Remotely Positioned MetaSurface-Drone Attack

Zhambyl Shaikhanov
Rice University
zs16@rice.edu

Sherif Badran
Northeastern University
badran.s@northeastern.edu

Josep M. Jornet
Northeastern University
j.jornet@northeastern.edu

Daniel M. Mittleman
Brown University
daniel_mittleman@brown.edu

Edward W. Knightly
Rice University
knightly@rice.edu

ABSTRACT

We demonstrate for the first time security vulnerabilities of wireless backhaul links to aerial metasurfaces. Considering over-the-air threats and a strong adversary, we define and experimentally demonstrate the "**R**emotely Positioned **M**etaSurface-**D**rone" (**RMD**) attack. In the attack, the adversary Eve remotely approaches hard-to-reach wireless backhaul links, e.g., between towers and rooftops, and stealthily manipulates highly directive backhaul transmissions on-the-fly, enabling remote eavesdropping. To realize the attack, she designs a lightweight power-free transmissive on-drone diffractive metasurface. Exploring the foundations of the attack, we show how Eve induces a secret 3D diffraction radiation beam on the intercepted transmission, re-purposing it for eavesdropping. We investigate Eve's bit-error-rate (BER)-driven flight navigation strategy and show how she can adapt the RMD flight pattern to dynamically shape the diffraction radiation beam and consistently improve her signal reception at a remote location. We implement the attack and perform a series of preliminary experiments with wireless links above 100 GHz having multi-GHz-wide bandwidth. Our results reveal that the RMD attacker can intercept backhaul transmissions with nearly zero BER while maintaining minimal impact on legitimate communication.

CCS CONCEPTS

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

KEYWORDS

metasurfaces, drones, wireless backhaul links, mmWave/sub-THz

ACM Reference Format:
Zhambyl Shaikhanov, Sherif Badran, Josep M. Jornet, Daniel M. Mittleman, and Edward W. Knightly. 2023. Remotely Positioned MetaSurface-Drone Attack. In *The 24th International Workshop on Mobile Computing Systems and Applications (HotMobile '23), February 22–23, 2023, Newport Beach, CA, USA.* ACM, New York, NY, USA, 7 pages. https://doi.org/10.1145/3572864.3580343

1 INTRODUCTION

Wireless backhaul links are an integral part of wireless communication and are widely employed for many critical functions, including financial trading on Wall Street [1], medical record exchange in hospitals [2], and private data sharing in 5G [3]. Wireless backhaul antennas are generally positioned in elevated hard-to-reach 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 transmissions [4, 5].

Because wireless backhaul links i) are typically encrypted using methods such as RSA for secure key exchange and ii) employ highly directive hard-to-reach beams, they are assumed to be highly secure. However, due to the rapid advancement of quantum computing and human/operator-centric network management, such encryptions are vulnerable to quantum computing attacks [6] and misconfiguration [7]. In this paper, we show for the first time, that the latter property is unfortunately equally mistaken with a strong adversary. In particular, we demonstrate *"**R**emotely Positioned **M**etaSurface-Drone" (**RMD**)* attacks in which the adversary secretly manipulates wireless backhaul transmission wavefront to enable remote eavesdropping. We perform a theoretical and experimental study of the attack and make the following contributions.

First, we analyze the foundations of the RMD attack and investigate the attacker's principles of aerial transmission manipulations. To begin, we show that the eavesdropper, Eve, overcomes the physical challenges of the backhaul setting by exploiting an off-the-shelf drone to remotely approach the targeted link. To avoid obstructing the link and thereby revealing the attack, Eve designs a transmissive on-drone metasurface and stealthily manipulates the backhaul link on-the-fly. That is, she covertly generates an additional 3D diffractive eavesdropping link steered from the metasurface towards her position. We explore the fundamentals of RMD-induced aerial diffraction radiation patterns via the analysis of generalized Snell's law in 3D and study the impact of RMD state, i.e., position and orientation, on the effective diffraction radiation pattern. We show how the attacker leverages the mobility of the RMD to shape the targeted diffraction radiation patterns dynamically, mimicking a programmable metasurface. It allows Eve to adapt her physical position to a self-selected remote location in her attack mission.

