Zhambyl Shaikhanov *University of Maryland, College Park, MD* **Fahid Hassan** *Rice University, Houston, TX*
Sherif Badran *Northeastern University, Boston, MA* **Hichem Guerboukha** *University of Missouri, Kansas City, MO*
Josep Miquel Jornet *Northeastern University, Boston, MA* **Daniel M. Mittleman** *Brown University, Providence, RI*
Edward Knightly *Rice University, Houston, TX*

Editor: Nirupam Roy

METAFLY:
Aerial "MetaSurface-in-The-Middle" Attacks on Wireless Backhaul Links

Transcending the capabilities of traditional architectures, metasurfaces offer near-limitless control over the fundamental electromagnetic properties of wireless signals, presenting new opportunities for wireless communication. However, they also bring forth unprecedented security challenges, particularly for millimeter-wave and sub-THz wireless backhaul links employed for many critical functions, such as financial trading on Wall Street. In this article, we expose a new category of aerial "MetaSurface-in-the-Middle" attacks, wherein an adversary armed with an on-drone metasurface, *MetaFly*, can intercept wireless backhaul links with an almost imperceptible trace. Strikingly, such adversarial metasurfaces can be fabricated in minutes using standard office items like a foil sheet and a laminator. The attack is implemented and experimentally evaluated in both a large indoor atrium and outdoor rooftops in a large metropolitan area, demonstrating the adversary's ability to establish a secondary diffraction beam for eavesdropping while maintaining minimal impact on legitimate communication.

Wireless backhaul links are ubiquitous and widely employed for many critical functions, including low-latency financial trading on Wall Street [1] and 5G base station interconnectivity [2], and can cover distances in the range of kilometers [3]. Wireless backhaul antennas are generally positioned in elevated regions such as towers and rooftops and commonly exploit millimeter-wave and sub-THz frequency bands (30-300 GHz) with large bandwidths for high-date rate and low-latency communication [4, 5]. Because such links employ highly directive beams and are positioned 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, advances in millimeter-wave to sub-terahertz metasurfaces, with their abilities to covertly manipulate the electromagnetic wave-front of the signals, are challenging traditional wireless security principles, necessitating a foundational rethinking.

Indeed, metasurfaces exhibit incredibly diverse and highly customizable electromagnetic properties, even beyond what is available in nature [6]. These engineered structures have been used to enhance wireless communication performance in numerous ways, e.g., relaying signals via transparent metasurfaces embedded in windows [7], mitigating antenna polarization mismatch with wall-integrated metasurfaces [8], and extending signal coverage through metamorphic surfaces on curtains and blinds [9]. Yet adversarial metasurfaces equally enable attackers to artificially control electromagnetic waves artificially, launching sophisticated "MetaSurface-in-the-Middle" attacks and intercepting wireless backhaul links while leaving a minimal attack footprint.

FIGURE 1. Zhambyl Shaikhanov shows a foil sheet he used to create a "metasurface" – a 2D structure that adversaries employ to secretly manipulate electromagnetic wave-fronts and launch acute "metasurface-in-the-middle" attacks on high-frequency transmissions crucial for wireless backhauls and 6G networks.

