Thwarting attacks on cell phone mesh networks

January 20 2011

A Mobile Ad hoc NETwork (MANET) or cell phone mesh network uses software to transparently hook together numerous active cell phones in a location to provide greater bandwidth and better network connections by allowing users to share "spare" resources while they use their phones, making data transfers faster and smoother.

However, the usefulness of such ad hoc networks can be offset by vulnerabilities. Like any network, a MANET can be susceptible to attack from people with malicious intent. Illicit users might, for instance, hook up to such a network and impersonate a legitimate user in an effort to access data and logins to which they do not have approval, others may implant harmful software, malware. The most worrying form of attack, however, is the distributed denial of service (DDoS), which effectively swamps the network with random data requests until it is overwhelmed. This might simply be for the sake of causing disruption but it a DDoS attack might also be used to hook into security loopholes and quickly and transparently implant malware to harvest logins, bank details and other private information.

Now, Yinghua Guo of the Defence and Systems Institute, at the University of South Australia, in Mawson Lakes and Sylvie Perreau of the Institute for Telecommunications Research, in Mawson Lakes, have developed a computer algorithm that runs on the network and rapidly, within 10-22 seconds, identifies when a DDoS is initiated based on the new, unexpected pattern of data triggered by the attack. The false positive rate is very low and it allows the system to trace the illicit

activity back to the main nodes from which it is originating and to deny them access to the network, so thwarting the attack very quickly.

The researchers say that their technique can halt 80% of the DDoS attack traffic and so allow users to continue using their devices almost as normal and to block the window of opportunity through malware might be implanted during such an attack. More importantly, from a computer science point of view is that the study provides a model framework on which better security systems might be built for MANETs and other networks.

More information: "Detect DDoS flooding attacks in mobile ad hoc networks" in *Int. J. Security and Networks*, 2010, 5, 259-269

Provided by Inderscience Publishers