Abstract

Denial of Service (DoS) attack is a major problem prevalent in Wireless Local Area Network (WLAN). Many security techniques were introduced to prevent the DoS attacks in WLAN. However, there are still many weaknesses which provide interest and way for hackers to do such attacks. This research mainly deals with the two types of DoS attacks, namely
EAPOL (Extensible Authentication Protocol over LAN) start and EAPOL logoff frame over Access Point (AP) and wireless client. The experimental test bed is taken and the solutions are simulated using NS-2, a Linux based simulator, to analyze how far it prevents the DoS attacks in WLAN. The Central Manager (CM) along with Intruder Database (IDB) is proposed to defend the two different types of attacks targeted on Access Point and Client. The CM and IDB can be combined together and called as Integrated Central Manager (ICM). It acts as an Authenticated Server (AS) which manages the communication between the client and the Access Point. The proposed solution increases the throughput. When there is a chance of the failure of the ICM, maintaining a duplicate ICM is proposed which secure the client and Access Point from the attacks.

Reference

- Mina Malekzadeh, Abdul Azim Abdul Ghani, Shamala Subramaniam, and Jalil Desa, “Emprical Analysis of Virtual Carrier Sense Flooding Attacks Over Wireless Local Area
Inhibition of Denial of Service Attack in WLAN using the Integrated Central Manager

- Tuttorial for the Netwrok Simulator "ns", available at http://www.isi.edu/nsnam/ns/tutorial/