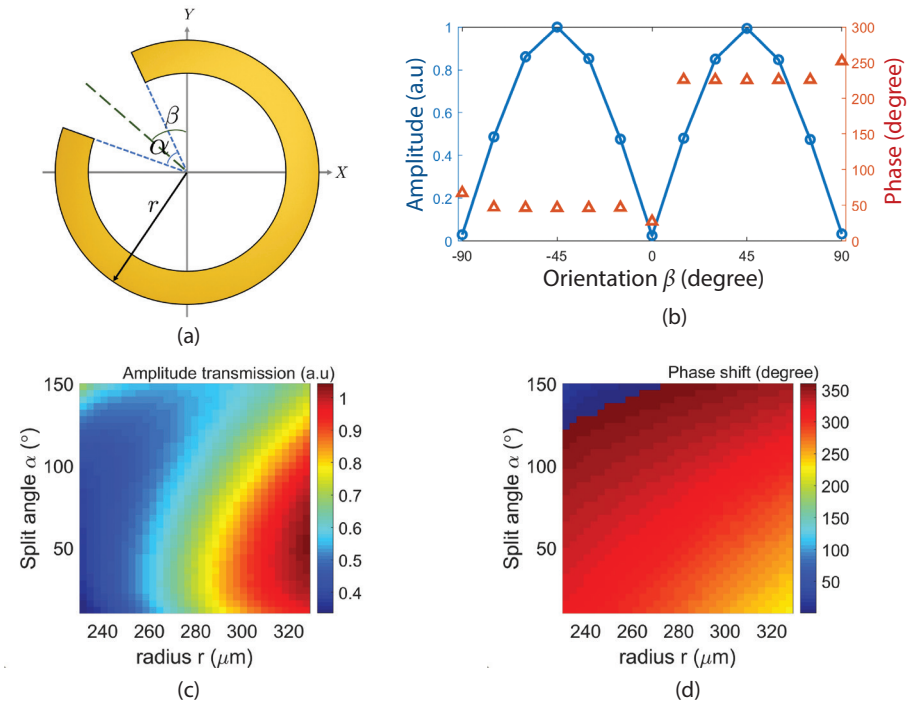

FIGURE 2. Attacker exploits a C-shape meta-atom as a building unit of an adversarial metasurface. (a) is a schematic view of the meta-atom and (b)-(d) are finite element method simulation results demonstrating controllable amplitude and phase responses.

THREAT MODEL AND ATTACKER DESIGN SPACE

A wireless backhaul network is considered 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.

Eve leverages the publicly available Federal Communications Commission (FCC) database [10] 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

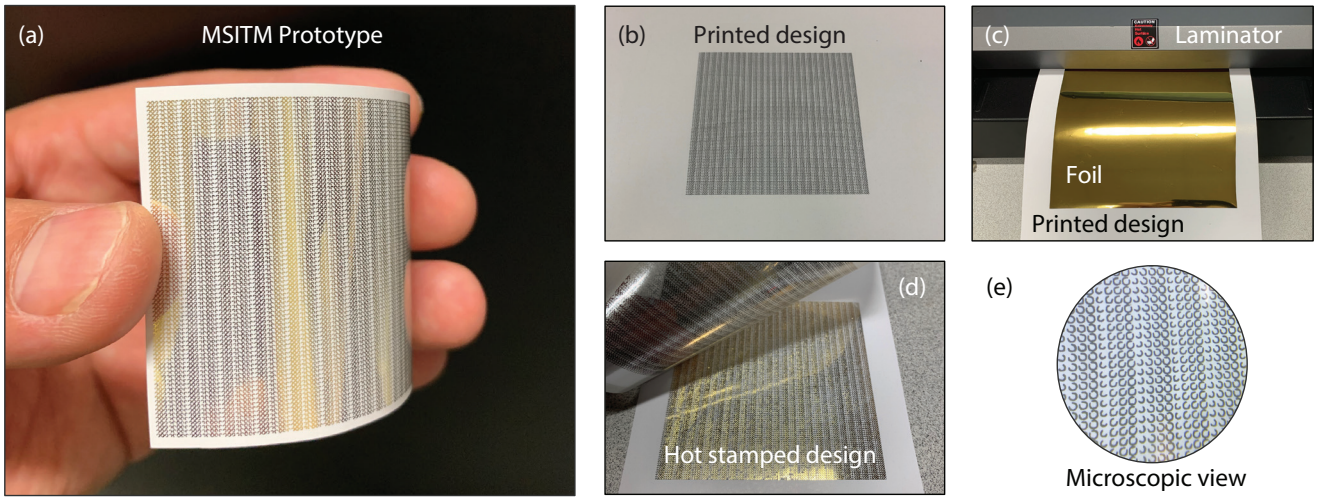

FIGURE 3. (a) is a prototype of the Metasurface-in-the-Middle (MSITM). Eve employs a low-cost and rapid fabrication method that involves (b) printing the designed pattern and (c) passing printed paper patterns along with metallic foil through a laminator. The surface (d) can also be cleaned with tape to remove excessive foil powder, and (e) is a microscopic view of the fabricated metasurface.

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 exploiting the generalized Snell's law in 3D [11], steering it from the metasurface towards her remote position, while letting the Alice-Bob link pass through.

