Assignment 3

Assumptions:

Link Bandwidth= 4 mB
Link Delay= 5 ms
Queuing Strategy= RED

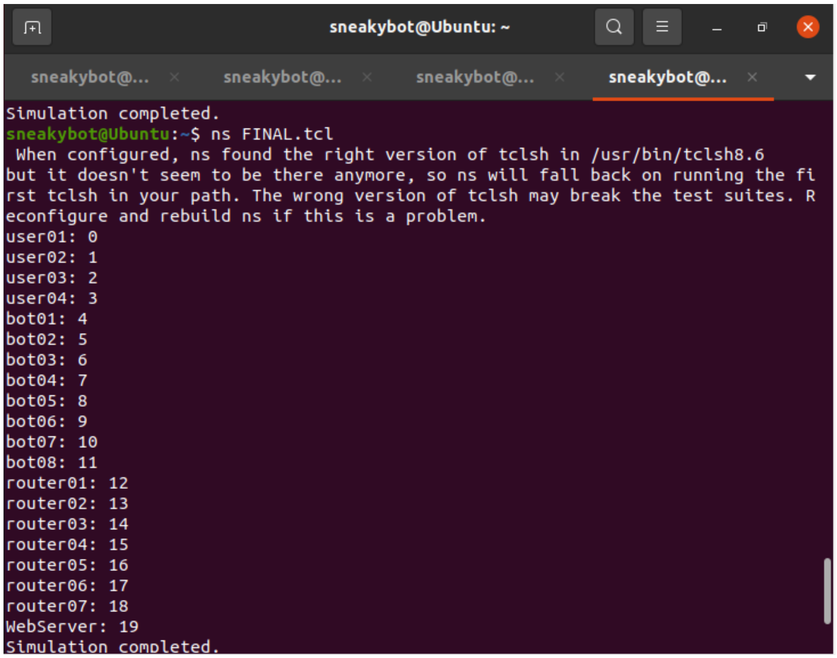
Purpose:

The objective of this assignment was to simulate a DDoS attack on a small network, and to analyze the packet output within the tracer file. I have analyzed my results with a graph and python script that kept track of sent packets and dropped packets from each user node during each second of the simulation. Using the given network topology for the assignment I created a situation where I could maximize degradation with 8 bots.

Method:

The simulation was carried out using an NS-2 simulator. The simulation consisted of a small network with 8 bots, 4 users, and 7 routers. The simulation was run for 10 seconds, and the trace file was analyzed to determine the packet degradation ratio.

Output:



```
Simulation completed.
sneakybot@Ubuntu:~$ ns FINAL.tcl
 When configured, ns found the right version of tclsh in /usr/bin/tclsh8.6
but it doesn't seem to be there anymore, so ns will fall back on running the fi
rst tclsh in your path. The wrong version of tclsh may break the test suites. R
econfigure and rebuild ns if this is a problem.
user01: 0
user02: 1
user03: 2
user04: 3
bot01: 4
bot02: 5
bot03: 6
bot04: 7
bot05: 8
bot06: 9
bot07: 10
bot08: 11
router01: 12
router02: 13
router03: 14
router04: 15
router05: 16
router06: 17
router07: 18
WebServer: 19
Simulation completed.
```

Maximizing Degradation:
To maximize degradation I added 8 bots and targeted two specific routers, which in this case was router05 and router07. I maintained the bots at a rate of 1Mb/sec so they could stay undetected from user traffic. Having 8 bots resulted in 25762 dropped packets and 49648 sent packets. Therefore, my degradation rate was approximately 51.89%.

Packet degradation was found by dividing packets dropped by packets sent:
25762 / 49648 = 51.88930067676442%

The data obtained from the out.tr file showed that the packets were dropped from all the user nodes in the network. The plot of the number of packets dropped from each user node in every second during the simulation showed that the packet drop rate increased as the traffic rate of bots and users increased.

