Modeling and Simulation of DDoS Attack using Omnet++

Design Review

Student name & IDs:

Roee Afriat 208499137

Liel Sinn 209195155

Contents

1. Introduction

1.1 Definitions and abbreviations

Abbreviations:

DDoS - Distributed Denial of Service

UDP - User Datagram Protocol

ICMP - Internet Control Message Protocol

SIP - Session Initiation Protocol

OMNET++ - Objective Module Network Testbed in C++

REASE - Realistic Simulation Environment

Definitions:

SYN flood attack – the attacker sends synchronize messages of the TCP protocol rapidly without finalizing the connection.

Ping of Death attack – ICMP packets that are bigger than the maximum size of usual ICMP packets thus buffer overflow can occur.

Slowloris attack – partial requested are send to the target application server periodically in order to keep connections open as long as possible.

SIP INVITE flood attack – used in VoIP(Voice over IP), floods the VoIP Server with high volume INVITE packets.

1.2 Overview

DDoS attacks is an evolving subject these days. Its' popularity stems from its' easy accomplishment, hard tracing and disastrous effect on the victim. The goal of this type of attacks is to occupy the server victim with irrelevant request thus keeping the victim from giving service of legitimate clients. DoS attack using one host to attack the target, while DDoS attack uses multiple hosts to do so. In order to perform a DDoS attack, the attacker generates a network of compromised hosts ("zombies") to send a lot of traffic towards the target victim. To do so, the attacker will discover vulnerable hosts, on which he will install a special malicious program. This program will make those hosts capable of discovering and handling a lot of "zombies" (other compromised hosts) by installing attack tools on them. The impact of the DDoS attack is measured according the parameters throughput, percentage link utilization and packet drop counts.

1.3 Goals of the simulation

The purpose of the paper and this simulation is to study the impact of DDoS attacks with regard to two parameters. The first parameter is the intensity of the attack, which means the volume of the attack's rate. The second parameter is the buffer size of network components. Moreover, this simulation is measuring the impact of DDoS attacks in large-scale networks with random distribution of DDoS zombies.

