Network Security Project Report

Group - 8

Sai Kumar Siddu - R11779742
Mounika Subhakari Gandham - R11789255
Chandana Tulluru - R11800872
Akhil Katkam - R11784414
Srinivasa Chanakya Maramashetti - R11803400

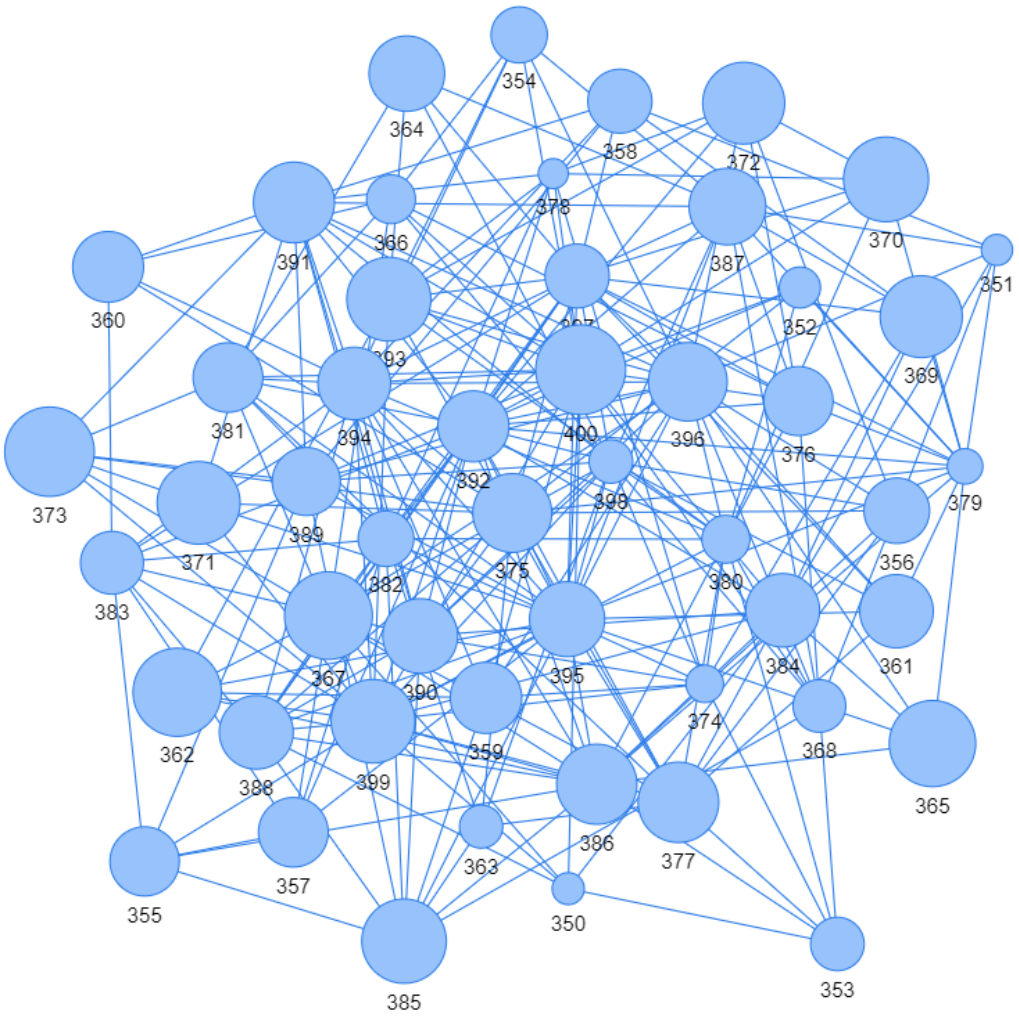
Steps followed for determining the Network connectivity for Nodes(350 to 400)

Step1 : Calculate the average number of packets received by each host using the below formula.