Second, we study Eve's design choices in realizing the on-drone metasurface and explore her flight navigation strategy that enables improved signal reception. In particular, inheriting drone system challenges, e.g., limited battery power and minimal payload carrying capability, we show how Eve strategically designs lightweight static on-drone metasurface. Specifically, she first constructs passive C-shape meta-atoms (whose EM responses she controls via

HotMobile '23, February 22–23, 2023, Newport Beach, CA, USA

ACM ISBN 979-8-4007-0017-0/23/02…$15.00
https://doi.org/10.1145/3572864.3580343

the geometrical properties of the C-shape) and then systematically arranges an array of meta-atoms on the sub-THz transmissive substrate to yield targeted diffractive metasurface. As we fabricate and demonstrate, such an aerial metasurface can weigh only several grams and requires no power source. Moreover, the choice of the sub-THz transmissive substrate in the design allows Eve to pass through most of the transmission energy and maintain the legitimate link, thus making the attack challenging to detect. In addition, we describe Eve's feedback-driven RMD flight navigation strategy and show how she adapts flight patterns based on her observed signal quality at a remote location. Specifically, she designs a bit-error-rate (BER)-centric navigation controller that continually adjusts the RMD flight to minimize her received BER. Such adaptive flight technique is particularly relevant when the drone drifts during the attack, e.g., due to GPS error, inertial sensor imperfections, or wind impact, and needs readjustment to restore the diffraction radiation beams.

Third, we implement the attack and perform experimental evaluations: We first configure a sub-THz communication testbed in which Alice and Bob establish a highly directional link using horn antennas. Alice transmits modulated data to Bob at 130 GHz carrier frequency using 5 GHz bandwidth. Next, we design and prototype Eve's lightweight diffractive metasurface targeting the center frequency, and integrate it with an off-the-shelf drone platform. To demonstrate the principles of the attack, we perform a series of proof-of-concept experiments. First, we perform a feasibility study of the attack and show how RMD can induce a phase discontinuity at the on-drone metasurface and generate the targeted eavesdropping diffraction link on the fly, with Eve remotely intercepting. Next, we investigate the effectiveness of the attack by analyzing Eve's BER performance with varying modulation orders. The results reveal that Eve can obtain 10^{-4} scale BER at lower modulation orders, however, it gradually degrades as the order increases and becomes more sensitive to small-scale drone mobility such as wobbling. Finally, we explore the stealthiness of the attack by analyzing the attack's footprint at Bob, as the disruption of the Alice-Bob link might alert him of the attack. Investigating the power spectral profile of Bob with and without the RMD, we find that Eve leaves a minimal attack footprint of several dB power decrease at Bob, a difference that may be hard for Alice and Bob to differentiate from effects of weather.

Additionally, we highlight that the RMD attack yields an acute vulnerability, even when the wireless encryption is in place and not broken. That is, the attack leaves some control information exposed as standards do not encrypt all components of control information such as packet headers, channel state feedback, and addresses [8]. Moreover, under the RMD attack, associated timing information would also be exposed and thus yield vulnerable side channel information exploitable by strong adversaries [9, 10]

2 SYSTEM AND ADVERSARY MODEL

2.1 Threat Model and Topology

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

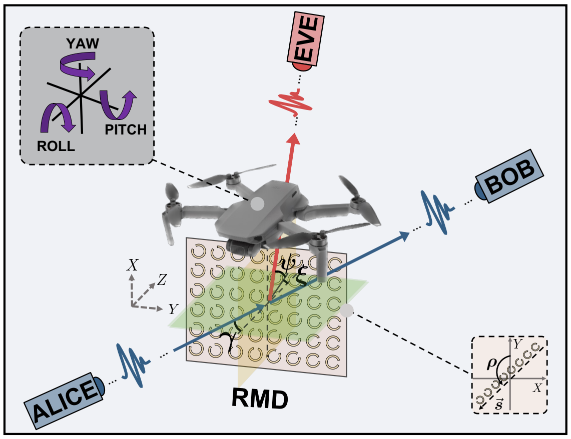


Figure 1: Overview of the RMD attack

We designate the carrier frequency and bandwidth of the transmission as f_c and B, respectively, and consider modulated data exchange between Alice and Bob. Without loss of generality, we demonstrate the attack with a M-QAM modulation scheme where M indicates modulation order. The geographical coordinates of the communications parties are denoted as C^{Alice}, $\mathbf{C}^{\text{Bob}}$ and $\mathbf{C}^{\text{Eve}}$ where $\mathbf{C}^{\text{Alice}} = (x^{\text{Alice}}, y^{\text{Alice}}, z^{\text{Alice}})$. Eve knows the locations of Alice and Bob and has general transmission information such as carrier frequency, bandwidth, and modulation scheme.