Meta-Atom by Meta-Atom Design

One of the key challenges for Eve is to physically realize the targeted phase profile based on the specified eavesdropping angle discussed. To achieve this, Eve constructs carefully engineered structures – meta-atoms – that enable the controllable manipulation of electromagnetic waves at the sub-wavelength scale. These metallic elements provide a wide range of amplitude and phase responses and can be configured based on their geometrical features. Eve then assembles an array of such unique meta-atoms, forming a supercell, to collectively generate the $\nabla\Phi$ phase profile across spatially periodic structures.

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 [12]. Composed of metallic rings shown in Figure 2, 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. Importantly, the meta-atom geometries, specifically its radius r, slit opening α, and orientation β, enable accurate control over the electromagnetic properties. Eve can obtain the entire 2π phase shift by selectively choosing radius r and opening angle α values as shown in Figure 2. In the design, Eve generates amplitude transmission and phase shift heatmaps, similar to one in Figure 2, and selects 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.

Rapid and Inexpensive Fabrication

Conventionally, complex and costly methods such as photolithography are employed to fabricate metasurfaces. However, an advanced adversary exploits recent inexpensive and rapid fabrication alternatives such as the hot-stamping technique [13]. Specifically, Eve first prints the aerial metasurface design pattern, as shown in Figure 3, using a standard toner printer. She employs mmWave and sub-THz transmissive substrates, such as off-the-shelf glossy paper and transparent plastic sheet, to print the design. Then, she puts an off-the-shelf metallic foil (commonly used for crafting) on top of the printed pattern and passes it through a laminator heated to a temperature of 290°F, as shown in Figure 3. 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. Also, note that 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.

Also, 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 [14, 15]. 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, 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. 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. We fabricate and demonstrate aerial metasurface of letter paper size and only several grams, making it a negligible addition to MetaFly.

METAFLY EXPERIMENTS

We conduct large-scale outdoor experiments and controllable indoor atrium experiments to investigate the impact of different attack factors. As shown in Figure 4, 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 (~ 22°) away from Bob to observe the 130 GHz eavesdropping diffraction beam generated by the aerial metasurface.

In the experiment, Alice transmits modulated data to Bob at 130 GHz carrier frequency using 10 GHz bandwidth, employing an M-QAM modulation scheme. Our experiments include up to 1024-QAM. The QAM frame structure consists of an 18-bit header, followed by 1500 log2 (M) pilot bits and 10000log2(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.

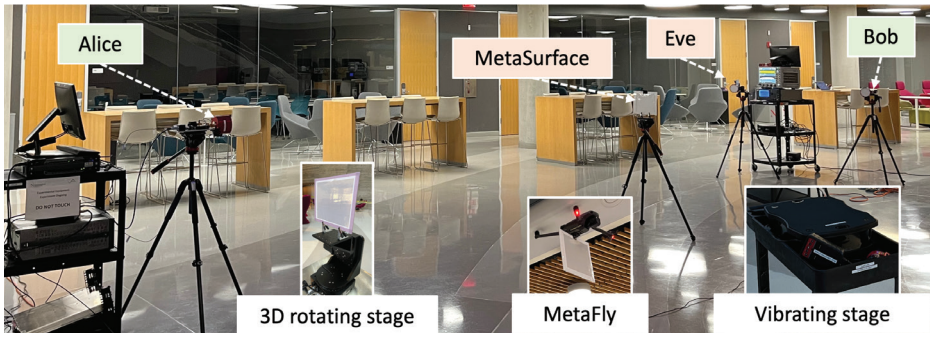

FIGURE 4. Large atrium experimental setup with state-of-the-art sub-THz communication testbed and MetaFly.

