CHAPTER-3:
TOOLS AND METHODS

3.1 NETOWORK SIMULATORS

There are various network simulators available for networking simulation.

The general process of creating a simulation can be divided into several steps [119]:

1. Topology definition: to ease the creation of basic facilities and define their interrelationships, ns-3 has a system of containers and helpers that facilitates this process.

2. Model development: models are added to simulation (for example, UDP, IPv4, point-to-point devices and links, applications); most of the time this is done using helpers.

3. Node and link configuration: models set their default values (for example, the size of packets sent by an application or MTU of a point-to-point link); most of the time this is done using the attribute system.

4. Execution: simulation facilities generate events, data requested by the user is logged.

5. Performance analysis: after the simulation is finished and data is available as a time-stamped event trace. This data can then be statistically analysed with tools like R to draw conclusions.

6. Graphical Visualization: raw or processed data collected in a simulation can be graphed using tools like Gnuplot, matplotlib or XGRAPH.

-- 55 --
3.1.1 Network simulator-2

Network simulator-2 is a name for series of discrete event network simulators, primarily used in Research and teaching. NS2 is free software, publicly available under the GNU GPLv2 license for research, development and use. NS2 is a discrete event simulator targeted at networking research[67]. NS2 provides substantial support for simulation of TCP, routing, and multicast protocols over wired and wireless networks.

3.1.2 GloMoSim

Global Mobile Information System Simulator (GloMoSim) is a network protocol simulation software that simulates wireless and wired network systems[139]. GloMoSim is designed using the parallel discrete event simulation capability provided by Parsec, a parallel programming language. GloMoSim currently supports protocols for a purely wireless network. It uses the Parsec compiler to compile the simulation protocols. Parsec is a C-based simulation language, developed by the Parallel Computing Laboratory at UCLA, for sequential and parallel execution of discrete-event simulation models.

3.1.3. OPENET Technologies

OPNET Technologies is a software business organization that provides performance analysis for computer networks and applications[129]. OPNET is leader in the modeling, simulation, and analysis of strategic and tactical defense communications networks and net-centric applications. OPNET provides simulator for an in-depth understanding of networking technologies and protocols (e.g., IP, IPv6, HAIPE, LTE, MANET, MPLS, QoS, VoIP, and VPN, etc.), optimization techniques, and best practice methodologies in constructive modeling. OPNET IT Guru Academic Edition is a utility designed with educational purposes in mind, specifically to help
users be introduced to the domain of networking. By the use of OPNET IT Guru Academic Edition a simulation test bed scenario is created for WLAN. In which a typical scenario of WLAN is developed in which different nodes are considered connecting through an access points. A WLAN includes a leased line or wired internet at the back, the same is connected to the server through router and various access points are connected through different switches. These access points are points where WLAN users log-on to connect the nets.

3.1.4 NS2 Simulation Model

NS2 is used for Simulation of Model for

a) Different Network Evaluation

b) Wired Vs. Wireless effectiveness

c) Secure Routing and Degraded Performance Metrics

d) Performance of WLAN- Increased and better throughput.

3.2 Scanner Tools

There are several tools by which one can come to know the physical address of any node in the network[128]. These IP Scanner is a free, fast and easy-to-use network scanner. IP Scanner is able to locate all the computers on wired or wireless local network and conduct a scan of their ports. It can detect all the IP addresses on any Wi-Fi network. Even advanced IP Scanner, can wake up and shut down remote groups of Windows machines. The list is as follows:

3.2.1 Advanced IP Scanner 2.2.224,

3.2.2 Colasoft MAC Scanner Pro 2.2,

3.2.3 Angry IP Scanner 2.x, IPScan-II.

The tool which has been used for scanning the network is free open source Angry IP scanner.
It is a very fast IP address and port scanner. It can scan IP addresses in any range as well as any their ports. It is cross-platform and lightweight. Angry IP scanner simply pings each IP address to check if it is alive, then optionally it is resolving its hostname, determines the MAC address, scans ports, etc. It also has additional features, like NetBIOS information (computer name, workgroup name, and currently logged in Windows user), favorite IP address ranges, web server detection, customizable openers, etc. There are currently two different versions available: New cross-platform version, 3.x - still in beta, Old Windows-only version, 2.x. which can be used for scanning purpose.