Given the hard-to-access backhaul link environment, the attacker strategy exploits a drone as a remotely controlled aerial platform to be positioned to the vicinity of the link. Eve designs a lightweight on-drone metasurface that enables advanced on-the-fly electromagnetic wavefront manipulation capability. 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 RMD. The location and orientation of the metasurface at time t is denoted as $\mathbf{C}_t^{\text{RMD}}$ and $\boldsymbol{\theta}_t^{\text{RMD}}$, respectively. We define the orientation of the RMD as $\boldsymbol{\theta}_t^{\text{RMD}} = (\theta_{t,\,yaw}^{\text{RMD}}, \theta_{t,\,pitch}^{\text{RMD}}, \theta_{t,\,roll}^{\text{RMD}})$ 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 the design choice of the on-drone metasurface in §3.1.

2.2 Aerial Wavefront Manipulation

Eve generates a 3D diffraction at the metasurface by creating a cross-polarized diffracted beam via a phase change at the interface. That is, she creates a cross-polarized eavesdropping link from $\mathbf{C}^{\text{RMD}}$ to $\mathbf{C}^{\text{Eve}}$, while also allowing the original beam to pass through with its original polarization for reception at Bob.

To demonstrate the principles, consider Fig. 1 in which Alice and Bob are in the yz-plane and Eve's on-drone metasurface is in the xz-plane. Eve intercepts Alice's transmission with angle γ relative to the z-axis. She then establishes a diffraction beam directed toward herself at angle ψ and ξ, in which ψ denotes 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. Importantly, Eve controls the direction of the generated diffraction beam governed by the generalized Snell's law in 3D [11] as:

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

In Eq. (1), c is the speed of light and $n_\gamma(n_\psi)$ denotes the refractive index of the propagation medium, approximated as one given the over-the-air transmission. $\nabla\Phi$ is the imposed phase gradient with $d\Phi/dx$ and $d\Phi/dy$ indicating the phase changes along x-axis and y-axis. In its absence, i.e., $d\Phi/dx = 0$ and $d\Phi/dy = 0$, Eq. (1) reduces to standard Snell's law, describing transmission direction change due to different medium. However, Eve purposefully introduces a spatially periodic phase gradient at the on-drone metasurface to induce diffraction radiation patterns in 3D and controls diffracted beam direction via Eq. (1). She physically realizes such phase gradient by strategically designing and arranging a group of meta-atoms (C-shaped elements in Fig. 1) as we discuss in §3.1. 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.

Eve also leverages the mobility of the RMD to dynamically steer generated diffraction beams. For instance, given the static on-drone metasurface, she can adjust ψ and ξ during the flight via the corresponding roll movement of the RMD. That is, via rolling around the longitudinal axis, RMD can effectively rotate the attached on-drone metasurface and configure the orientation ρ such that targeted $d\Phi/dx$ and $d\Phi/dy$ phase changes are induced at the interface, yielding desired diffraction beam angle. Eve can leverage the yaw movement of the RMD to intercept the transmission with different incidence angles γ, such mobility enabling control over the ψ component of the beam with a sinusoidal effect.

Moreover, with the RMD mobility, Eve can generate diffraction beams in 3D as formulated in Eq. (1). For instance, she could adjust the RMD flight pattern (i.e., yaw movement directed towards zero phase gradient orientation) to induce phase change only in the y-axis. In doing so, she creates a diffractive link in the same Alice-Bob transmission plane. She might favor such a configuration when eavesdropping on the backhaul link from the nearby building rooftop of the same altitude as Bob. However, modifying RMD flight to have non-zero ρ enables phase discontinuities periodically along both axes. This allows Eve to generate a diffraction link directed out of Alice-Bob's transmission plane, such effect governed via the parameter ξ in Eq. (1). Eve is likely to undertake it when she is physically at a different altitude than Bob, e.g., eavesdropping from the ground level or a building of a different height.