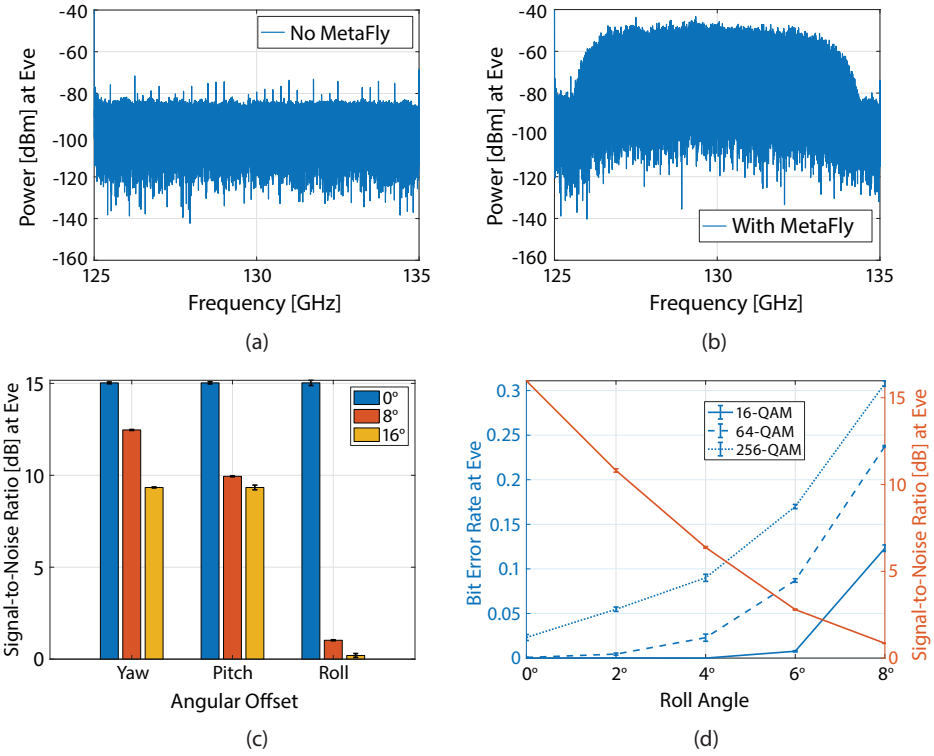

FIGURE 5. Feasibility of the attack, with (a) and (b) without MetaFly. (c) Impact of Eve's metasurface orientation offset on her remote eavesdropping SNR. (d) Effect of metasurface roll offset on Eve's SNR and BER.

Attack Demonstration

We begin by studying the feasibility of the attack, and in Figure 5a-b, we depict Eve's power spectral profile results for two scenarios: one where Eve employs MetaFly in the attack, and one where she does not. Notice the significant difference between the power spectrum in Figure 5a vs. Figure 5b. Specifically, Eve largely receives noise without MetaFly, with the blue curve mostly fluctuating below −80 dBm. 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 Figure 12b. By remote positioning MetaFly and stealthy interception of the link, she induces her targeted abrupt phase changes on the transmission wavefront. As such, she generates an eavesdropping diffracted beam steered toward her antenna.

In general, the effectiveness of the attack is governed by several factors, including the orientation offset of the aerial metasurface, the vibration of the drone, and the positioning of the aerial metasurface relative to Alice and Bob. In fact, Eve aims to orient the aerial 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. In the results in Figure 5c, we show a range of yaw, pitch,