3.3 MAC Address Spoofer/changer

3.3.1 SMAC

SMAC is a powerful MAC Address Spoofer for Windows 7, VISTA, 2008, 2003, XP, 2000 systems. SMAC is developed by Certified Professionals (CISSP, CISA, CIPP, and MCSE) SMAC capabilities are : 1. Automatically Activate new MAC Address right after changing it. 2. Show the manufacturer of the MAC Address. 3. Randomly generate any New MAC Address or based on a selected manufacturer. 4. Pre-load MAC Addresses List and choose the new MAC address from the list.
3.3.2. TMAC

Technium MAC Address Changer or TMAC can change (spoof) Media Access Control (MAC) Address of Network Interface Card (NIC) or Wireless Network Card (Wi-Fi), irrespective of the drivers of NICs or its manufacturer[10]. It has many new features which can to change IP Address, Gateway, DNS Servers, IPv6 support, enable/disable DHCP in one click, network configuration presets and also many other features.
3.3.3 Register Editor of Window

Registry of Editor of window can also be used to change the MAC Address of Node.

3.4 WEP AND WPA-PSK KEY CRACKER

3.4.1 WEP Cracker

A Bootable DVD of Backtrack which contains various utilities used for cracking, Wireless card and the WEP network which needs to be active. Aircrack-ng is an 802.11 WEP and WPA-PSK keys cracking program that can recover keys once enough data packets have been captured. It implements the standard FMS attack along with some optimizations like KoreK attacks, as well as the all-new PTW attack, thus making the attack much faster compared to other WEP cracking tools.
3.4.2 WPA2 Analysis

Wireless LAN deployments should be made as secure as possible. Many network security threats today are spread over the Internet. The responsibility of network administer is to provide network resources to the legitimate and authorized users and at the same is to protect it from illegitimate and misuse by unauthorized, immoral unlawful clients and cyber criminals and also to find the solution for the other security threats such as Phishing, malware and malicious code. The Network resources are made available by way of authentication and authorization of users. The protection against illegal and misuse of network is taken place by applying some RSNA and WPA2 Methods.

3.5 OTHER SECURITY TOOLS

3.5.1 windows Firewall, Windows Defender, Smart Screen Filter, InPrivate filtering and activex Control

The organization must use latest software and hardware for network securities and APs with a built-in firewall. On the other hand, some security features such as windows Firewall, Windows Defender, Smart Screen Filter, InPrivate filtering and activex Control can also be used at the connecting nodes in order to solve the
problem of misuse of network. Microsoft SmartScreen Filter is a feature in Windows Internet Explorer that helps in detecting the phishing and Malware websites. Such websites fraudulently got to reveal personal and financial information from the users.

3.6 Software and Hardware Firewall

A firewall is like a gatekeeper that checks information coming from outside and decide to block or allows it. Firewall is a software or hardware that checks information coming from the Internet or a network. Windows Firewall with Advanced Security is a Microsoft Management Console snap-in that provides more advanced options for IT professionals. Firewall can be in the form of hardware such as router or hardware firewalls are incorporated into the router that is placed between a computer and an Internet gateway. A Firewall has one or more of three methods to control traffic flowing in and out of the network: Packet Filters, Proxy Servers and Stateful Packets Filters.

![Firewall Diagram](image)

- Packet filtering - Packets (small chunks of data) are analyzed against a set of filters and are sent to the requesting system and all others are discarded.

- Proxy service - Information from the Internet is retrieved by the firewall and then sent to the requesting system and vice versa.

- Stateful inspection - A newer method that does not examine the contents of each packet but instead compares certain key parts of the packet to a database of trusted
information. Information traveling from inside the firewall to the outside is monitored for specific defining characteristics, and then incoming information is compared to these characteristics. If the comparison yields a reasonable match, the information is allowed through. Otherwise it is discarded.

Firewalls are used as filters based on several conditions [32]. If a certain IP address outside the company is reading too many files from a server, the firewall can block all traffic to or from that IP address. One can customize the settings for each type of network location in Windows Firewall as shown in the figure.

![Windows firewall Setting for Protection](image)

The advantages of a hardware firewall include the following:
Software firewalls utilize more system resources, like disk space and memory than hardware firewalls that results in reduced speed. A single hardware firewall provides protection for the complete network, which means all computers get protection and single hardware firewall is affordable. Hardware firewalls work perfectly for businesses that use a broadband Internet connection, like DSL or cable modem. A hardware firewall is not easily vulnerable to any malicious software unlike software firewalls.
Disadvantages: Configuration of a hardware firewall is difficult therefore a novice might not be able to install it. The traffic going out from the website is considered safe by the hardware firewall, this can create an issue if malware, penetrates your network and tries to connect to the internet.