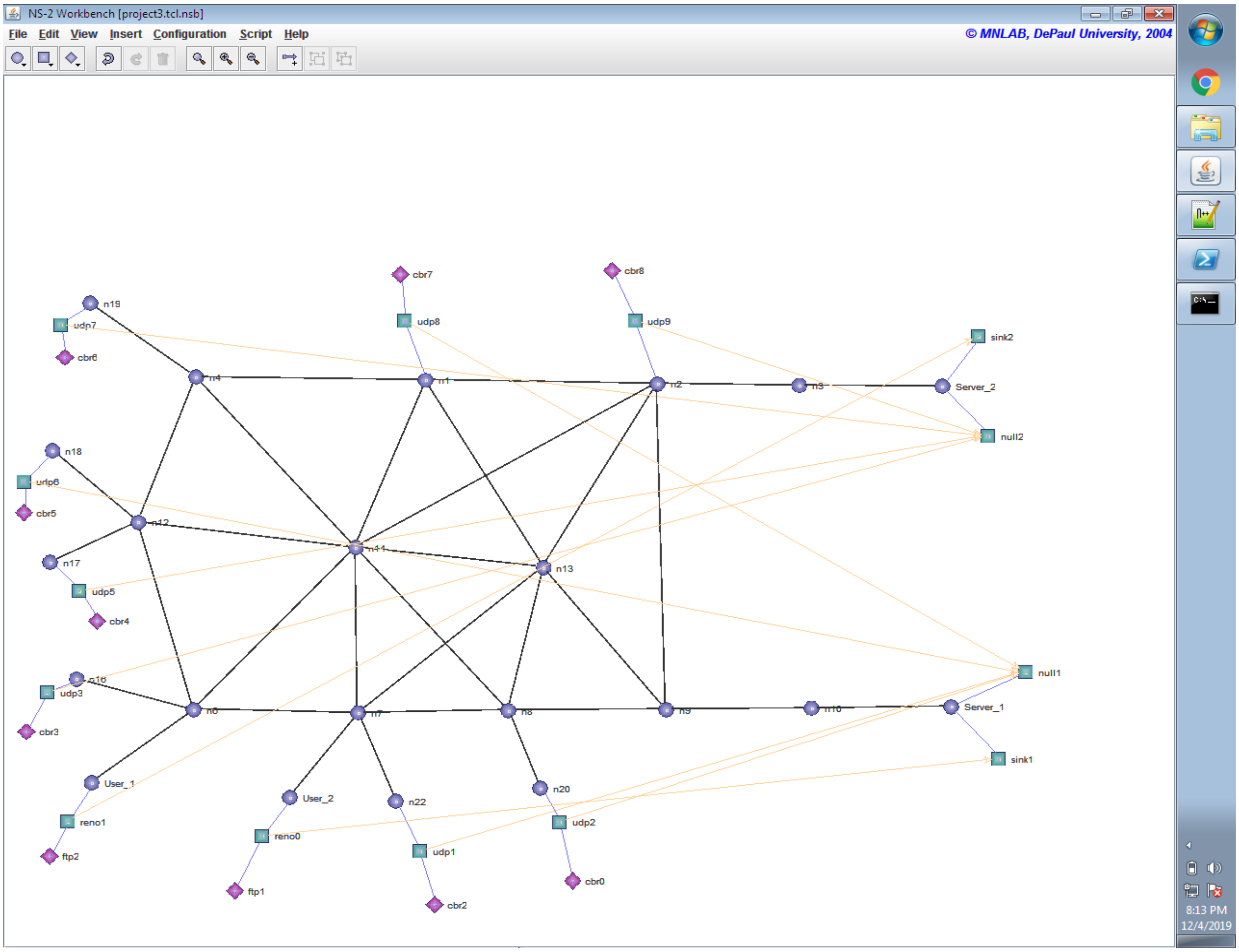
ITIS 6167 – Network Security

Project 3 – DDoS Attack Simulation

Sahil Bhirud

The network is created in the following manner:



1. **Table**

Source (attacker)	**Destination**	**Traffic Rate (Kbps)**
CBR0	Server 1	448kbps
CBR2	Server 1	448kbps
CBR3	Server 2	448kbps
CBR4	Server 2	448kbps
CBR5	Server 1	448kbps
CBR6	Server 2	448kbps
CBR7	Server 1	448kbps
CBR8	Server 2	448kbps
Total number of bots = 8		**Total Traffic Rate = 3584kbps**

2.

