ABSTRACT

The development of increasingly fast and large internet networks has encouraged an increase in the use of *Wireless* Local Area Network (WLAN) networks as a gateway for device endpoints to access internet networks. WLAN has the advantage of having high data transfer speeds, practical use, and flexibility because it uses radio wave transmission media to connect with users. However, because packet transmission is carried out openly, making WLAN networks more vulnerable to data theft and attack by cybers.

To secure the WLAN network, there is a security system that is qualified, namely the *Wireless* Intrusion Detection System (WIDS). WIDS has the same principles as IDS but is specifically intended to protect WLAN networks from attacks. So that WIDS is suitable to be installed on a WLAN network because it can detect attacks in the air so the network admin can take action before the attack damages important components, namely the server, access point, and client.

In this final project, the WIDS security system will be installed on a WLAN network that is run using the Mininet-Wifi emulator. Systems that have been made are tested using attacks specifically intended for WLAN networks (WEP, WPA, WPA2 Cracking; Denial of Service; and Evil-Twin) and QoS performance is tested before and after WIDS is installed and when run with video and VoIP traffic with backround traffic of 10 Mbps to 58 Mbps. The result is that the system can detect WEP, WPA, and WPA2 Cracking attacks; and Denial of Service but cannot determine the source of the attack correctly (false positive). Evil-Twin attacks can be detected properly by the system. From the performance test, it was found that the WIDS installation results only affected the increase in average delay. Likewise, with different background traffic conditions there is only a linear increase in average delay. For jitter throughput, and packet loss tend to be stable from the results of two performance tests performed.

Keywords : WLAN, WIDS, *access point*.