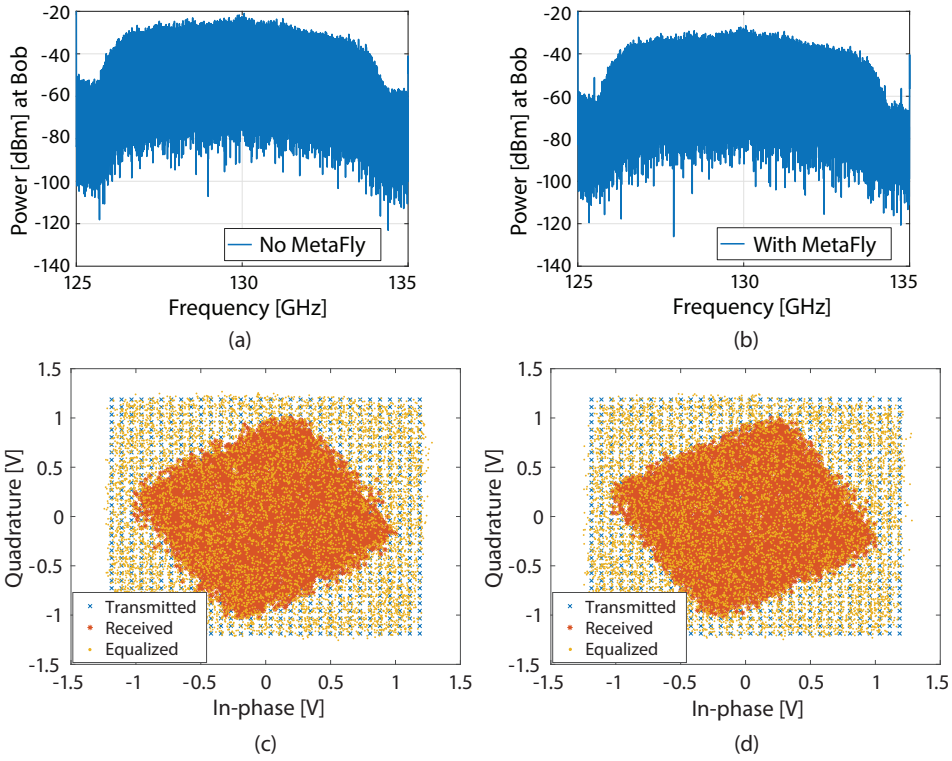

FIGURE 6. Energy footprint of the attack without (a) and with (b) MetaFly, as viewed at Bob. Constellation diagrams without (c) and with (d) MetaFly, as observed at Bob.

and roll offset angles on the x-axis and Eve's corresponding SNR on the y-axis. 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 impact on Eve's observed signal power. Eve is less sensitive to yaw and pitch offsets compared to roll, as roll offsets significantly alter the phase discontinuity response across the x and y axes of the metasurface interface, causing the beam to diffract in a direction other than Eve's location. Ultimately, Eve's BER performance further governed by the Alice's underlying transmission modulation order as depicted in Figure 5d, which Alice will select according to the SNR of the Alice to Bob link.

Impact at Bob

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. Specifically, we investigate the energy footprint of the attack and depict Bob's power spectral profile in two different scenarios, presenting results in Figure 6a-b.

We find 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. Moreover, the results reveal no evident frequency-selective response of the metasurface at Bob, but rather a nearly uniform few dBm power decrease. In fact, wireless backhaul channels can encounter similar channel variations even without MetaFly in between the Alice-Bob link. That is, backhaul infrastructure on towers and buildings is 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. As such, Eve not only establishes an eavesdropping link but also maintains the legitimate link, leaving a minimal energy footprint.

Moreover, prior work has shown that weather conditions such as rain and snow introduce path loss increase at sub-THz

METAFLY CAN INTERCEPT WIRELESS BACKHAUL LINKS WITH AN ALMOST IMPERCEPTIBLE TRACE

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.

To study the effect of the attack at a symbol level, we present the constellation diagrams observed at Bob for both scenarios, with and without MetaFly in between the Alice-Bob link, in Figure 6c-d. Notice that without MetaFly, the raw received constellations are rotated (and shrunk) compared to the transmitted ones. These are mainly the impact of the device and channel effects, such as oscillator phase noise, IQ imbalance, and multipath propagation, among others. Yet, 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 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, making the attack even more challenging to detect for Bob.

ROOFTOP ATTACK DEMONSTRATION

Finally, we realize the attack on outdoor rooftops in a large metropolitan area and explore Eve's ability to intercept the sub-THz

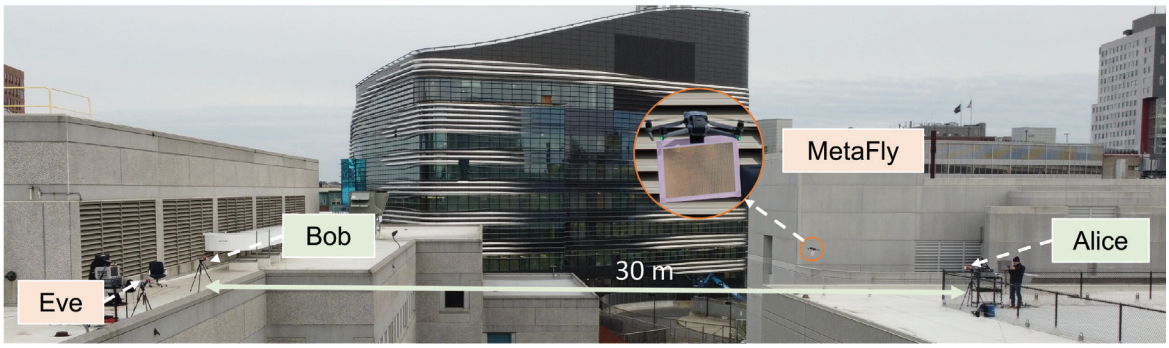

FIGURE 7. Eve armed with MetaFly intercepting a rooftop wireless backhaul link in a large metropolitan area.

