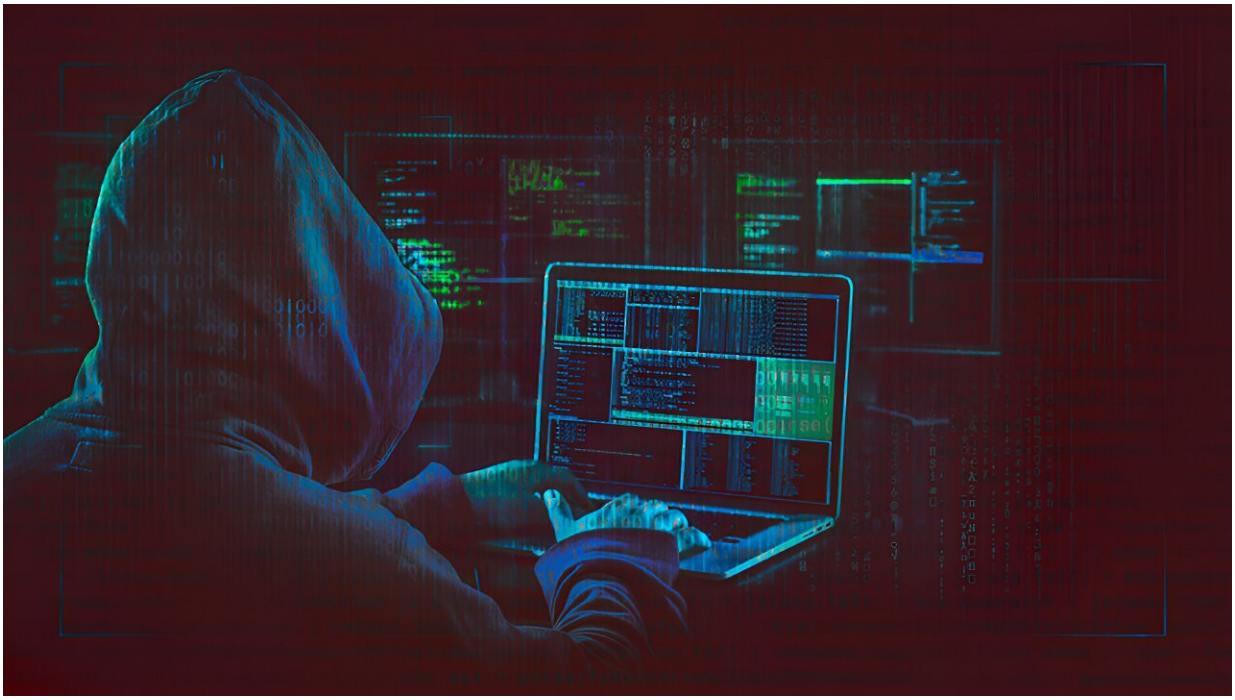
# Research describes new protocol for stopping network interlopers

February 13 2024, by Katie Satterlee



Credit: Texas A&M Engineering

Dr. Santosh Ganji, a recent computer engineering doctoral graduate, and Dr. P.R. Kumar, a professor in the Department of Electrical and Computer Engineering at Texas A&M University College of Engineering, work on the security of wireless networks.

In the wireless world, when two entities communicate, it is difficult to

tell when a man-in-the-middle (MiM) is in between them. Kumar and Ganji have figured out how to flush out MiM through a timing-based protocol called REVEAL that overwhelms the MiM with messages and causes it to fail.

Their work is published on the *arXiv* preprint server. Source code and hardware architecture are available to implement the REVEAL protocol on 4G networks.

"Suppose the base station communicates data or voice to your phone," Kumar said. "Your phone thinks it's connected to the base station, but there may be an interloper in the middle, listening and forwarding messages. This is called a man-in-the-middle attack. The MiM may intercept the message and pass it on."

When a user sends a message or a file, their device transmits packets—a collection of thousands of bits at a time—to the base station over the air, reorders them following communication standards, and presents them to the intended user seamlessly as one video, image or news article.

"For privacy reasons, you want to know if your packets are going through somebody else," Kumar said. "Because packets are encoded, the MiM may be unable to read those packets. But your link is at the mercy of someone who could cut it off anytime, so you're very vulnerable. If there's a man in the middle, you want to discover it."


Software defined radio programmed as a man-in-the-middle. Credit: Texas A&M Engineering

This is a particularly difficult issue because a MiM is basically invisible to the users. When a user sends a packet, it may have reached a MiM who then forwarded it to the base station. The returned reply could also

have been communicated via the MiM. Both transactions may have gone through the MiM without their knowledge.

"The MiM Nodes can have different capabilities: Half-duplex, Full Duplex, and Double Full Duplex. For each of those, we have the capability to flush the MiM out," Kumar said.

"We can detect the presence of an MiM in 4G and 5G cellular networks ," Ganji said.

A MiM may be capable of listening or talking but not simultaneously (Half-duplex), talking and listening at the same time (Full Duplex), or talking and listening to two streams at the same time (Double Full Duplex). The REVEAL protocol challenges and overwhelms the capability of the MiM by carefully timing its packets, causing the MiM to fail.

**More information:** Santosh Ganji et al, Seeing the Unseen: The REVEAL protocol to expose the wireless Man-in-the-Middle, *arXiv* (2023). DOI: 10.48550/arxiv.2308.09213

Provided by Texas A&M University College of Engineering