OPTICA

Audio misinformation encoding via an on-phone sub-terahertz metasurface

Zhambyl Shaikhanov,[1,*] Mahmoud Al-Madi,[1] Hou-Tong Chen,[2] Chun-Chieh Chang,[2] Sadhvikas Addamane,[3] Daniel M. Mittleman,[4] and Edward W. Knightly[1]

[1]Department of Electrical and Computer Engineering, Rice University, Houston, Texas 77005, USA
[2]Center for Integrated Nanotechnologies, Los Alamos National Laboratory, Los Alamos, New Mexico 87545, USA
[3]Center for Integrated Nanotechnologies, Sandia National Laboratories, Albuquerque, New Mexico 87185, USA
[4]School of Engineering, Brown University, Providence, Rhode Island 02912, USA
*zs16@rice.edu

Received 29 May 2024; revised 25 June 2024; accepted 1 July 2024; published 6 August 2024

We demonstrate a wireless security application to protect the weakest link in phone-to-phone communication, using a terahertz metasurface. To our knowledge, this is the first example of an eavesdropping countermeasure in which the attacker is actively misled.

https://doi.org/10.1364/OPTICA.531175

Active metasurfaces operating in the millimeter-wave and sub-terahertz spectral ranges have become a significant focus of recent research [1], especially with advancements toward 6G wireless systems [2]. Such devices, which are generally configured in an array-of-subarrays architecture, are envisioned as valuable tools for manipulating millimeter-wave or terahertz beams, or for modulation [3] or high-speed wavefront manipulation [4]. In this context, a common goal has been to enhance the switching speed of such devices, first through the use of materials with intrinsically fast response [5] and then by reducing the device area to minimize its RC time constant [6,7]. This latter approach renders free-space coupling challenging due to the small size of the device. However, there are advantages in taking the opposite point of view and exploiting relatively low-speed (∼kHz) operation of a device with a large (∼ cm^2) surface area to unlock fundamentally different capabilities. We report a novel countermeasure against a new and dangerous type of audio eavesdropping attack that is enabled by such a structure, which is unprecedented in the security literature.

With the emergence of low-cost millimeter-wave radar systems in the last few years, a new type of eavesdropping attack has been identified that threatens the security of information discussed during phone conversations [8,9]. An eavesdropper (Eve) can use such radars to remotely and covertly detect the tiny vibrations of a smartphone caused by the motion of the speaker. These vibrations modulate the phase of the radar beam reflected from the phone's case, thus encoding the audio information on the millimeter-wave signal. Specifically, the demodulated signal provides information on the phase change $\Delta\phi$ corresponding to the sound-vibration displacement Δd at time t as

$$\Delta\phi(t) = \frac{4\pi\,\Delta d(t)}{\lambda}, \tag{1}$$

where λ is the wavelength of the radar. By monitoring this phase shift, Eve can track the small vibrations with high resolution. Using a typical inexpensive mmWave radar, a phase change as small as ∼1° can be detected, corresponding to an acoustic-vibration displacement of about 5 μm for a radar frequency of 77 GHz. We point out that this attack targets the physical medium, which cannot be protected by digital encryption, making it very challenging to counter with existing methods.

In this paper, we develop the first countermeasure for this type of attack. Indeed, our approach not only thwarts such attacks but also injects false signatures to fool Eve into believing that she has succeeded. Although there are many eavesdropping protection techniques in the literature, e.g., [10], we report a unique innovation that enables the user to hide his private acoustic signals and simultaneously inject an alternative signal to mislead the attacker, using a sub-terahertz metasurface.