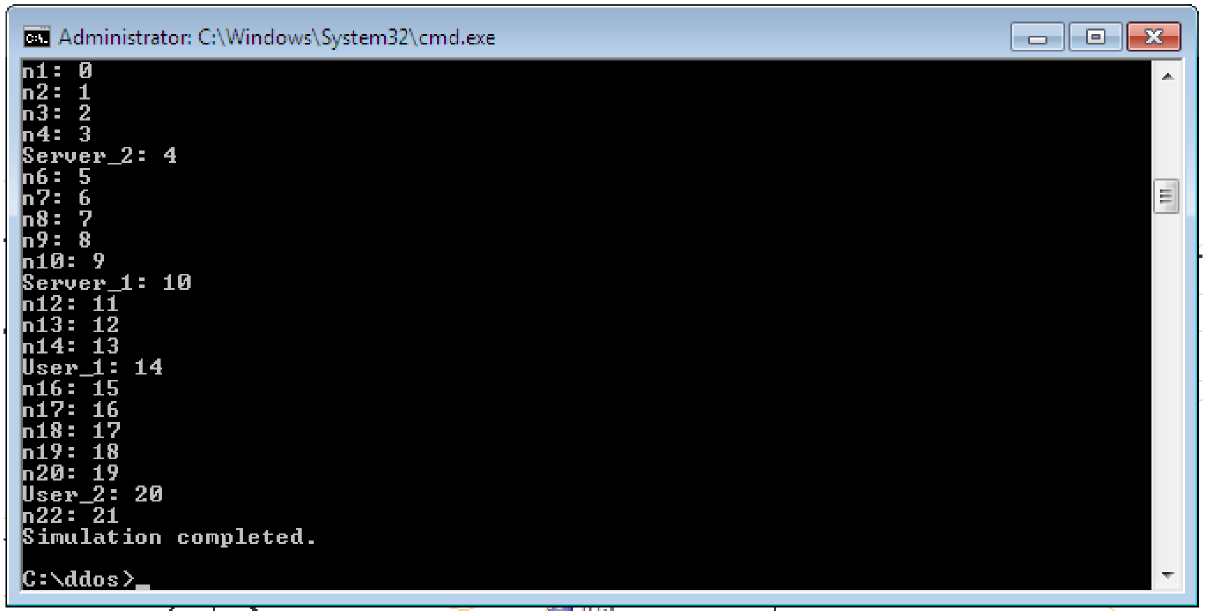
Case 1: Between User 1 and Server 2

The link between nodes n2(1) and n3(2) prevented the traffic to flow between the end users.

