Validating reliability of OMNeT++ in wireless networks DoS attacks: simulation vs. testbed.

ABSTRACT

Despite current 802.11i security protocol, wireless net- works are vulnerable to Denial of Service (DoS) attacks. Sending a continuous stream of forgery control frames by an attacker can easily flood wireless channel so that the network cannot be available for its associated users. These attacks are possible because wireless control frames do not carry any cryptographic mechanism to detect and discard forgery frames. In this research in parallel to our experiments, we develop an extension module for wireless DoS attacks using OMNeT ++ to assess the reliability of this simulation tool in compare to our real 802.11 wireless network testbed. To fulfill these goals, throughput, end- to-end delay, and pocket lost ratio are considered as our performance measures running on both real testbed and simulation model. The results are used as a comparative acceptance of the simulation environment. Hereby we can confirm accuracy of the simulation results and OMNeT ++ in wireless DoS attack domain

Keyword: Dos attack simulation; OMNeT++; Wireless DoS attack; Wireless security; 802.11 networks.