3 ATTACKER'S STRATEGY

3.1 On-Drone Metasurface Design

There are multiple design criteria the attacker considers when realizing the on-drone metasurface. First, Eve's on-drone metasurface must be lightweight so that RMD can efficiently carry it in the mission without majorly spending (already limited) battery resources on the additional heavy payload. Second, the metasurface must be sub-THz transmissive such that Eve can (not only establish an eavesdropping link but also) maintain the Alice-Bob link, passing through most of the signal energy and not revealing the attack. Third, the metasurface must be able to perform aerial wavefront manipulation functionalities described in §2.2. Lastly, the physical realization of such a metasurface should be inexpensive for Eve to reduce the overall cost of the attack.

Following these criteria, the RMD attacker designs a static metasurface on a very thin ($\ll$ wavelength) substrate. That is, meta-atoms (unit elements) in the RMD design provide targeted phase and amplitude responses based on their geometrical properties (orientation and size), in contrast to active metasurfaces that need external power to activate the elements. Although active metasurfaces can provide dynamic wavefront manipulation capability, Eve is likely to avoid such designs because they add extra payload (e.g., additional switching components, external power supply, and FPGA-based controller unit) and can drain her RMD battery increasingly fast, potentially leading to failed attack. As we prototype and demonstrate in §4, the static metasurface of the attacker could be as light as several grams.

Also, Eve purposefully selects a sub-THz transparent material (with a low refractive index) as the metasurface substrate in her design to secretly carry out the attack. Specifically, she chooses materials like paper and polymer sheets that incur negligible absorption loss at these high frequencies and arranges meta-atoms on such substrates. This enables Eve to pass through most of the Alice to Bob signal power, maintaining the high SNR legitimate link. With the RMD, Eve then efficiently intercepts and re-directs only a portion of the power to herself, which is quite sufficient to eavesdrop with very low BER as we show in §4.2.

A meta-atom is a sub-wavelength scale metallic structure that functions as the building block of a metasurface. We demonstrate the RMD with a C-shaped split ring resonator meta-atom which exhibits a strong response at sub-THz frequencies. Importantly, Eve can control the amplitude and phase response of such meta-atoms based on their radius r, slit opening α, and orientation β [12]. As an example, she can induce π phase shift by rotating the C-shape by 90° and exploits a symmetrical amplitude response that follows the $|\sin 2\beta|$ function. To expedite the design process, she generates phase shift and amplitude transmission heatmaps as a function of different geometrical parameters and selectively chooses parameter values corresponding to the targeted responses. As we demonstrate in [13], Eve then strategically arranges a group of meta-atoms (supercell) to induce abrupt phase changes across a spatial period. Specifically, she constructs a supercell consisting of eight different meta-atoms that realizes phase discontinuity covering 2π across that spatial period. We demonstrate the RMD attack with the following meta-atom configurations (r, α, β): $(240\mu m, 136^\circ, -45^\circ)$,

$(284\mu m, 82°, -45°)$, $(296\mu m, 32°, -45°)$, $(320\mu m, 12°, -45°)$ and their $90°$ rotated counterparts, corresponding to the $|\nabla\Phi| = 2\pi/6.11mm$.

Eve employs a simple yet effective fabrication technique to create low-cost on-drone metasurface. In particular, she takes advantage of the hot-stamping method [14], printing a designed metasurface pattern on a piece of paper and stamping it on a metallic foil sheet via a heated laminator. Importantly, Eve needs only standard office supplies, such as a printer, and laminator, and can fabricate the metasurface in minutes [15], bringing the cost of the attack to a minimum.

3.2 BER-adaptive Flight Navigation

Although RMD enables access to hard-to-reach backhaul links, it also incurs positioning inaccuracies and occasional instabilities, resulting from different factors, such as navigation sensor errors and wind impact. Then, wobbling and fluctuations of the RMD are likely to distort generated diffraction radiation beam and degrade Eve's SNR. In the attack mission, Eve adapts RMD flight patterns in real-time to dynamically manipulate and adjust the transmission wavefront, mimicking a programmable metasurface. For that, she designs the BER feedback-driven RMD flight adaptation strategy.