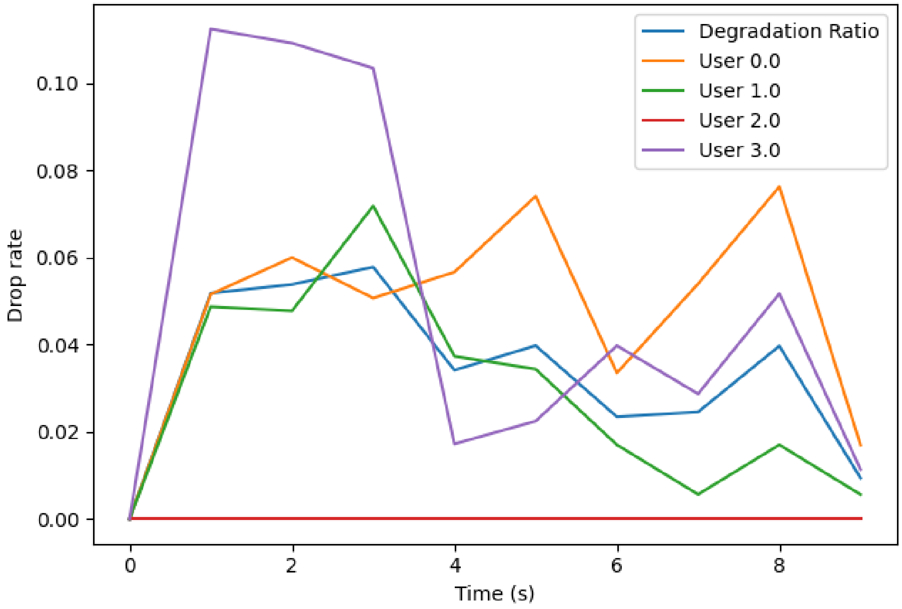
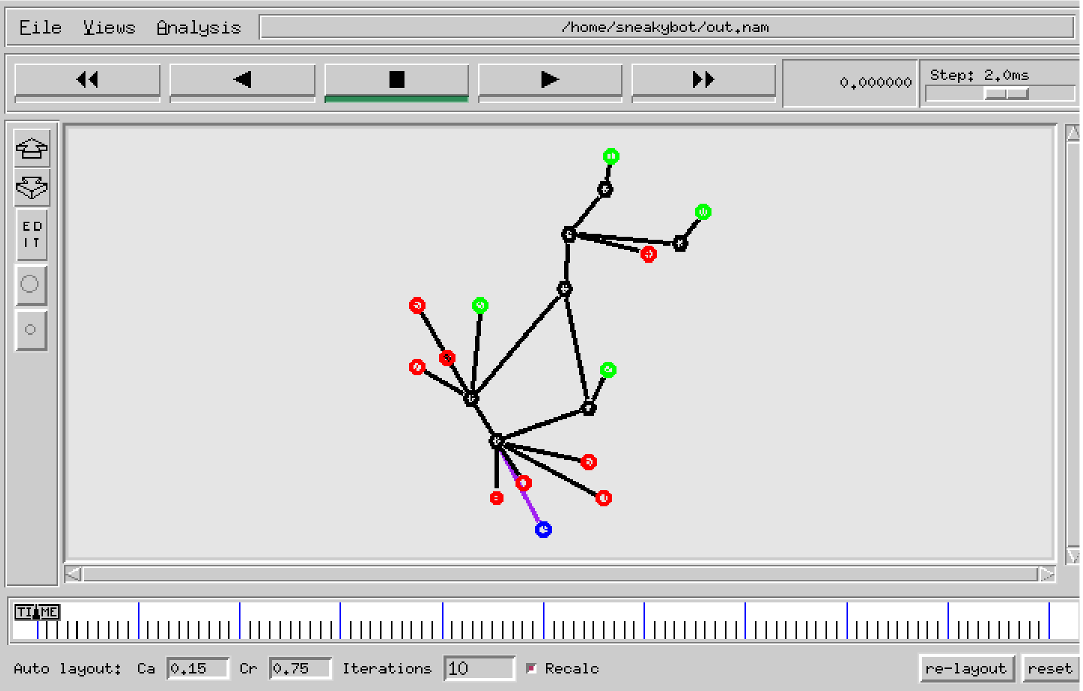


Figure 1: Graph displaying the drop rate of packets for each user node across the time span of 10 seconds.

Network Topology:

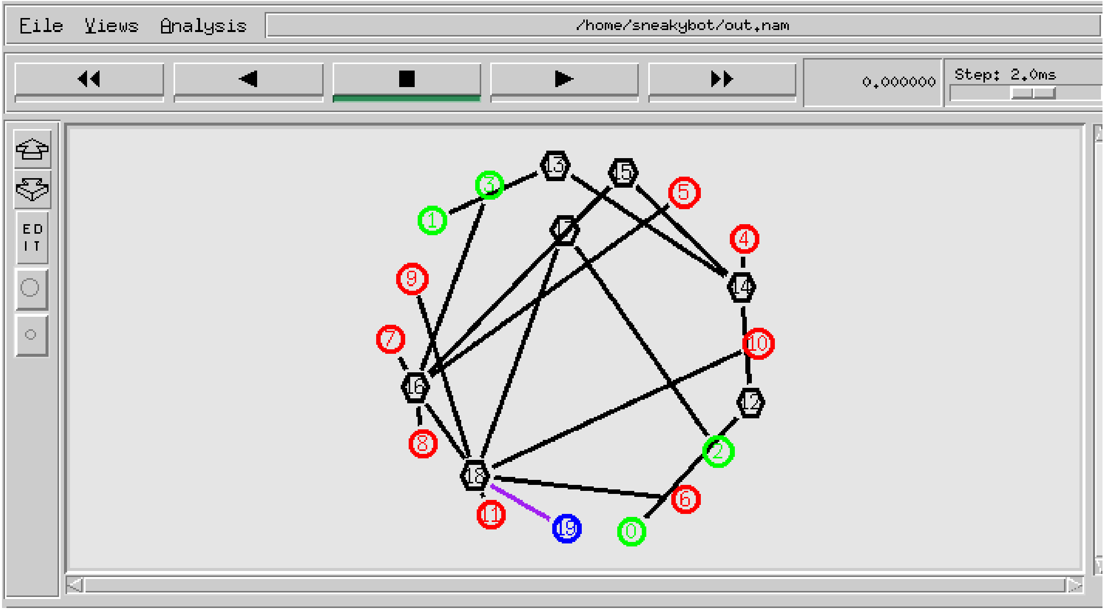


/home/sneakybot/out.nam

0.000000

Step: 2.0ms

Auto layout: Ca 0.15 Cr 0.75 Iterations 10 ☒ Recalc



/home/sneakybot/out.nam

0.000000

Step: 2.0ms

Figure 2: Network topology shown in nam simulation.

Conclusion:

The objective of this task is to replicate a DDoS attack on a small network using Network Simulation (NS). By analyzing the trace file, a graph can be plotted to display the total number of dropped packets from each user node every second during the simulation. The network topology has already been provided. As the traffic rate of bots and users increases, the number of dropped packets also rises. Moreover, if the simulation time is increased, the degradation ratio will also increase. This simulation has demonstrated the importance of understanding network topology, as it helps in identifying the nodes involved in the attack. Understanding where the attack is coming from and targeting, as well as keeping track of dropped packets is important. This is necessary information so one can reduce network vulnerabilities. The high packet degradation ratio shows that the network is not adequately protected against such attacks. The simulation results suggest that there is a need for additional security measures to protect against crossfire attacks.