Case 2: Between User 2 and Server 1

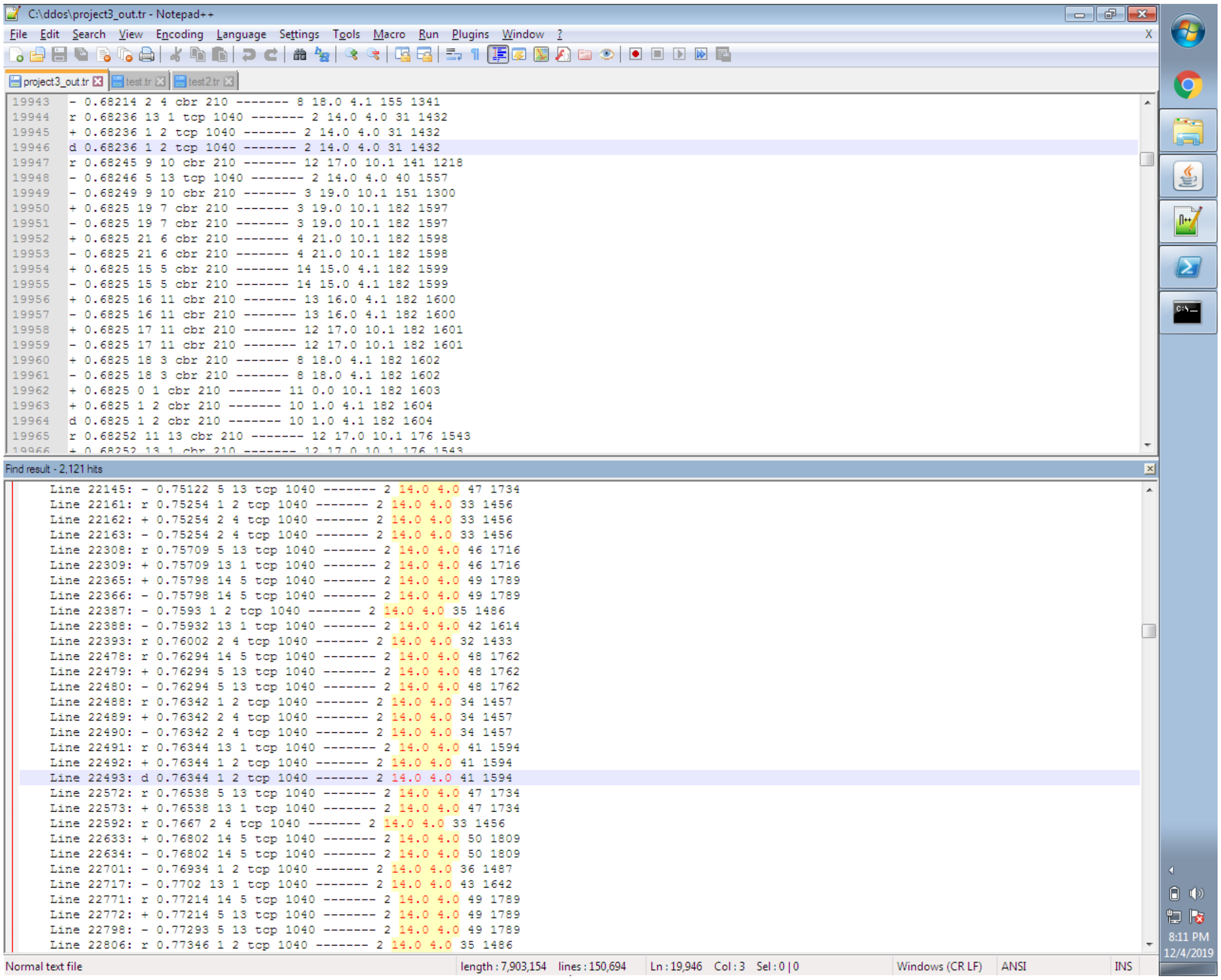
The nodes n9(8) and n10(9) are preventing User 2 to connect to Server 1.

3. **Screenshots**



```
n1: 0
n2: 1
n3: 2
n4: 3
Server_2: 4
n6: 5
n7: 6
n8: 7
n9: 8
n10: 9
Server_1: 10
n12: 11
n13: 12
n14: 13
User_1: 14
n16: 15
n17: 16
n18: 17
n19: 18
n20: 19
User_2: 20
n22: 21
Simulation completed.

C:\ddos>_
```