- $average\ number\ of\ packets\ = \frac{total\ number\ of\ packets\ received\ within\ time\ T}{Window\ T}$
- Average number of packets received by each host before the attack (350 to 400 nodes) are (node, degree):
  [(350, 63), (351, 58), (352, 114), (353, 183), (354, 198), (355, 271), (356, 250), (357, 273), (358, 242), (359, 283), (360, 280), (361, 294), (362, 377), (363, 125), (364, 306), (365, 366), (366, 157), (367, 374), (368, 178), (369, 342), (370, 358), (371, 347), (372, 342), (373, 384), (374, 94), (375, 325), (376, 270), (377, 334), (378, 51), (379, 82), (380, 152), (381, 273), (382, 195), (383, 236), (384, 296), (385, 356), (386, 332), (387, 312), (388, 296), (389, 265), (390, 302), (391, 336), (392, 281), (393, 353), (394, 290), (395, 303), (396, 324), (397, 242), (398, 128), (399, 352), (400, 386)]
- Average number of packets received by each host after the attack (350 to 400 nodes) are (node, degree):
  [(350, 200), (351, 249), (352, 190), (353, 210), (354, 221), (355, 230), (356, 194), (357, 166), (358, 220), (359, 207), (360, 198), (361, 155), (362, 176), (363, 171), (364, 230), (365, 207), (366, 175), (367, 184), (368, 197), (369, 188), (370, 209), (371, 192), (372, 191), (373, 216), (374, 244), (375, 135), (376, 235), (377, 152), (378, 203), (379, 184), (380, 171), (381, 186), (382, 169), (383, 207), (384, 155), (385, 178), (386, 228), (387, 413), (388, 209), (389, 570), (390, 214), (391, 267), (393, 166)]

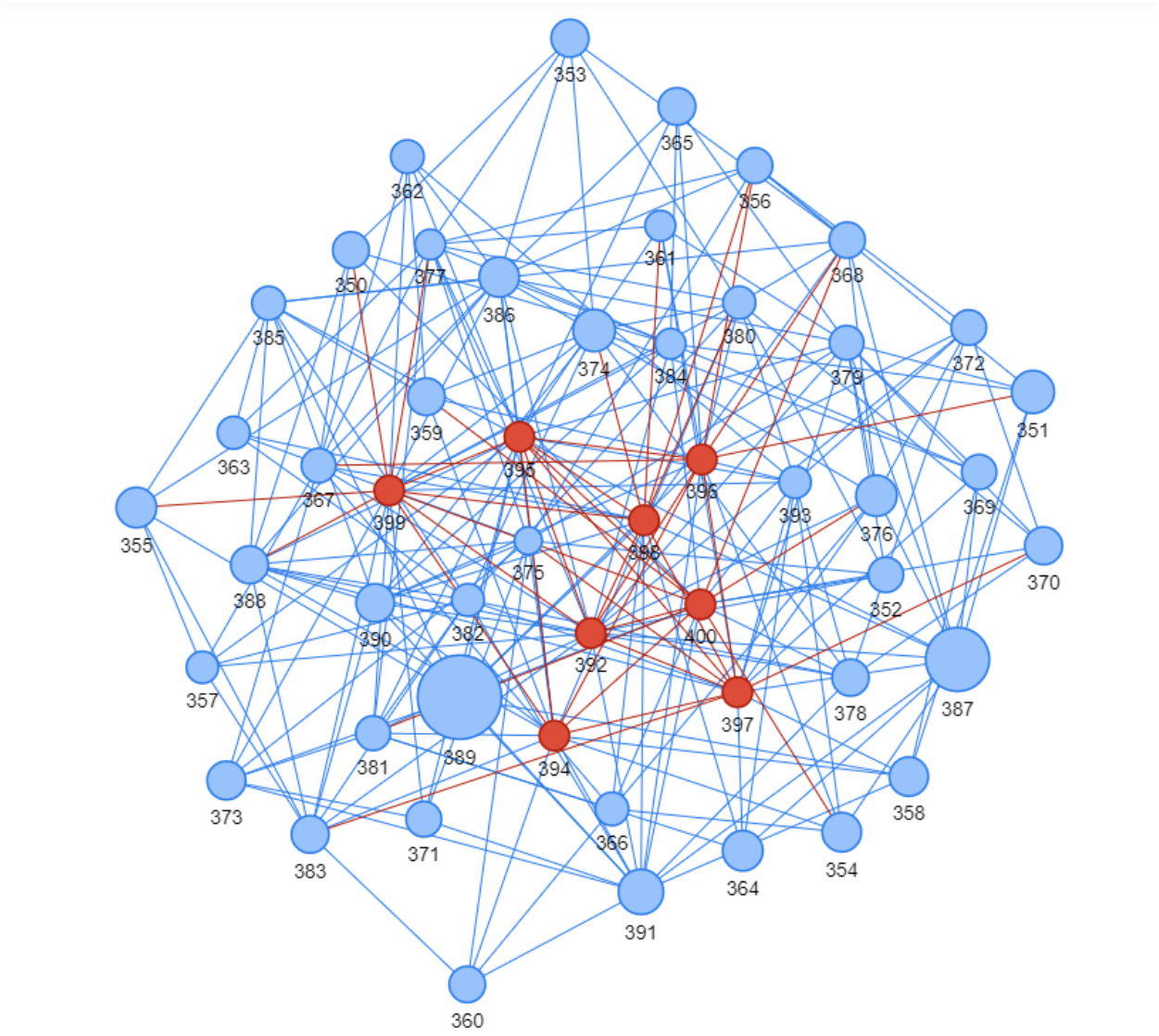
Step2 : Plotting Network Graph for routers(350 to 400) Before DDoS Attack

