International J. of Engg. Research & Indu. Appls. (IJERIA).
ISSN 0974-1518, Vol.4, No. III (August 2011), pp 309-318

DETECTION OF ILLEGAL ACCESS POINTS USING FILTERS AND NETWORK ATTACKS USING SIGNATURES FOR PROVIDIG SECURITY IN WLAN

SNEHAL S. BEHEDE, SANDEEP B. VANJALE AND P. B. MANE

Abstract

Rough access point on enterprise network poses serious security threat. One of the most important parts in network security which concerns with network administrators is the presence of rogue access points. Rogue access points, if undetected, can be an open door to sensitive information on the network. Many hackers have taken advantage of the undetected rogue access points in enterprises to not only get free Internet access, but also to view confidential information. Furthermore, rogue APs may interfere with nearby well-planned APs and lead to performance problems inside the network. They potentially open up the network to unauthorized parties, who may utilize the resources of the network, steal sensitive information or even launch attacks to the network. This has forced the issue to develop systems that will not only detect the unauthorized access points but also detect network attacks performed by authorized or unauthorized access points so that it protects data from external misuse. Due to the these security and performance threats, this research study attempts to present novel approach towards detecting unauthorized access points as well as detecting network attacks performed by either authorized or unauthorized access points. It is possible to detect unauthorized access points using various filters and detecting network attacks using digital signatures which are created from known signature.

Keywords : Wireless network security, Rogue Access Point, Network attacks.