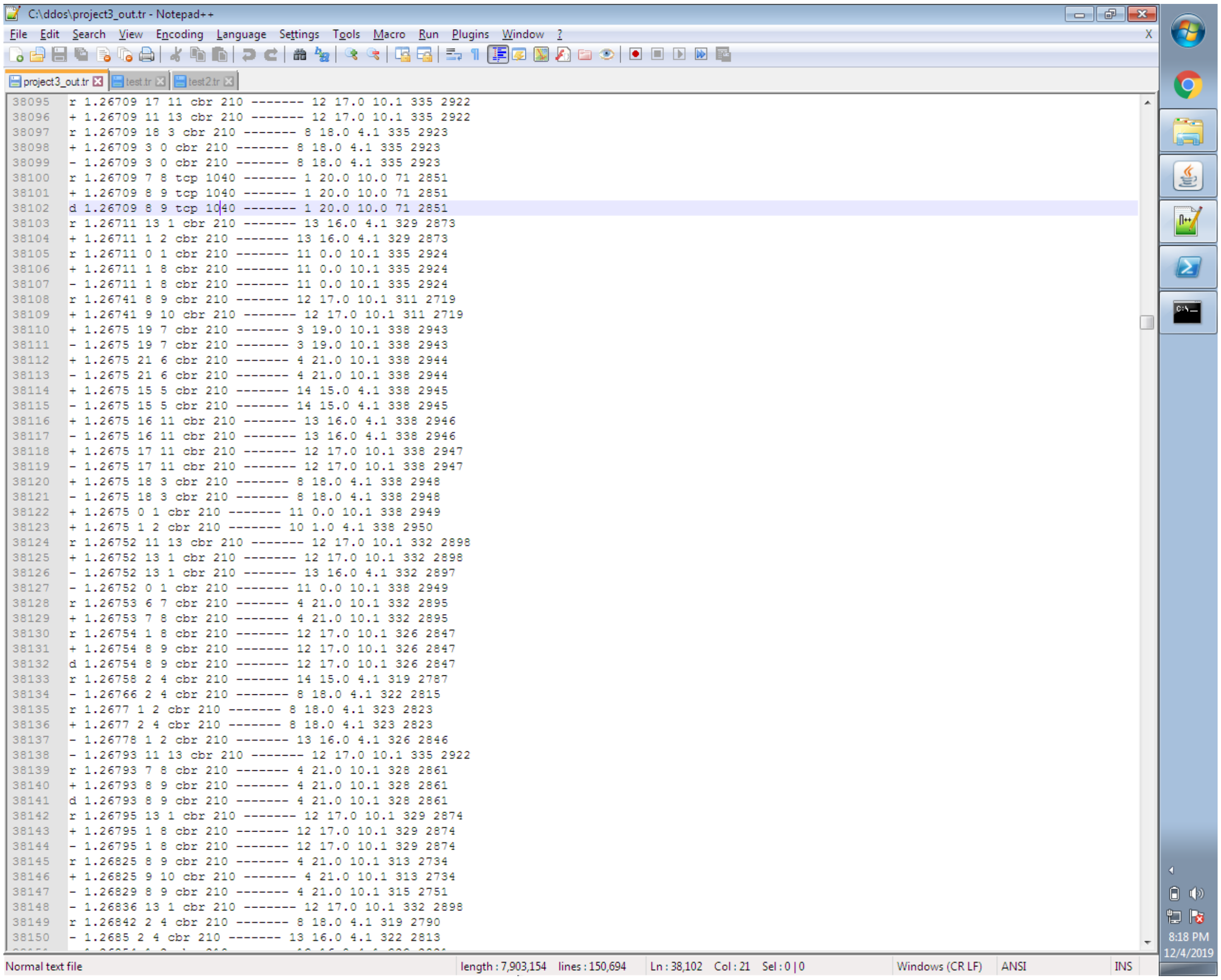

C:\ddos\project3_out.tr - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
project3_out.tr
test.tr
test2.tr
8:11 PM
12/4/2019

```
- 0.68214 2 4 cbr 210 ------- 8 18.0 4.1 155 1341
r 0.68236 13 1 tcp 1040 ------- 2 14.0 4.0 31 1432
+ 0.68236 1 2 tcp 1040 ------- 2 14.0 4.0 31 1432
d 0.68236 1 2 tcp 1040 ------- 2 14.0 4.0 31 1432
r 0.68245 9 10 cbr 210 ------- 12 17.0 10.1 141 1218
- 0.68246 5 13 tcp 1040 ------- 2 14.0 4.0 40 1557
- 0.68249 9 10 cbr 210 ------- 3 19.0 10.1 151 1300
+ 0.6825 19 7 cbr 210 ------- 3 19.0 10.1 182 1597
- 0.6825 19 7 cbr 210 ------- 3 19.0 10.1 182 1597
+ 0.6825 21 6 cbr 210 ------- 4 21.0 10.1 182 1598
- 0.6825 21 6 cbr 210 ------- 4 21.0 10.1 182 1598
+ 0.6825 15 5 cbr 210 ------- 14 15.0 4.1 182 1599
- 0.6825 15 5 cbr 210 ------- 14 15.0 4.1 182 1599
+ 0.6825 16 11 cbr 210 ------- 13 16.0 4.1 182 1600
- 0.6825 16 11 cbr 210 ------- 13 16.0 4.1 182 1600
+ 0.6825 17 11 cbr 210 ------- 12 17.0 10.1 182 1601
- 0.6825 17 11 cbr 210 ------- 12 17.0 10.1 182 1601
+ 0.6825 18 3 cbr 210 ------- 8 18.0 4.1 182 1602
- 0.6825 18 3 cbr 210 ------- 8 18.0 4.1 182 1602
+ 0.6825 0 1 cbr 210 ------- 11 0.0 10.1 182 1603
+ 0.6825 1 2 cbr 210 ------- 10 1.0 4.1 182 1604
d 0.6825 1 2 cbr 210 ------- 10 1.0 4.1 182 1604
r 0.68252 11 13 cbr 210 ------- 12 17.0 10.1 176 1543
+ 0.68252 13 1 cbr 210 ------- 12 17.0 10.1 176 1543
```

Find result - 2,121 hits

```
    Line 22145: - 0.75122 5 13 tcp 1040 ------- 2 14.0 4.0 47 1734
    Line 22161: r 0.75254 1 2 tcp 1040 ------- 2 14.0 4.0 33 1456
    Line 22162: + 0.75254 2 4 tcp 1040 ------- 2 14.0 4.0 33 1456
    Line 22163: - 0.75254 2 4 tcp 1040 ------- 2 14.0 4.0 33 1456
    Line 22308: r 0.75709 5 13 tcp 1040 ------- 2 14.0 4.0 46 1716
