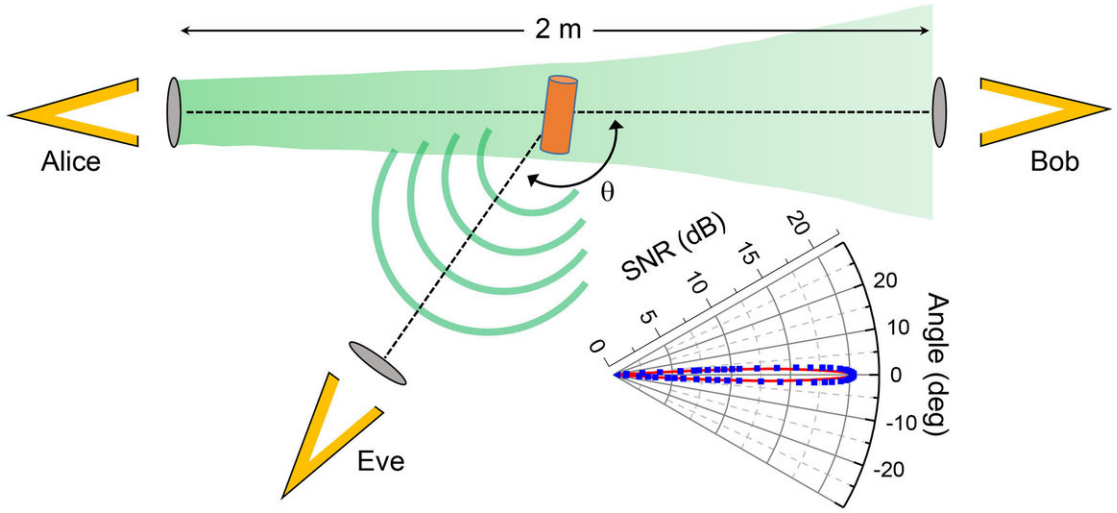
Study exposes security vulnerabilities in terahertz data links

October 15 2018



Terahertz radiation may one day be used in wireless data networks that are many times faster than today's microwave networks. The conventional wisdom in the research community has been that, in addition to greater speed, terahertz data links would also have an inherent immunity to eavesdropping. Unlike microwaves, which travel in wide-angle broadcasts, terahertz waves travel directly from transmitter to receiver in narrow beams. The assumption was that it would be impossible to for an eavesdropper to intercept a terahertz signal without blocking some or all of the beam, which would be easily detected by an

intended receiver. But new research finds that a clever eavesdropper can indeed steal terahertz signals undetected. In order for a link to be reliable, the beam's diameter must be slightly larger than the aperture of the receiver. That leaves a sliver of signal available for an attacker to steal without casting a shadow in a receiver. Credit: Mittleman lab / Brown University

A new study shows that terahertz data links, which may play a role in ultra-high-speed wireless data networks of the future, aren't as immune to eavesdropping as many researchers have assumed. The research, published in the journal *Nature*, shows that it is possible for a clever eavesdropper to intercept a signal from a terahertz transmitter without the intrusion being detected at the receiver.

"The conventional wisdom in the terahertz community has been that it's virtually impossible to spy on a terahertz data link without the attack being noticed," said Daniel Mittleman, a professor in Brown University's School of Engineering and a coauthor of the research. "But we show that undetected eavesdropping in the terahertz realm is easier than most people had assumed and that we need to be thinking about security issues as we think about designing network architectures."

Because of its higher frequency, terahertz radiation can carry up to 100 times more data than the microwaves used in wireless communication today, which makes terahertz an attractive option for use in future wireless networks. Along with enhanced bandwidth, it has also been generally assumed that the way in which high-frequency waves propagate would naturally enhance security. Unlike microwaves, which propagate in wide-angle broadcasts, terahertz waves travel in narrow, very directional beams.

"In microwave communications, an eavesdropper can put an antenna just

about anywhere in the broadcast cone and pick up the signal without interfering with the intended receiver," Mittleman said. "Assuming that the attacker can decode that signal, they can then eavesdrop without being detected. But in terahertz networks, the narrow beams would mean that an eavesdropper would have to place the antenna between the transmitter and receiver. The thought was that there would be no way to do that without blocking some or all of the signal, which would make an eavesdropping attempt easily detectable by the intended receiver."

Mittleman and colleagues from Brown, Rice University and the University at Buffalo set out to test that notion. They set up a direct line-of-site terahertz data link between a transmitter and receiver, and experimented with devices capable of intercepting signal. They were able show several strategies that could steal signal without being detected—even when the data-carrying beam is very directional, with a cone angle of less than 2 degrees (in contrast to microwave transmission, where the angle is often as large as 120 degrees).

One set of strategies involves placing objects at the very edge of a beam that is capable of scattering a tiny portion of the beam. In order for a data link to be reliable, the diameter of the beam must be slightly larger than the aperture of the receiver. That leaves a sliver of signal for an attacker to work with without casting a detectable shadow on the receiver.

The researchers showed that a flat piece of metal could redirect a portion of the beam to a secondary receiver operated by an attacker. The researchers were able to acquire a usable signal at the second receiver with no significant loss of power at the primary receiver.

The team showed an even more flexible approach (from the attacker's perspective) by using a metal cylinder in the beam instead of a flat plate.

"Cylinders have the advantage that they scatter light in all directions, giving an attacker more options in setting up a receiver," said Josep Jornet, an assistant professor of engineering at Buffalo and a study co-author. "And given the physics of terahertz wave propagation, even a very small cylinder can significantly scatter the signal without blocking the line-of-sight path."

The researchers went on to demonstrate another type of attack involving a lossless beam splitter that would also be difficult, if not impossible, to detect. The beam splitter placed in front of a transmitter would enable an attacker to steal just enough to be useful, yet not so much that it would set off alarm bells among network administrators.

The bottom line, the researchers say, is that while there are inherent security enhancements associated with terahertz links in comparison with lower frequencies, these security improvements are still far from foolproof.

"Securing wireless transmission from eavesdroppers has been a challenge since the days of Marconi," said Edward Knightly, professor of electrical and computer engineering at Rice University and a study coauthor. "While terahertz bands take a huge leap in this direction, we unfortunately found that a determined adversary can still be effective in intercepting the signal."

More information: Jianjun Ma et al, Security and eavesdropping in terahertz wireless links, *Nature* (2018). DOI: 10.1038/s41586-018-0609-x

Provided by Brown University