As shown in the feedback control loop in Fig. 2, Eve's adaption controller computes the next best RMD location $\mathbf{C}^{*\text{RMD}}_{t+1}$ to fly and the orientation $\boldsymbol{\theta}^{*\text{RMD}}_{t+1}$ to take while the actuator receives the command and executes it. With RMD establishing diffraction link, the controller receives information regarding Eve's observed signal quality and the RMD status (on-drone metasurface and navigation information) and targets to find the next RMD state at $t + 1$ that minimizes BER^{Eve}_{t+1}. Formally, for as long as the attack mission lasts and the RMD has sufficient battery power to operate, it performs the following operation:

$$
\begin{aligned}
\{\mathbf{C}^{*\text{RMD}}_{t+1},\ \boldsymbol{\theta}^{*\text{RMD}}_{t+1}\} = \underset{\mathbf{C}^{\text{RMD}}_{t+1},\ \boldsymbol{\theta}^{\text{RMD}}_{t+1}}{\arg\min}\ & BER^{\text{Eve}}_{t+1}(\mathbf{C}^{\text{RMD}}_{t+1}, \boldsymbol{\theta}^{\text{RMD}}_{t+1}, \mathscr{L}) \\
\text{subject to }\ & \mathbf{C}^{\text{RMD}}_{t+1} \in \mathscr{P} \\
& \boldsymbol{\theta}^{\text{RMD}}_{t+1} \in \mathscr{R}
\end{aligned}
\tag{2}
$$

where $\mathscr{P}$ is the set containing all locations that RMD can reposition at time $t + 1$, $\mathscr{R}$ is the set of all achievable RMD orientations at $t + 1$, and $\mathscr{L}$ is the set containing previous observations $\{\mathbf{C}^{\text{RMD}}_{\tau},\ \boldsymbol{\theta}^{\text{RMD}}_{\tau}, BER^{\text{Eve}}_{\tau}\}$ where $\tau = 0, 1, 2, ..., t$.

In the decision process, the adaptation controller leverages the fundamental knowledge of how the RMD flight pattern affects the diffraction beam formation discussed in §2.2. In particular, it exploits the impact of the corresponding RMD roll movement on the induced phase gradient magnitude $|\nabla\Phi|$ and ρ. In doing so, it, in principle, defines the direction of the diffraction beam as formulated in Eq. (1), re-directing it towards Eve. Also, the controller takes advantage of the yaw rotation to enable transmission interception with different impinging angles, thus adjusting the ψ value of the diffraction beam angle as needed. Importantly, such mobility effects on the aerial wavefront manipulation are integrated as a part of the adaptation decision process and assist in RMD flight navigation to improve signal reception at Eve.

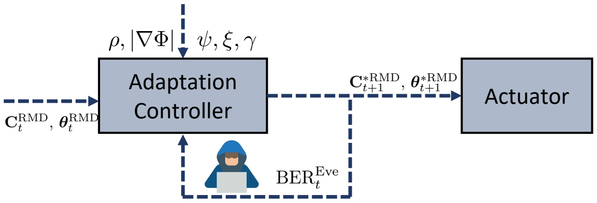

$\rho, |\nabla\Phi|$
ψ, ξ, γ
Adaptation Controller
$\mathbf{C}^{\text{RMD}}_{t}, \boldsymbol{\theta}^{\text{RMD}}_{t}$
$\mathbf{C}^{*\text{RMD}}_{t+1}, \boldsymbol{\theta}^{*\text{RMD}}_{t+1}$
Actuator
$\text{BER}^{\text{Eve}}_{t}$

Figure 2: The BER-adaptive flight navigation controller

Moreover, the controller keeps a record of the prior observations and leverages them to learn from the previous flight decisions. In Eq. (2), this is indicated with expression $\mathscr{L}$ capturing information on previous BER observations and corresponding reposition and reorientation decisions. As such, RMD flight decisions are also refined based on the history of RMD flight patterns and resulting diffraction radiation beams, minimizing the BER by learning from the past. Eve updates the RMD state at the interval of T. It could be static as well as dynamic and dictated mainly by how well she can maintain a particular BER before the diffraction beam gets distorted. Obviously, achievable BER and its consistency over time also depend on the quality of her underlying drone platform and navigation sensors. The more the attacker is willing to invest in the drone infrastructure, the more accurately she can navigate the RMD and precisely manipulate the aerial wavefront, eavesdropping with low BER.