    Line 22309: + 0.75709 13 1 tcp 1040 ------- 2 14.0 4.0 46 1716
    Line 22365: + 0.75798 14 5 tcp 1040 ------- 2 14.0 4.0 49 1789
    Line 22366: - 0.75798 14 5 tcp 1040 ------- 2 14.0 4.0 49 1789
    Line 22387: - 0.7593 1 2 tcp 1040 ------- 2 14.0 4.0 35 1486
    Line 22388: - 0.75932 13 1 tcp 1040 ------- 2 14.0 4.0 42 1614
    Line 22393: r 0.76002 2 4 tcp 1040 ------- 2 14.0 4.0 32 1433
    Line 22478: r 0.76294 14 5 tcp 1040 ------- 2 14.0 4.0 48 1762
    Line 22479: + 0.76294 5 13 tcp 1040 ------- 2 14.0 4.0 48 1762
    Line 22480: - 0.76294 5 13 tcp 1040 ------- 2 14.0 4.0 48 1762
    Line 22488: r 0.76342 1 2 tcp 1040 ------- 2 14.0 4.0 34 1457
    Line 22489: + 0.76342 2 4 tcp 1040 ------- 2 14.0 4.0 34 1457
    Line 22490: - 0.76342 2 4 tcp 1040 ------- 2 14.0 4.0 34 1457
    Line 22491: r 0.76344 13 1 tcp 1040 ------- 2 14.0 4.0 41 1594
    Line 22492: + 0.76344 1 2 tcp 1040 ------- 2 14.0 4.0 41 1594
    Line 22493: d 0.76344 1 2 tcp 1040 ------- 2 14.0 4.0 41 1594
    Line 22572: r 0.76538 5 13 tcp 1040 ------- 2 14.0 4.0 47 1734
    Line 22573: + 0.76538 13 1 tcp 1040 ------- 2 14.0 4.0 47 1734
    Line 22592: r 0.7667 2 4 tcp 1040 ------- 2 14.0 4.0 33 1456
    Line 22633: + 0.76802 14 5 tcp 1040 ------- 2 14.0 4.0 50 1809
    Line 22634: - 0.76802 14 5 tcp 1040 ------- 2 14.0 4.0 50 1809
    Line 22701: - 0.76934 1 2 tcp 1040 ------- 2 14.0 4.0 36 1487
    Line 22717: - 0.7702 13 1 tcp 1040 ------- 2 14.0 4.0 43 1642
    Line 22771: r 0.77214 14 5 tcp 1040 ------- 2 14.0 4.0 49 1789
    Line 22772: + 0.77214 5 13 tcp 1040 ------- 2 14.0 4.0 49 1789
    Line 22798: - 0.77293 5 13 tcp 1040 ------- 2 14.0 4.0 49 1789
    Line 22806: r 0.77346 1 2 tcp 1040 ------- 2 14.0 4.0 35 1486
```

