Discovery highlights 'critical oversight' in perceived security of wireless networks

June 7 2024, by Marcy de Luna

A research team led by Rice University's Edward Knightly has uncovered an eavesdropping security vulnerability in high-frequency and high-speed wireless backhaul links. Credit: Rice University.

A research team led by Rice University's Edward Knightly has uncovered an eavesdropping security vulnerability in high-frequency and

high-speed wireless backhaul links, widely employed in critical applications such as 5G wireless cell phone signals and low-latency financial trading on Wall Street.

Contrary to the common belief that these links are inherently secure due to their elevated positioning and highly directive millimeter-wave and sub-terahertz "pencil-beams," the team exposed a novel method of interception using a metasurface-equipped drone dubbed MetaFly. Their findings were published as part of the *2024 IEEE Symposium on Security and Privacy (SP)*.

"The implications of our research are far-reaching, potentially affecting a broad spectrum of companies, government agencies and individuals relying on these links," said Knightly, the Sheafor-Lindsay Professor of Electrical and Computer Engineering and professor of computer science. "Importantly, understanding this vulnerability is the first step toward developing robust countermeasures."

Wireless backhaul links, crucial for the backbone of modern communication networks connecting end users to the main networks, have been assumed to be immune from eavesdropping because of their underlying physical and technological barriers.

Knightly and electrical and computer engineering Ph.D. research assistant Zhambyl Shaikhanov, in collaboration with researchers at Brown University and Northeastern University, have demonstrated how a strong adversary can bypass these defenses with alarming ease. By deploying MetaFly, they intercepted high-frequency signals between rooftops in the Boston metropolitan area, leaving almost no trace.

"Our discovery highlights a critical oversight in the perceived security of our wireless backhaul links," Shaikhanov said.

As wireless technology advances into the realms of 5G and beyond, ensuring the security of these networks is paramount. The Rice team's work is a significant step toward understanding sophisticated threats such as MetaFly and also safeguarding the communication infrastructure.

More information: Zhambyl Shaikhanov et al, MetaFly: Wireless Backhaul Interception via Aerial Wavefront Manipulation. *2024 IEEE Symposium on Security and Privacy (SP)* (2024), DOI: 10.1109/SP54263.2024.00151. www.computer.org/csdl/proceedi … 3000a151/1Ub2491z20w

Provided by Rice University