4 IMPLEMENTATION AND PRELIMINARY EXPERIMENTAL RESULTS

4.1 RMD Prototype and Setup

We create a small-scale indoor experimental test setup depicted in Fig. 4(a). Built upon the TeraNova sub-THz testbed, it consists of one transmitter (Bob), two receivers (Alice and Eve), and the RMD. The distances between Alice and the RMD, the RMD and Bob, the RMD and Eve, and Bob and Eve are 140, 170, 160, and 72 cm respectively, an equal height of 150 cm to mimic the future outdoor rooftop experiment. In fact, the authors have demonstrated rooftop-scale wireless links above 100 GHz with this testbed as shown in Fig. 3 [16].

We design and fabricate an on-drone metasurface following the procedures in §3.1. Illustrated in Fig. 4(c), the prototype is of size A4 paper and weighs only 8 grams (without frame). We design a plastic frame to hold the metasurface and integrate it into the DJI Mavic drone shown in Fig. 4(b).

Alice's modulated data waveforms are sent in the intermediate frequency (IF) with 5 GHz transmission bandwidth to the transmitter frontend, upconverted to 130 GHz, and then transmitted over the air with 20 mW of power via a high gain 40 dBi directional lens horn antenna to the receiver. At the receiver (Bob and Eve),

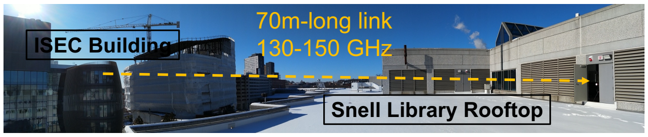


Figure 3: Outdoor backhaul-scale link above 100 GHz

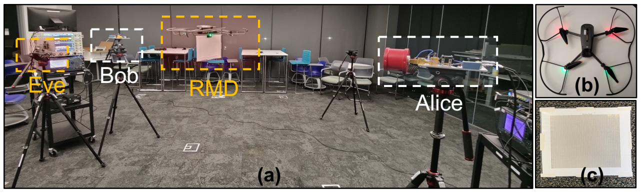


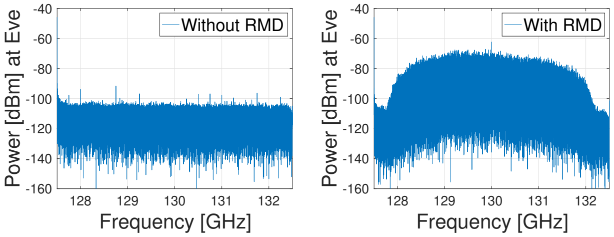
Figure 4: RMD attack experimental setup

the signal is picked up using 22 dBi horn antennas, amplified, filtered, downconverted back to IF, digitized, and stored using a digital storage oscilloscope for further signal processing. Alice and Bob's antennas are horizontally polarized, while Eve rotates her antenna 90° to observe cross-polarized signals diffracted from the RMD. The TeraNova backend is employed to perform channel estimation, equalization, and demodulation.

4.2 Attack Feasibility Study

First, we perform a feasibility study of the RMD attack, investigating the RMD ability to generate a targeted eavesdropping diffraction link with remote Eve intercepting it.

We consider the on-drone metasurface design discussed in §3.1 and the setup described in §4.1. We configure the RMD to hover between Alice and Bob (no flight adaptation). Eve is positioned at approximately 23° from Bob, observing the diffraction beam peak. As a baseline, we consider the case when Eve does not employ the RMD in the attack.