- Size of the nodes in the below graph is proportional to the average number of packets each node received
  - From the above, Router 400 has highest average packets received(i.e., 386)



Step3: Plotting Network Graph for routers(350 to 400) After DDoS Attack

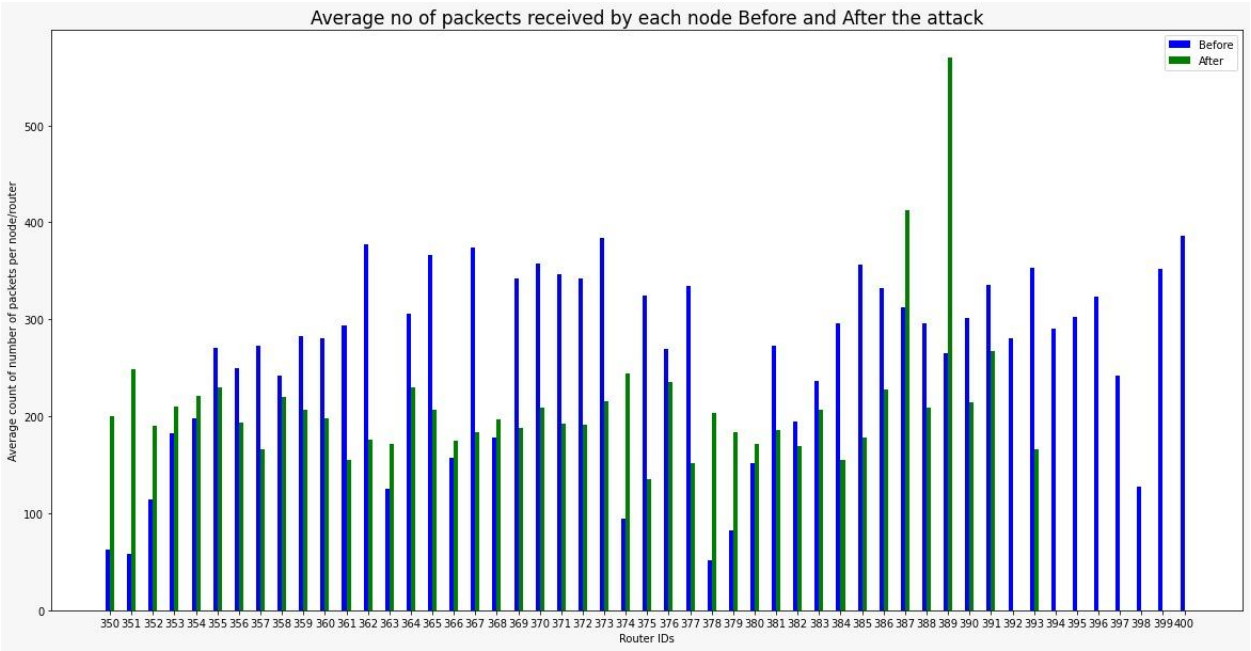
- Red Nodes here are the ones removed from the network
- The number of routers ***n*** removed is *selected based on the highest degree of router.*
- Routers removed are (router,degree):
  - [(392, 22), (395, 21), (399, 19), (400, 18), (396, 18), (397, 18), (394, 17), (398, 17)]
- Size of the nodes in the below graph is proportional to the average number of packets each node received.
  - From the above, Router 389 has highest average packets received (i.e.,570).



