International Journal of Computer Science Engineering and Information Technology Research (IJCSEITR)
ISSN(P): 2249-6831; ISSN(E): 2249-7943
Vol. 4, Issue 1, Feb 2014, 35-42

A NOVEL APPROACH FOR FAKE ACCESS POINT DETECTION AND PREVENTION IN WIRELESS NETWORK

SANDIP S. THITE[1], SANDEEP VANJALE[2] & P. B. MANE[3]

[1,2]Department of Computer, BVDUCOE, Pune, Maharastra, India

[3]Department. of Electronics, AISSMS, Pune Maharastra, India

ABSTRACT

Currently many organizations utilize the wireless LAN to provide the access channel to the Internet and Intranet enabling the flexible workforce. While doing so, communications with the Internet is continuously maintained. The growing acceptance of wireless network causes a risk of wireless security attack. However the wireless security is always a primary concern. So for securing data in WLAN it is necessary to detect unauthorized access points which are installed without explicit authorization from a local network management. Rogue APs 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. In network attacks, the hackers try to break the security of the network, by affecting host and then proceeding towards further damage. Due to the above security and performance threats, detecting unauthorized APs as well as detecting attacks performed by unauthorized or authorized AP'S is one of the most important tasks for a network manager.

KEYWORDS: Wireless Security, Fake Access Point, RSSI, 802.11