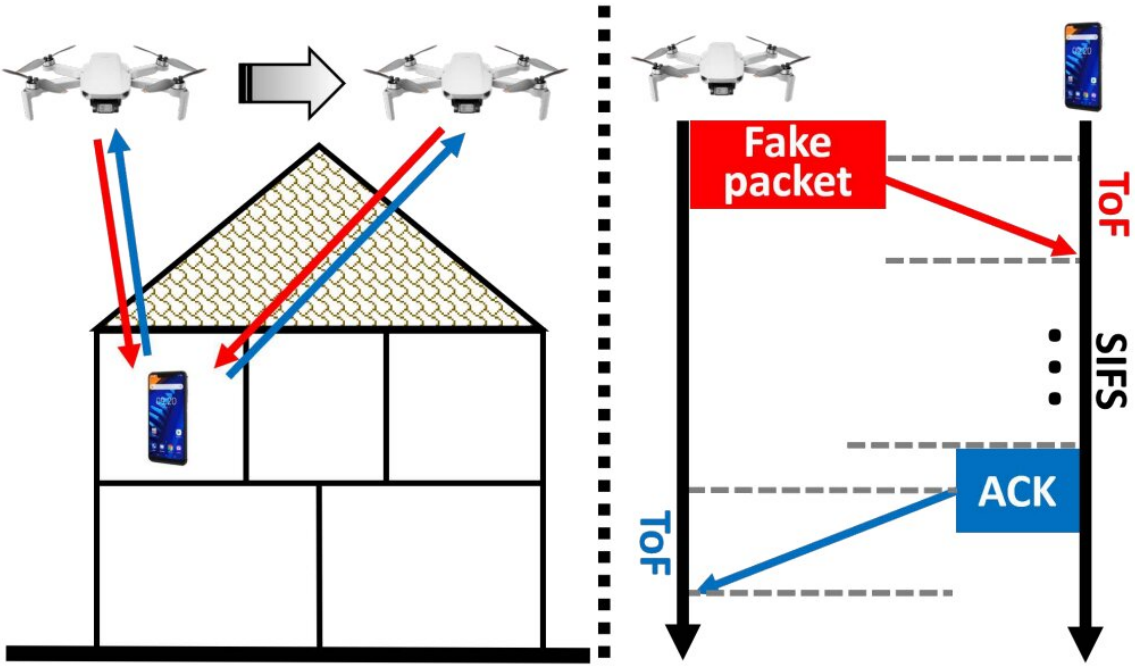
Researchers discover security loophole allowing attackers to use Wi-Fi to see through walls

November 3 2022



Overview of Wi-Peep. Credit: *Proceedings of the 28th Annual International Conference on Mobile Computing And Networking* (2022). DOI: 10.1145/3495243.3560530

A research team based out of the University of Waterloo has developed a drone-powered device that can use Wi-Fi networks to see through

walls.

The device, nicknamed Wi-Peep, can fly near a building and then use the inhabitants' Wi-Fi network to identify and locate all Wi-Fi-enabled devices inside in a matter of seconds.

The Wi-Peep exploits a loophole the researchers call polite Wi-Fi. Even if a network is password protected, smart devices will automatically respond to contact attempts from any device within range. The Wi-Peep sends several messages to a device as it flies and then measures the response time on each, enabling it to identify the device's location to within a meter.

Dr. Ali Abedi, an adjunct professor of computer science at Waterloo, explains the significance of this discovery.

"The Wi-Peep devices are like lights in the visible spectrum, and the walls are like glass," Abedi said. "Using similar technology, one could track the movements of security guards inside a bank by following the location of their phones or smartwatches. Likewise, a thief could identify the location and type of smart devices in a home, including security cameras, laptops, and smart TVs, to find a good candidate for a break-in. In addition, the device's operation via drone means that it can be used quickly and remotely without much chance of the user being detected."

While scientists have explored Wi-Fi security vulnerability in the past using bulky, expensive devices, the Wi-Peep is notable because of its accessibility and ease of transportation. Abedi's team built it using a store-bought drone and $20 of easily purchased hardware.

"As soon as the Polite Wi-Fi loophole was discovered, we realized this kind of attack was possible," Abedi said.

The team built the Wi-Peep to test their theory and quickly realized that anyone with the right expertise could easily create a similar device.

"On a fundamental level, we need to fix the Polite Wi-Fi loophole so that our devices do not respond to strangers," Abedi said. "We hope our work will inform the design of next-generation protocols."

In the meantime, he urges Wi-Fi chip manufacturers to introduce an artificial, randomized variation in device response time, which will make calculations like the ones the Wi-Peep uses wildly inaccurate.

The paper summarizing this research, Non-cooperative Wi-Fi localization & its privacy implications, was presented at the 28th Annual International Conference on Mobile Computing and Networking.

More information: Ali Abedi et al, Non-cooperative wi-fi localization & its privacy implications, *Proceedings of the 28th Annual International Conference on Mobile Computing And Networking* (2022). DOI: 10.1145/3495243.3560530

Provided by University of Waterloo