Step4 : **Interpretation of graph:**
Comparison of average number of packets received by each host before and the after the DoS/DDoS attack.

- In the above graph, with the average *number of packets received by each host on Y-Axis* and *Number of Hosts (350-400) Hosts on X Axis*. Blue bars indicate the avg number of packets received by each host before attack and green bars indicate the same after the Dos attack
- **Interpreting the plot above:** We can see that the number of packets received by each host (from 350 - 400) before the attack is higher than that received after launching the DOS Attack.
- **Justification for above plot:** So, in the after attack scenario as some nodes deny providing the service , the before attack bars in blue received a higher number of packets than ones in green.

Also , for the 8 nodes(that were removed) we see that they have received 0 packets simulating perfect Denial.



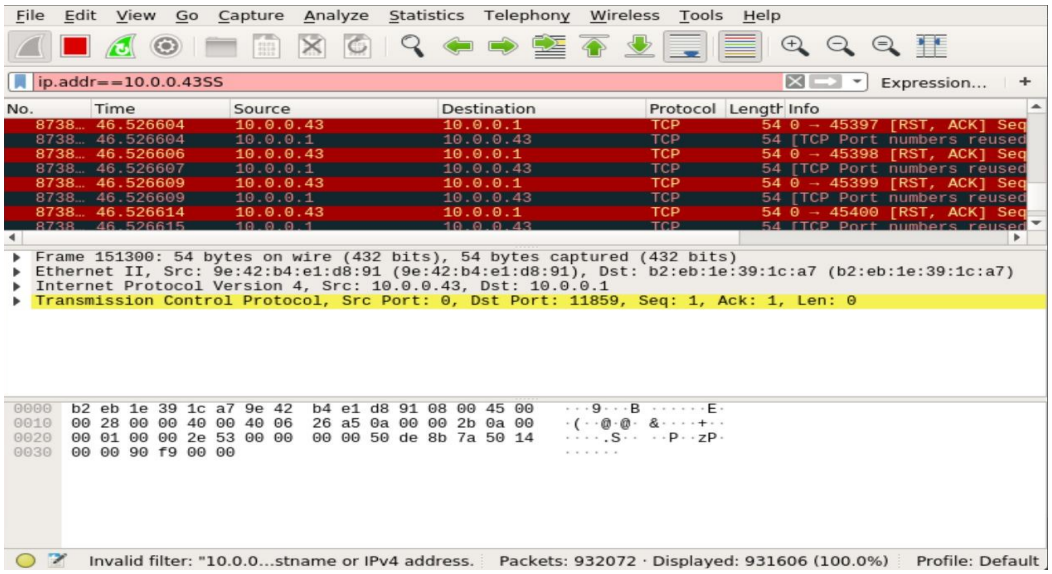
Lessons Learnt:

