# DOS ATTACKS IN INTRUSION DETECTION AND INHIBITION TECHNOLOGY FOR WIRELESS COMPUTER NETWORK

**Dr. Sanjeev Dhull**
Associate Professor, RPIIT Karnal, Dept of Computer Science

**ABSTRACT**

The DoS attack is the most popular attack in the network security with the development of network and internet. In this paper, the DoS attack principle is discussed and some DoS attack methods are deeply analyzed. The DoS attack detection technologies which include network traffic detection and packet content detection are presented. The DDoS based on DoS is introduced and some DDoS tools are described and the important TCP flood DoS attack theory is discussed. The DoS attack program and a DoS attack detection program based on Winpcap for experiment are designed and the network packet generation and capture are implemented. The experiment expressed the key progress of DoS attack and detection in detail. Wireless networking technologies are increasingly penetrating into everyday life [1, 2]. A wireless LAN (Local Area Network) is a type of local-area network that uses high-frequency radio waves rather than wires to communicate between nodes. Today, wireless LANs introduce the concept of complete mobility; communication is no longer limited to the infrastructure of wires. This provides new opportunities and challenges such as security. Security techniques in Wireless computer networks have been increasingly needed. There are many basic risks associated with the WLAN such as insertion attacks, interception and unauthorized monitoring of wireless traffic, jamming, and denial of service [3]. There are many security techniques that already exist such as WEB, Virtual Private Networking (VPN), 802.1X, the Extensible Authentication Protocol

(EAP) and Remote Authentication Dial In User Service (RADIUS). These security techniques tried to solve the security bugs in WLAN. However, there are still some problems in the security that are not solved yet [4, 5, 6, 7]. In this work, we will concentrate on one of these problems that is the Denial Of Service (DOS) attack. Potential DOS attacks are a significant risk for any application where loss of wireless LAN access affects life, profits or reputation. For example, when the network is used for public use in the hot spots for surfing the Internet, the DOS will decrease the profit of the firm that provides the service. DOS attacks can be single or distributed [8, 9]. A WLAN that uses IEEE 802.11i protocol are the most likely candidate protocol to become widely prevalent in cooperate environment. Its low cost of entry is what makes it so attractive. However, inexpensive equipment also makes it easier for attackers to mount an attack.

## INTRODUCTION

The term **Denial of Service (DoS)** refers to a form of attacking computer systems over a network. DoS is normally a malicious attempt to render a networked system unusable (though often without permanently damaging it).

Security is one of the most important issues to be considered in the Wireless Local Area Networks (WLANs). There are many weakness points of security in WLANs due its nature. Many security techniques were introduced to solve the available security bugs. However, there are still many bugs that were not solved yet such as Denial Of Service (DOS) attacks. In this paper, a new security technique is proposed that aims to detect the DOS attacks in WLANs and further prevent the detected attackers, in the future, from accessing the network. The proposed technique uses an intruders' database (IDB), which it creates and modifies each

time an intruder is detected. This database will be used by the technique to inhibit intruders from bringing the network down by a DOS attack. The simulation results of the proposed technique measure the Probability of Denied Service (PDS) with respect to the number of attacks and the maximum number of connections that access point allows. These results show the effectiveness of this technique in securing the WLAN against the DOS attacks.

Denial of service relies on methods that exploit the weaknesses of network technology. For example, one common form of DoS is Ping of Death. Ping of Death attacks work by generating and sending certain kinds of network messages that are technically unsupported but known to cause problems for systems that receive them. Denial of service attacks like Ping of Death may crash or "hang" computers. Other DoS attacks may simply fill or "flood" a network with useless data traffic, rendering systems incapable of acting on bona fide requests.

DoS attacks are most common against Web sites that provide controversial information or services. The commercial cost of such attacks can be very large. DoS may also occur unintentionally when developing or upgrading network systems.

**1. Signaling DOS**

This attack leverages active mobile sessions in the network. It involves sending small amounts of data to re-initiate a session after it has been released. The low-volume attack can create congestion at the radio network controller (RNC).

Overload of the RNC results in a denial of service for the subscriber.

### 2. Battery Drain

This attack also leverages active mobile sessions in the network. It sends packets to a mobile device to prevent the device from going into sleep mode. The attack can involve as little as sending 40 bytes every 10 seconds. This attack wastes radio resources and drains mobile batteries.

### 3. Peer-to-Peer Applications

Bell Labs found that one subscriber's excessive use of peer-to-peer Web sites was affecting the performance of a North American carrier's 3G network. The subscriber uploaded 1GB and downloaded 3.5GB communicating with 5,000 eDonkey and 37,000 Gnutella sites.

### 4. Malfunctioning Air Card

The same North American 3G carrier experienced DOS overloads due to a malfunctioning air card. Bell Labs says it took several man-months of effort to identify the rogue device.

