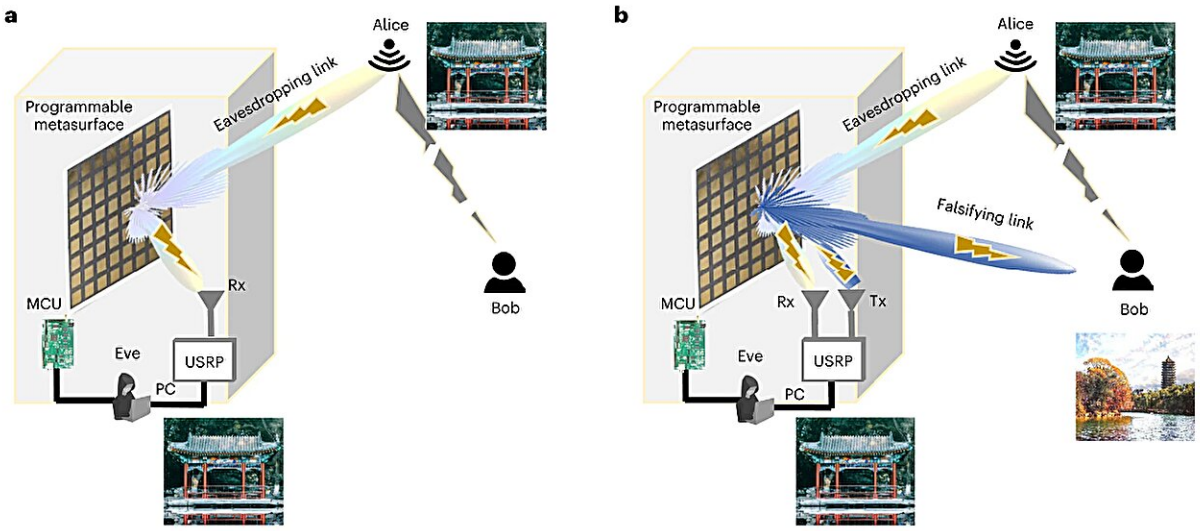
Study highlights the vulnerabilities of metasurface-based wireless communication systems

August 25 2023, by Ingrid Fadelli



Schematics of metasurface-based wireless attacks. (a) Passive mode: Alice aims to wirelessly transmit information to Bob while Eve, an eavesdropper, exploits a programmable metasurface to intercept or disrupt the communication. (b) Active mode: Eve not only eavesdrops but also utilizes the metasurface to transmit deceptive data, falsifying the information received by Bob. Rx: receiver; Tx: transmitter; PC: personal computer; URSP: universal software radio peripheral, MCU: micro control-unit. Credit: *Nature Electronics* (2023). DOI: 10.1038/s41928-023-01011-0

Metasurfaces, artificially engineered surfaces that can manipulate

electromagnetic signals in unique ways, have huge potential for several technological applications, including the implementation of sixth generation (6G) cellular communications. The limitations and vulnerabilities of these smart surfaces, however, are still poorly understood.

Researchers at Peking University, University of Sannio and Southeast University recently carried out a study aimed at better understanding the vulnerability of metasurfaces to wireless cyber-attacks. Their paper, published in *Nature Electronics*, outlines two types of attacks that should be considered and accounted for before metasurfaces can be deployed on a large-scale.

"This work was primarily driven by the need for enhancing security and privacy of wireless communications in the upcoming 6G era, characterized by unprecedented speeds, ultra-low latency, and vast connection nodes," Lianlin Li, Vincenzo Galdi and Tie Jun Cui, three of the researchers who carried out the study, told Tech Xplore.

"The open nature of wireless communication means that data and signals are essentially out in the open, making the risk of physical level attacks a major concern. Our project focuses on identifying some potential risks associated with programmable metasurfaces—a key enabling technology in the envisioned 6G landscape."

Electronics engineers specialized in wireless communications often highlighted the great promise of metasurfaces for the widespread implementation of 6G networks. In a hypothetical future, these carefully engineered surfaces could be easily integrated in everyday objects, for instance on wallpapers or window glasses, to provide these objects with electromagnetic properties and optimize wireless channels.

In their paper, Li and his colleagues set out to explore the possible

shortcomings of these envisioned metasurface-based systems. Their tests and analyses showed that metasurfaces could also be used to carry out malicious attacks on wireless networks that pose serious security threats.

"We have explored two operational modes: passive and active," Li, Galdi and Cui explained. "In the passive mode, we considered a scenario where an attacker (Eve) used a programmable metasurface to eavesdrop on Wi-Fi signals transmitted from a router (Alice) to a legitimate user (Bob). By suitably controlling the metasurface, Eve was able to enhance the power of the eavesdropped signal without consuming additional energy, while causing only a moderate decrease in the communication rate between Alice and Bob."

The researchers closely considered the scenario in which a user passively used a metasurface to eavesdrop on wireless communications between devices and interfere with it. They found that by rapidly switching the properties of a metasurface over time, an attacker could even disrupt the communication between a router (Alice) and a legitimate user (Bob), significantly reducing the speed at which data is transferred over a wireless network.

"In the active mode, on the other hand Eve attempted to eavesdrop on and falsify information transmitted from Alice to Bob," Li, Galdi and Cui said. "By controlling the metasurface, Eve established a falsifying link and actively transmitted deceptive data to Bob. In this case, the metasurface was optimized to maximize the falsifying communication rate while minimizing detectability. The results showed that Eve could successfully eavesdrop on and falsify the data streams, maintaining a low level of detectability."

The tests carried out by this team of researchers show that despite their huge promise for enhancing 6G wireless communications, in their present state metasurfaces could be maliciously used by attackers in both

passive and active ways. Specifically, an attacker could use a metasurface to eavesdrop on confidential communications over a wireless network, while also potentially disrupting the network's functioning or falsifying data transferred between devices.

"Our study has shed light on potential vulnerabilities associated with programmable metasurfaces in future 6G networks," Li, Galdi and Cui said. "It is of crucial importance to uncover such weaknesses during the early stages of a new technology like 6G, since it allows us to proactively develop countermeasures that can safeguard against potential attacks, ensuring that wireless communications remain confidential, intact, and available."

In the future, the results of this recent study could inform the development of new cyber-security solutions that increase the safety of metasurface based wireless networks. This could in turn facilitate the large-scale deployment of metasurfaces to enhance communications and data transfer between electronic devices worldwide.

"Continuing our research, we are dedicated to shaping secure 6G networks, taking into account both the benefits and challenges associated with programmable metasurfaces," Li, Galdi and Cui added. "Currently, we are focused on developing targeted defenses against physical-layer attacks, by exploiting strategies such as beamforming, cooperative jamming with artificial noise, index modulation, and adaptive modulation."

More information: Menglin Wei et al, Metasurface-enabled smart wireless attacks at the physical layer, *Nature Electronics* (2023). DOI: 10.1038/s41928-023-01011-0