transmitter. 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. Since our custom backhaul link is not in the FCC database (thus no publicly available information on antenna locations), we flew MetaFly manually via the remote controller. We conducted the rooftop experiment using the baseline continuous wave case, with Alice sending a sinusoidal tone at 130 GHz with transmit power of 13 dBm before the antenna, and her antenna is aimed directly at Bob as shown in Figure 7.

As depicted in the results of Figure 8, Eve can intercept the transmission with a signal strength more than 40 dB above the baseline at that frequency. The weather during the experiment was moderately windy, with an average wind speed of approximately 10 mph and gusty variations due to turbulence between buildings. Nonetheless, MetaFly provided sufficient flight stability (e.g., avoiding severe detrimental effects from high roll variations) to consistently generate an eavesdropping diffraction beam, allowing Eve to intercept it.

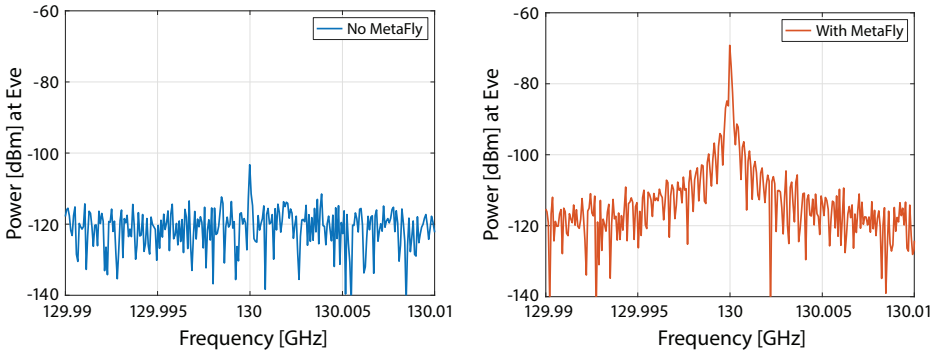

FIGURE 8. Eve intercepting a 130 GHz rooftop wireless backhaul transmitter.

CONCLUSIONS AND THE ROAD AHEAD

In this article, we expose adversarial aerial metasurfaces and demonstrate that wireless backhaul links, such as those used for low-latency financial trading on Wall Street, are highly vulnerable to "Metasurface-in-the-Middle" attacks. We explore attacker design strategies, including a meta-atom-by-atom design approach, and the fabrication of low-cost, lightweight, transmissive, and power-free aerial metasurfaces. We implement and experimentally demonstrate the attack in both indoor atrium and outdoor rooftop environments, showcasing its effectiveness. We also highlight the importance of future research on countermeasures against these fundamental and emerging wavefront manipulation threats, such as continual and rigorous monitoring of the links for any physical alterations, and the development of machine learning algorithms to detect suspicious electromagnetic footprints that could help expose such attacks. ■

Acknowledgment

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.

Zhambyl Shaikhanov is an Assistant Professor of Electrical and Computer Engineering at the University of Maryland, College Park. He received his PhD and MS from Rice University and his BS from the University of Texas at Austin. His research focuses on a broad spectrum of next-generation wireless. He designs, prototypes, and demonstrates in-the-field next-generation wireless systems and architectures with applications in networking, security, and sensing.

Fahid Hassan received his BSc in electrical engineering from Jordan University of Science and Technology, Jordan, in 2020, and his MS in Electrical and Computer Engineering from Rice University, Houston, TX in 2022. He is currently pursuing a PhD in Electrical and Computer Engineering at Rice University. His research interests are the design, implementation and experimental evaluation of next-generation wireless communication systems with focus on THz communications and integration of intelligent surfaces with wireless systems.

