (ACM WiSec)*, pages 317–328, 2023.

[42] Xingyu Chen, Zhengxiong Li, Baicheng Chen, Yi Zhu, Chris Xiaoxuan Lu, Zhengyu Peng, Feng Lin, Wenyao Xu, Kui Ren, and Chunming Qiao. MetaWave: Attacking mmWave sensing with metamaterial-enhanced tags. In *The 30th Network and Distributed System Security (NDSS) Symposium*, volume 2023, 2023.

[43] S. Rajendran et al. Injecting reliable radio frequency fingerprints using metasurface for the Internet of Things. *IEEE Transactions on Information Forensics and Security*, 16:1896–1911, 2020.

[44] X. Pang et al. When UAV meets IRS: Expanding air-ground networks via passive reflection. *IEEE Wireless Communications*, 28(5):164–170, 2021.

[45] T Shafique et al. Optimization of wireless relaying with flexible UAV-borne reflecting surfaces. *IEEE Transactions on Communications*, 69(1):309–325, 2020.

[46] Zhambyl Shaikhanov, Sherif Badran, Josep M Jornet, Daniel M Mittleman, and Edward W Knightly. Remotely positioned metasurface-drone attack. In *Proceedings of the 24th International Workshop on Mobile Computing Systems and Applications*, pages 110–116, 2023.