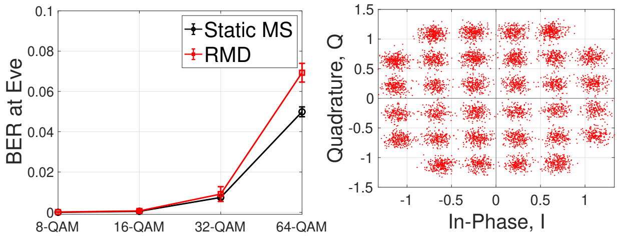
(a) Eve without RMD **(b) Eve employing RMD**

Figure 5: Exploring the diffraction beam establishment

In Fig. 5(a)-(b), we depict Eve's power spectral profile for the aforementioned two scenarios. Without the RMD to remotely approach and manipulate the Alice-Bob link, Eve is not able to observe the transmission and thus largely receives noise. It is indicated as blue curves fluctuating below −100dBm in Fig. 5(a). However, the RMD allows her to induce $|\nabla\Phi| = 2\pi/6.11mm$ phase discontinuity and generate a diffraction beam steered to her angular location as formulated in Eq. (1). Re-purposing it as an eavesdropping link, she can then obtain, on average, more than 20 dB above the noise floor signal power across the targeted 5 GHz bandwidth.

4.3 Effectiveness of the RMD Attack

Next, we explore the effectiveness of the attack by analyzing Eve's BER performance as a function of modulation orders.



(a) BER performance **(b) 32-QAM**

Figure 6: Investigating the effectiveness of the attack

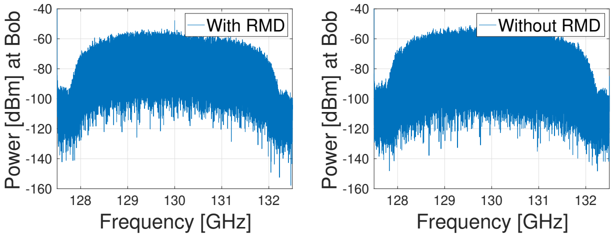
We consider the previously described RMD design and experimental setup and vary Alice's transmission from 8-QAM to 32QAM. For each modulation order, we run experiments at least 10 times and report the mean and the standard deviation of the observed BER. As a baseline, we consider a static metasurface (MS) scenario with similar design parameters and located in a similar position as the on-drone metasurface. We report results in Fig. 6(a) and show an exemplary constellation at Eve with 32-QAM in Fig. 6(b).

Observe that, with lower modulation orders, i.e., 8-QAM and 16-QAM, Eve's BER performance with RMD is similar to one with static MS, 10^{-4} scale in both cases. However, that pattern changes as the order increases. In particular, the RMD results in higher mean BER and fluctuations relative to the static MS counterpart, despite both cases having identical metasurface design and positioning. For instance, her mean BER with RMD at 64-QAM is 39% larger than the one with static MS in a similar order. It is mainly due to the wobbling and unsteady hover motion of the RMD, which is particularly dominant in an indoor environment that lacks GPS. Such mobility is likely to change phase gradient orientation and, consequently, alters spatial phase gradients $d\Phi/dy$ and $d\Phi/dx$. In turn, it alters the generated diffraction beam discussed in §2.2, increasing Eve's observed BER. This effect is similarly shown in Fig. 6(b) as spreading out of circles in the constellation points, indicating the sensitivity of Eve's BER to RMD stability, especially at higher modulation order.

4.4 Impact of the Attack at Bob

Here, we investigate stealthiness of the attack by studying the energy footprint of the RMD at Bob, as the disruption of the legitimate link likely to alter him of a possible attack. We consider Bob's observation without RMD as a baseline and employ a similar setup discussed previously.

In Fig. 7(a)-(b), we show Bob's power spectral profile with and without RMD, respectively. Notice that the power spectrum patterns in the two scenarios are quite similar, albeit with a few dBm power shifts. That is, Eve purposefully exploits the sub-THz transparent structure (paper in this demonstration) as the on-drone metasurface substrate to allow Alice's transmission to pass through and reach Bob. In doing so, she maintains the legitimate link and leaves a minimal attack footprint. Moreover, our preliminary BER results reveal that Bob, on average, sustains below 10^{-3} BER across different modulation schemes when the RMD is employed in the attack, indicating the low-profile nature of the attack.



(a) Bob with RMD **(b) Bob without RMD**

Figure 7: RMD presence as observed by Bob

Eve manipulates the transmission in a cross-polarized regime and re-directs a portion of the energy towards herself, which is exhibited in the form of a few dBm power decrease in Fig. 7. Yet, detecting such an energy footprint would be extremely challenging for Bob because wireless backhaul channels observe similar channel variations even without the RMD. Specifically, backhaul infrastructures on towers and buildings are prone to swaying due to wind. 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 between a few dB to several tens of dB compared to the clear weather at these frequencies [16].