1.4 Assumptions

2. Design and Flow

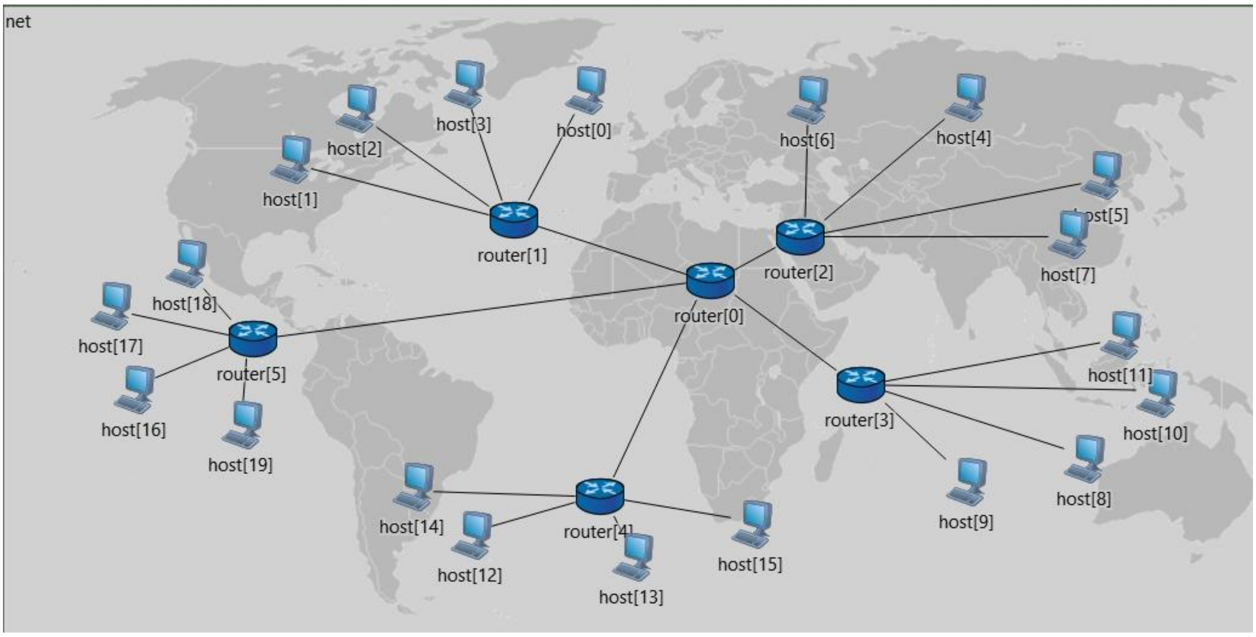
2.1 Overview

The system consists of twenty devices and six routers. The network is build of 5 LANs(local area network), each LAN contains four devices and one router that connects the LAN to the internet. Router zero represent the 'internet'. The program uses 3 simple modules in order to build the compound modules in the network:

App- responsible to generate traffic and receiving packets.

L2Quene- represents the network interface for point to point connection. Packets that arrive while a previous packet is being transmitted are queued up.

Routing- responsible for routing packets according to the destination address given in the header of the packet. It contains a routing table that is built at the beginning of the simulation.



2.2 Modules overview

The system is build of two compound modules: Node and Router that are build of 3 simple modules:

Simple Module: App

Description: This module implies the application layer. Generates packets with uniform distributed destination address and handles incoming traffic.

Variables: Address – self IP address

destAddress – destination IP address

sendTaTime- time between generation packets

packetLenght-length of one message

Functions:

Statistics Gathering:

Simple Module: L2Quene

Description: This module implies the physical layer of the links in the network. Packets that arrive while a previous packet is being transmitted are queued up.

Variables: frameCapacity- max number of packets that can be queued up

Functions:

Statistics Gathering:

Simple Module: Routing

Description: This module implies the network layer. It's purpose is to determine the route of a packet according to it's destination IP address.

Variables:

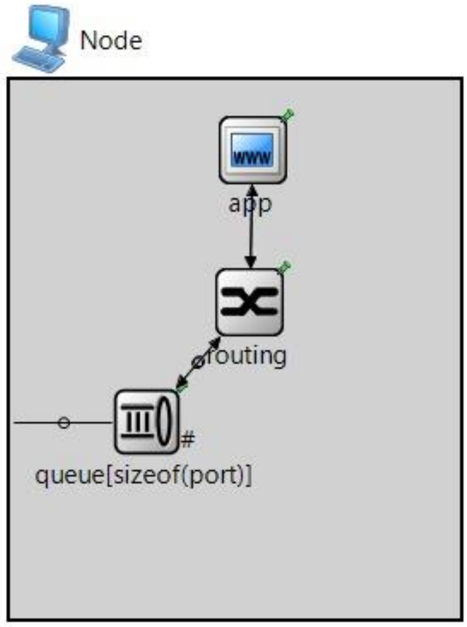
Functions:

Statistics Gathering:

Compound Module: Node

Description: The Node module contains three simple modules as can be seen in the figure below. Represent the host devices in the network.

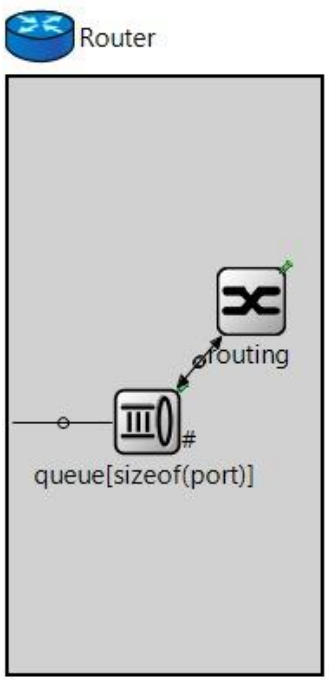
Variables: address- represents the network layer address of the specific node



Compound Module: Router

Description: The Router module contains two simple modules as can be seen in the figure below. Represent the router devices in the network.

Variables: address- represents the network layer address of the specific node



2.3 Application Interfaces

2.4 Results and Test measurements