Sherif Badran received his BS in Electrical Engineering from Ain Shams University, Cairo, Egypt, in 2021, and his MS degree in electrical and computer engineering from Northeastern University, Boston, MA, in 2023. He is currently pursuing his PhD in Electrical Engineering at Northeastern University. where he also serves as a Graduate Research Assistant in the Department of Electrical and Computer Engineering. His research interests include terahertz communications, wireless communications, and information and coding theory.

Hichem Guerboukha is an Assistant Professor of Electrical and Computer Engineering at the University of Missouri, Kansas City, MO. He earned his PhD in Engineering Physics from Polytechnique Montreal, Canada, in 2019. His research is at the intersection of THz

communications, sensing, and imaging, with a recent emphasis on engineering wavefronts for near-field applications.

Josep Miquel Jornet is a Professor and the Interim Chair of the Department of Electrical and Computer Engineering at Northeastern University, the Associate Director of the Institute for the Wireless Internet of Things at NU, and the director of the Ultrabroadband Nanonetworking (UN) Laboratory. He received his PhD in Electrical and Computer Engineering from the Georgia Institute of Technology, Atlanta, GA, in August 2013. His research interests are in terahertz communication networks and wireless nano-bio-communication.

Daniel M. Mittleman is a Professor of engineering at Brown University. His research interests involve the science and technology of terahertz radiation. He is a Fellow of the OSA, the APS, and the IEEE, and is a 2018 recipient of the Humboldt Research Award. In 2018-2020, he served a three-year term as Chair of the International Society for Infrared Millimeter and Terahertz Waves, and received the Society's Exceptional Service Award in 2022. He is a Mercator Fellow of the Deutsche Forschungsgemeinschaft (DFG), in affiliation with the Meteracom project for the 2023-2025 term.

Edward Knightly is the Sheafor–Lindsay Professor of Electrical and Computer Engineering and Computer Science at Rice University. He received his PhD and MS from the University of California at Berkeley and his BS from Auburn University. He received the IEEE INFOCOM Achievement Award, the Dynamic Spectrum Alliance Award for Research on New Opportunities for Dynamic Spectrum Access, the George R. Brown School of Engineering Teaching + Research Excellence Award, and the National Science Foundation CAREER Award.

REFERENCES

[1] Anova Financial Networks. Low latency financial connectivity. https://anovanetworks.com/

[2] Xiaohu Ge, Hui Cheng, Mohsen Guizani, and Tao Han. 2014. 5G wireless backhaul networks: Challenges and research advances. *IEEE Network*, 28(6):6–1.

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

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

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

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

[7] Daisuke Kitayama, Yuto Hama, Kenta Goto, Kensuke Miyachi, Takeshi Motegi, and Osamu Kagaya. 2021. Transparent dynamic metasurface for a visually unaffected reconfigurable intelligent surface: controlling transmission/reflection and making a window into an rf lens. *Optics Express*, 29(18):29292-29307.

[8] Lili Chen, Wenjun Hu, Kyle Jamieson, Xiaojiang Chen, Dingyi Fang, and Jeremy Gummeson. 2021. Pushing the physical limits of iot devices with programmable metasurfaces. *18th USENIX Symposium on Networked Systems Design and Implementation (NSDI 21)*, 425-438.

[9] R. Ivan Zelaya, Ruichun Ma, and Wenjun Hu. 2021.Towards 6g and beyond: Smarten everything with metamorphic surfaces. *Proceedings of the 20th ACM Workshop on Hot Topics in Networks*, 155-162.

[10] Federal Communications Commission (FCC). Universal licensing system. https://wireless2.fcc.gov/UlsApp/UlsSearch/searchAdvanced.jsp

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

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

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

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

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

[16] Priyangshu Sen, Jacob Hall, Michele Polese, Vitaly Petrov, Duschia Bodet, Francesco Restuccia, Tommaso Melodia, and Josep M. Jornet. 2022. Terahertz communications can work in rain and snow: Impact of adverse weather conditions on channels at 140 GHz. *Proceedings of the 6th ACM Workshop on Millimeter-Wave and Terahertz Networks and Sensing Systems (ACM mmNets)*, 3–18.