The core of our idea relies on the fact that Alice can counter Eve's radar attack by controllably modifying the phase of Eve's radar signal. Alice proactively introduces dynamic phase changes in the reflected radar signal that are larger than (and significantly different from) the phase change due to the audio vibration. To accomplish this, Alice employs a smartphone-mounted dynamic metasurface—a 2D structure consisting of an array of subwavelength elements with a programmable electromagnetic (EM) response. She can program this device to impose a time-varying phase change on the radar signal, and enable it during sensitive phone conversations. As this time-varying phase is intended to mimic human speech, its spectrum lies in the low kilohertz range. Thus, even a metasurface with a relatively slow (kHz-scale) response can be employed, as long as the range of accessible phase modulation is sufficiently large. We design an experimental testbed realization of this system utilizing a 2.5 cm × 2 cm dynamic metasurface. We employ an off-the-shelf FMCW radar situated 0.5 m from a conventional smartphone, which is oriented to reflect radar signals back to Eve. The radar transmits a chirped signal spanning 77–81 GHz at 10 kHz. The metasurface, located on the exterior surface of the phone, is similar to that described in [10]. Our metasurface is designed for a resonant response over a relatively narrow ∼20 GHz bandwidth centered at a frequency of 150 GHz, but it manifests a phase response over a much broader

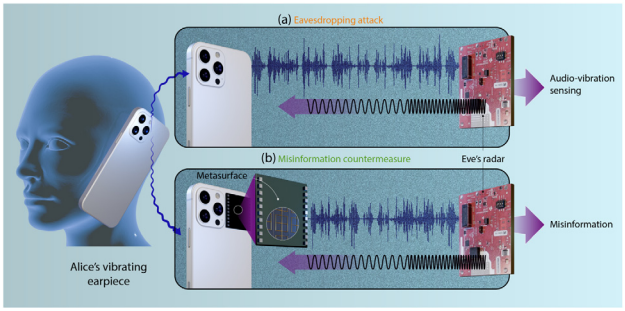

Fig. 1. (a) Eve directs a radar signal towards Alice, who is engaged in phone conversation, to sense micron-scale audio-vibrations and recover audio. (b) Our system dynamically modifies Eve's fundamental sensing observations, introducing targeted false signatures to mislead her.

range [11,12], extending below the frequency band of the radar. By varying the bias applied to the metasurface, we control the phase of the reflected radar signal, thus modifying Eve's observations (see Fig. 1).

To implement this scheme, Alice must program the metasurface using a voltage signal that varies at audio frequencies to create a phase change that mimics an audio-vibration signature. We first conduct experiments to study Eve's observed phase range as Alice switches her smartphone-metasurface at different frequencies. Figure 2(a) shows this measured response, which represents the RC response of the split-ring resonator array. At low frequencies, Alice has a broad range of phase control exceeding 10°, with a 3 dB bandwidth of about 3 kHz. The imposed phase varies nearly linearly within the 0–7.1 V reverse bias control signal range, saturating at higher reverse bias. With this mapping between her control signal $\vec{v}$ and the corresponding phase response ϕ characterized, Alice can generate a targeted vibration pattern to mimic voiced speech. We note that low audio frequencies, typically ranging from about 85 to 255 Hz, contribute to the fundamental pitch of a person's voice and form the basis for perceived tonal quality [13,14]. Alice has extremely fine control over the displacement resolution, down to sub-micrometer, and can accurately reproduce even complex vibrational wave forms while operating at an audio sampling rate.

We experimentally demonstrate our method with a series of exemplary 12 s audio clips from a phone conversation. These are recorded at a 48 kHz sampling rate. The first, Visualization 1, contains sensitive information such as names (James Kelly), bank account details (1, 2, 3, 5, 6, 7), and social security numbers (8, 9, 10). Visualization 2 is the eavesdropper's reconstructed audio using wireless radar signals when the signal from Visualization 1 is played through the phone's speaker, with no counter-measure implemented. An Amazon audio-to-text transcription shows that the eavesdropper can accurately transcribe every single word. However, Visualization 3 is the eavesdropper's reconstructed audio when Alice employs our counter-measure with the goal of scrambling the eavesdropper's observation by superimposing a random signal on top of the eavesdropper's measurement. Consequently, the eavesdropper hears only noise. Next, we apply a control sequence to the metasurface with the signatures of an alternate audio stream Visualization 4 with a similar audio information signal as in Visualization 1, but featuring an altered name (John Wick), bank account details (7, 7, 3, 8, 0, 1), and social security numbers (3, 5, 9). Then, Visualization 5 is the eavesdropper's spoofed observation, in which she reconstructs audio misinformation despite the absence of any mechanical vibrations of the phone,