### Ad-hoc networks

Ad-hoc networks can pose a security threat. Ad-hoc networks are defined as peer-to-peer networks between wireless computers that do not have an access point in between them. While these types of networks usually have little protection, encryption methods can be used to provide security.

The security hole provided by Ad-hoc networking is not the Ad-hoc network itself

but the bridge it provides into other networks, usually in the corporate

environment, and the unfortunate default settings in most versions of Microsoft Windows to have this feature turned on unless explicitly disabled. Thus the user may not even know they have an unsecured Ad-hoc network in operation on their computer. If they are also using a wired or wireless infrastructure network at the same time, they are providing a bridge to the secured organizational network through the unsecured Ad-hoc connection. Bridging is in two forms. A direct bridge, which requires the user actually configure a bridge between the two connections and is thus unlikely to be initiated unless explicitly desired, and an indirect bridge which is the shared resources on the user computer. The indirect bridge provides two security hazards. The first is that critical organizational data obtained via the secured network may be on the user's end node computer drive and thus exposed to discovery via the unsecured Ad-hoc network. The second is that a computer virus or otherwise undesirable code may be placed on the user's computer via the unsecured Ad-hoc connection and thus has a route to the organizational secured network. In this case, the person placing the malicious code need not "crack" the passwords to the organizational network, the legitimate user has provided access via a normal and routine log-in. The malfactor simply needs to place the malicious code on the unsuspecting user's end node system via the open (unsecured) Ad-hoc networks.

**Denial of service**

A Denial-of-Service attack (DoS) occurs when an attacker continually bombards a targeted AP (Access Point) or network with bogus requests, premature successful connection messages, failure messages, and/or other commands. These cause legitimate users to not be able to get on the network and may even cause the

network to crash. These attacks rely on the abuse of protocols such as the Extensible Authentication Protocol (EAP).

The DoS attack in itself does little to expose organizational data to a malicious attacker, since the interruption of the network prevents the flow of data and actually indirectly protects data by preventing it from being transmitted. The usual reason for performing a DoS attack is to observe the recovery of the wireless network, during which all of the initial handshake codes are re-transmitted by all devices, providing an opportunity for the malicious attacker to record these codes and use various "cracking" tools to analyze security weaknesses and exploit them to gain unauthorized access to the system. This works best on weakly encrypted systems such as WEP, where there are a number of tools available which can launch a dictionary style attack of "possibly accepted" security keys based on the "model" security key captured during the network recovery.

**Implementing network encryption**

In order to implement 802.11i, one must first make sure both that the router/access point(s), as well as all client devices are indeed equipped to support the network encryption. If this is done, a server such as RADIUS, ADS, NDS, or LDAP needs to be integrated. This server can be a computer on the local network, an access point / router with integrated authentication server, or a remote server. AP's/routers with integrated authentication servers are often very expensive and specifically an option for commercial usage like hot spots. Hosted 802.1X servers via the Internet require a monthly fee; running a private server is free yet has the disadvantage that one must set it up and that the server needs to be on continuously [25]

To set up a server, server and client software must be installed. Server software required is a enterprise authentication server such as RADIUS, ADS, NDS, or LDAP. The required software can be picked from various suppliers as Microsoft, Cisco, Funk Software, Meetinghouse Data, and from some open-source projects. Software includes:

- Cisco Secure Access Control Software
- Microsoft Internet Authentication Service
- Meetinghouse Data EAGIS
- Funk Software Steel Belted RADIUS (**Odyssey**)
- freeRADIUS (open-source)

## REFERENCES

1. "Fitting the WLAN Security pieces together". pcworld.com. http://www.pcworld.com/businesscenter/article/144647/guide_to_wireless_lan_security.html. Retrieved 2008-10-30.
2. "Network Security Tips". *Cisco*. http://www.linksysbycisco.com/EU/en/learningcenter/HowtoSecureYourNetwork. Retrieved 2011-04-19.
3. "The Hidden Downside Of Wireless Networking". http://www.districtadministration.com/viewarticle.aspx?articleid=207. Retrieved 2010-10-28.
4. "How to: Define Wireless Network Security Policies". http://www.wireless-nets.com/resources/tutorials/define_wireless_security_policies.html.

Retrieved 2008-10-09.

5. "Wireless Security Primer (Part II)". windowsecurity.com. http://www.windowsecurity.com/articles/Wireless_Security_Primer_Part_II.html. Retrieved 2008-04-27.

6. "Top reasons why corporate WiFi clients connect to unauthorized networks". InfoSecurity. http://www.infosecurity-us.com/view/7410/comment-top-reasons-why-corporate-wifi-clients-connect-to-unauthorized-networks-/. Retrieved 2010-03-22.