ABSTRACT

Wireless Local Area Network (WLAN) is a network that commonly used for variant places and purposes. One of factor that makes WLAN used generally is it's simplicity when accessing it. WLAN can be use to accessing the internet for public places like airport, university, mall, and other public places. Unfortunately it's access simplicity create vulnerability. Vulnerability exposed such as DOS, password cracking, WPS cracking, and one of them is evil twin[1][2][3]. This issues must be awared by user regarding the risk that exist in WLAN. Based on this issues, design for detection method for detecting WLAN exploit used in general in client side is needed especially for new WLAN the client encounter. Two WLAN attack that can be easily be launch is deauthentication attack and evil twin attack.

In attempt to mitigating WLAN attack detection, Intrusion Detection System (IDS) must be implemented for detecting the attack in the network. This mitigation detecting deauthentication attack and evil twin attack in client side evin in new enviroment. Method detection used to detecting deauthentication attack is packet threshold method and method detection used for detecting evil twin is by inspecting the network with ICMP protocol.

Based on this research, evil twin attack with signal strength 29,35 dBm around signal strength legitimate access point 56,5 dBm and 52,8 dBm has successfully detected by our designed WIDS. Meanwhile, deauthentication attack consist of two, four, ten, and twenty packets successfully detected too by our designed WIDS.

keyword: evil twin, deauthentication attack, ICMP, security