5 RELATED WORK

Metasurfaces and Wireless Security. Although there is a large literature on metasurfaces , only a few works focus on security, and those typically explore stationary structures. For instance, in [13], metasurfaces are hidden in the environment as a 'bug' and carry out metasurface-in-the-middle attacks on directive links; malicious metasurfaces in [17] generate multi-lobe multi-frequency reflection patterns for concealed sideband eavesdropping. Conversely, [18] study metasurface RF fingerprinting injection to enable secure authentication. Unlike prior work, we explore mobile aerial metasurfaces that dynamically manipulate wavefront by flight adaptation and pose security threats to backhauls.

Drones with Integrated Metasurfaces. A few recent works theoretically study drone systems with metasurfaces, investigating communication performance enhancement applications. For example, reflective structures integrated on drones are considered in [19] to relay signals and assist terrestrial communication while [20] 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, we theoretically investigate and experimentally demonstrate the first aerial transmissive metasurface and expose the security vulnerabilities of wireless backhaul links to over-the-air attacks.

6 CONCLUSION AND FUTURE WORK

In this paper, we demonstrate for the first time the security vulnerabilities of wireless backhaul links to aerial metasurfaces. We explore the foundations of the attack and study the strategy of the RMD attacker. We implement the attack and perform preliminary experimental evaluations.

In our future work, we plan to implement the attack in a long-range outdoor environment and experimentally evaluate Eve's BER-adaptive flight strategy and its performance. We also target to study the different scenarios of the attack such as Eve being at various locations, e.g., on the ground level, inside a building, and on a rooftop, and investigate RMD aerial wavefront manipulation capabilities in corresponding scenarios. Finally, we will explore countermeasures against RMD attacks and study their effectiveness.

7 ACKNOWLEDGEMENTS

This research was supported by Cisco, DoD: Army Research Laboratory grant W911NF19-2-0269, Intel, and by NSF grants CNS-1954780, CNS-2211616, CNS-1955004, CNS-2225590, CNS-1801865, CNS-1955075, and CNS-2211618

REFERENCES

[1] Anova Financial Networks. Low latency financial connectivity. Available: https://anovanetworks.com/, [Accessed: January 4, 2023].

[2] 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: January 4, 2023].

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

[4] 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 *2014 IEEE International Conference on Communications (ICC)*, pages 4862–4867. IEEE, 2014.

[5] Amit Singh, Mustafa Sayginer, Michael J Holyoak, Joseph Weiner, John Kimionis, Mohamed Elkhouly, Yves Baeyens, and Shahriar Shahramian. 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.

[6] Vasileios Mavroeidis, Kamer Vishi, Mateusz D Zych, and Audun Jøsang. The impact of quantum computing on present cryptography. *arXiv preprint arXiv:1804.00200*, 2018.

[7] 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*, pages 1272–1289, 2018.

[8] 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.

[9] 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.

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

[11] 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.

[12] 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.

[13] Zhambyl Shaikhanov, Fahid Hassan, Hichem Guerboukha, Daniel Mittleman, and Edward Knightly. 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*, pages 257–267, 2022.

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

[15] Zhambyl Shaikhanov, Fahid Hassan, Hichem Guerboukha, Daniel Mittleman, and Edward Knightly. Adversarial metasurfaces: Metasurface-in-the-middle attack. In *Proceedings of the 15th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, pages 274–276, 2022.

[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*, pages 13–18, 2022.

[17] Haoze Chen and Yasaman Ghasempour. Malicious mmWave reconfigurable surface: eavesdropping through harmonic steering. In *Proceedings of the 23rd Annual International Workshop on Mobile Computing Systems and Applications*, pages 54–60, 2022.

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

[19] Xiaowei Pang, Min Sheng, Nan Zhao, Jie Tang, Dusit Niyato, and Kai-Kit Wong. When UAV meets IRS: Expanding air-ground networks via passive reflection. *IEEE Wireless Communications*, 28(5):164–170, 2021.

[20] Taniya Shafique, Hina Tabassum, and Ekram Hossain. Optimization of wireless relaying with flexible UAV-borne reflecting surfaces. *IEEE Transactions on Communications*, 69(1):309–325, 2020.