1. From **project 1**, we have learned how we can represent the internet through Graph G(V,E) where V is a node/router and edges are links connecting routers. Also we have learned
   a. Creating the network in an interactive way using Pyvis .
   b. Visualizing the network by including features like Zoom in and out, change the node size and color proportional to its degree
   c. Understanding the Node degree distribution for all, the routers by plotting a histogram
2. From **project 2 and 3,** we have learned
   a. Building the network in Mininet and attaching hosts to each device and checking the communication between them through pinging them.
   b. Learned that Denial of service can be launched in 2 different ways
      i. By attacking the routers in the network, such that when service is requested from them, they would be unreachable.
         1. This is justified from the figure below, we attacked 8 routers, for example consider the router 392.
         2. When 392 is requested for a service, it will be unreachable to the client.
         3. 392 cannot ping or request a service from another router.

```
*** Results: 29% dropped (1806/2550 received)
mininet> 392 ping 350
PING 10.0.0.1 (10.0.0.1) 56(84) bytes of data.
From 10.0.0.43 icmp_seq=1 Destination Host Unreachable
From 10.0.0.43 icmp_seq=2 Destination Host Unreachable
From 10.0.0.43 icmp_seq=3 Destination Host Unreachable
From 10.0.0.43 icmp_seq=4 Destination Host Unreachable
From 10.0.0.43 icmp_seq=5 Destination Host Unreachable
From 10.0.0.43 icmp_seq=6 Destination Host Unreachable
From 10.0.0.43 icmp_seq=7 Destination Host Unreachable
From 10.0.0.43 icmp_seq=8 Destination Host Unreachable
From 10.0.0.43 icmp_seq=9 Destination Host Unreachable
^C
--- 10.0.0.1 ping statistics ---
10 packets transmitted, 0 received, +9 errors, 100% packet loss, time 9217ms
pipe 4
mininet>
```

```
mininet> 350 ping 392
PING 10.0.0.43 (10.0.0.43) 56(84) bytes of data.
From 10.0.0.1 icmp_seq=1 Destination Host Unreachable
From 10.0.0.1 icmp_seq=2 Destination Host Unreachable
From 10.0.0.1 icmp_seq=3 Destination Host Unreachable
From 10.0.0.1 icmp_seq=4 Destination Host Unreachable
From 10.0.0.1 icmp_seq=5 Destination Host Unreachable
From 10.0.0.1 icmp_seq=6 Destination Host Unreachable
From 10.0.0.1 icmp_seq=7 Destination Host Unreachable
From 10.0.0.1 icmp_seq=8 Destination Host Unreachable
From 10.0.0.1 icmp_seq=9 Destination Host Unreachable
^C
--- 10.0.0.43 ping statistics ---
10 packets transmitted, 0 received, +9 errors, 100% packet loss, time 9205ms
pipe 4
mininet>
```

ii. The second way is creating traffic or congestion for ‘n’ (8 nodes) and flooding them bringing routers down
    1. For example, flooding the router 392.
    2. 392 is pinged from 350, packets are not received at 392’s end.



c. How to capture packet Analysis and statistics using wireshark software.
d. Visualizing the DDOs attack and interpreting the before and After attack Scenarios.

Justification for how ‘n’ Nodes are selected:

- To launch the DDoS Attack, by removing the ‘n’ number of routers, the selection of ‘n’ (8 nodes here) is made based on the degree of the node.
- First 8 nodes with highest degree are selected and are removed as they have several connections and thus attacking them would impact the network on a large scale.
- Below is the List of (Router , degree) removed for launching the attack.
    - [(392, 22), (395, 21), (399, 19), (400, 18), (396, 18), (397, 18), (394, 17), (398, 17)]**.**