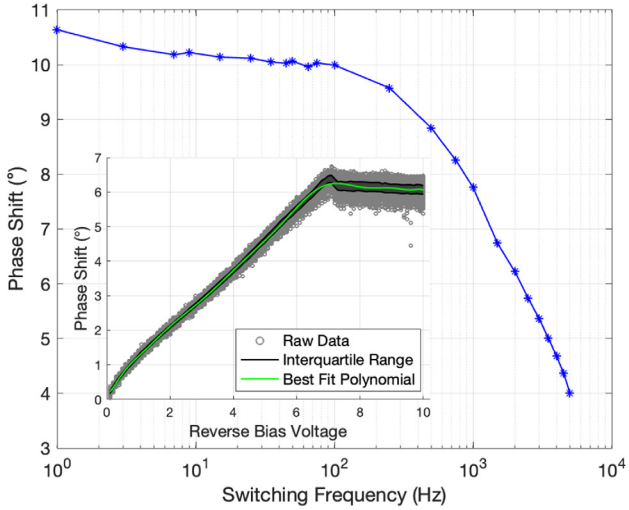

Fig. 2. Measured phase shift response. The on-phone metasurface is placed half a meter away from a radar, directly facing the radar beam. A square-wave signal with a 10 V peak-to-peak and −5 V offset is applied at varying switching frequencies, from 1 Hz to 5 kHz. The inset depicts the control signal versus phase shift mapping.

i.e., the phone speaker is off. Finally, Visualization 6 is Eve's recovered audio with overlaid audio misinformation generated by the metasurface (Visualization 1) *and simultaneously* audio information from the phone speaker (Visualization 4). The eavesdropper detects none of the original words emitted from the speaker, while the injected misinformation is fully reconstructed.

These results validate the idea of using a metasurface for protection against millimeter-wave radar eavesdropping attacks. Moreover, the idea of injecting misinformation into Eve's observation represents a new frontier for secure communications.

Funding. National Science Foundation (1954780, 1955075, 2211616, 2211618, 2148132); Center for Integrated Nanotechnologies (89233218CNA000001).

Disclosures. The authors declare no conflicts of interest.

Data availability. Data are available upon reasonable request.

REFERENCES

1. H. Zeng, S. Gong, L. Wang, *et al.*, Nanophotonics **11**, 415 (2022).
2. J. M. Jornet, E. W. Knightly, and D. M. Mittleman, Nat. Commun. **14**, 841 (2023).
3. Y. Zhang, S. Qiao, S. Liang, *et al.*, Nano Lett. **15**, 3501 (2015).
4. F. Lan, L. Wang, H. Zeng, *et al.*, Light Sci. Appl. **12**, 191 (2023).
5. S. Venkatesh, X. Lu, H. Saeidi, *et al.*, Nat. Electron. **3**, 785 (2020).
6. H.-T. Chen, S. Palit, T. Tyler, *et al.*, Appl. Phys. Lett. **93**, 091117 (2008).
7. Y. Zhang, K. Ding, H. Zeng, *et al.*, Optica **9**, 1268 (2022).
8. C. Wang, F. Lin, T. Liu, *et al.*, in *Proceedings of the 28th Annual International Conference on Mobile Computing and Networking* (2022), pp. 338–351.
9. S. Basak and M. Gowda, in *IEEE Symposium on Security and Privacy (SP)* (2022), pp. 1211–1228.
10. H.-T. Chen, W. J. Padilla, J. M. O. Zide, *et al.*, Nature **444**, 597 (2006).
11. H.-T. Chen, W. J. Padilla, M. J. Cich, *et al.*, Nat. Photonics **3**, 148 (2009).
12. N. Karl, K. Reichel, H.-T. Chen, *et al.*, Appl. Phys. Lett. **104**, 091115 (2014).
13. R. J. Baken, *Clinical Measurement of Speech and Voice*, 2nd ed. (Taylor and Francis Ltd, 2000).
14. J. L. Fitch and A. Holbrook, Arch. Otolaryngol. **92**, 379 (1970).