Researchers find way to measure effect of Wi-Fi attacks

September 12 2011

Researchers from North Carolina State University have developed a way to measure how badly a Wi-Fi network would be disrupted by different types of attacks – a valuable tool for developing new security technologies.

"This information can be used to help us design more effective security systems, because it tells us which attacks – and which circumstances – are most harmful to Wi-Fi systems," says Dr. Wenye Wang, an assistant professor of electrical and computer engineering at NC State and co-author of a paper describing the research.

Wi-Fi networks, which allow computer users to access the Internet via radio signals, are commonplace – found everywhere from offices to coffee shops. And, increasingly, Wi-Fi networks are important channels for business communication. As a result, attacks that jam Wi-Fi networks, blocking user access, are not only inconvenient but have significant economic consequences.

Wang and her team examined two generic Wi-Fi attack models. One model represented persistent attacks, where the attack continues non-stop until it can be identified and disabled. The second model represented an intermittent attack, which blocks access on a periodic basis, making it harder to identify and stop. The researchers compared how these attack strategies performed under varying conditions, such as with different numbers of users.

After assessing the performance of the models, the researchers created a metric called an "order gain" to measure the impact of the attack strategies in various scenarios. Order gain compares the probability of an attacker having access to the Wi-Fi network to the probability of a legitimate user having access to the network. For example, if an attacker has an 80 percent chance of accessing the network, and other users have the other 20 percent, the order gain would be 4 – because the attackers odds of having access are 4 to 1.

This metric is important because a Wi-Fi network can only serve once computer at a time, and normally functions by rapidly cycling through multiple requests. Attacks work by giving the attacker greater access to the network, which effectively blocks other users.

"If we want to design effective countermeasures," Wang says, "we have to target the attacks that can cause the most disruption. It's impossible to prevent every conceivable attack." So, one suggestion the researchers have is for countermeasures to focus on continuous attacks that target networks with large numbers of users – because that scenario has the largest order gain. Beyond that, network security professionals can use the new approach to assess a complicated range of potential impacts that vary according to type of attack and number of users.

More information: The paper, "Modeling and Evaluation of Backoff Misbehaving Nodes in CSMA/CA-based Wireless Networks," is forthcoming from *IEEE Transactions on Mobile Computing* and was co-authored by NC State Ph.D. student Zhuo Lu and Dr. Cliff Wang of the U.S. Army Research Office (ARO).

Provided by North Carolina State University