Normal text file   length : 7,903,154   lines : 150,694   Ln : 19,946   Col : 3   Sel : 0 | 0   Windows (CR LF)   ANSI   INS


C:\ddos\project3_out.tr - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
project3_out.tr
test.tr
test2.tr
Normal text file
length : 7,903,154 lines : 150,694
Ln : 38,102 Col : 21 Sel : 0 | 0
Windows (CR LF)
ANSI
INS
8:18 PM
12/4/2019

```
r 1.26709 17 11 cbr 210 ------- 12 17.0 10.1 335 2922
+ 1.26709 11 13 cbr 210 ------- 12 17.0 10.1 335 2922
r 1.26709 18 3 cbr 210 ------- 8 18.0 4.1 335 2923
+ 1.26709 3 0 cbr 210 ------- 8 18.0 4.1 335 2923
- 1.26709 3 0 cbr 210 ------- 8 18.0 4.1 335 2923
r 1.26709 7 8 tcp 1040 ------- 1 20.0 10.0 71 2851
+ 1.26709 8 9 tcp 1040 ------- 1 20.0 10.0 71 2851
d 1.26709 8 9 tcp 1040 ------- 1 20.0 10.0 71 2851
r 1.26711 13 1 cbr 210 ------- 13 16.0 4.1 329 2873
+ 1.26711 1 2 cbr 210 ------- 13 16.0 4.1 329 2873
r 1.26711 0 1 cbr 210 ------- 11 0.0 10.1 335 2924
+ 1.26711 1 8 cbr 210 ------- 11 0.0 10.1 335 2924
- 1.26711 1 8 cbr 210 ------- 11 0.0 10.1 335 2924
r 1.26741 8 9 cbr 210 ------- 12 17.0 10.1 311 2719
+ 1.26741 9 10 cbr 210 ------- 12 17.0 10.1 311 2719
+ 1.2675 19 7 cbr 210 ------- 3 19.0 10.1 338 2943
- 1.2675 19 7 cbr 210 ------- 3 19.0 10.1 338 2943
+ 1.2675 21 6 cbr 210 ------- 4 21.0 10.1 338 2944
- 1.2675 21 6 cbr 210 ------- 4 21.0 10.1 338 2944
+ 1.2675 15 5 cbr 210 ------- 14 15.0 4.1 338 2945
- 1.2675 15 5 cbr 210 ------- 14 15.0 4.1 338 2945
+ 1.2675 16 11 cbr 210 ------- 13 16.0 4.1 338 2946
- 1.2675 16 11 cbr 210 ------- 13 16.0 4.1 338 2946
+ 1.2675 17 11 cbr 210 ------- 12 17.0 10.1 338 2947
- 1.2675 17 11 cbr 210 ------- 12 17.0 10.1 338 2947
+ 1.2675 18 3 cbr 210 ------- 8 18.0 4.1 338 2948
- 1.2675 18 3 cbr 210 ------- 8 18.0 4.1 338 2948
+ 1.2675 0 1 cbr 210 ------- 11 0.0 10.1 338 2949
+ 1.2675 1 2 cbr 210 ------- 10 1.0 4.1 338 2950
r 1.26752 11 13 cbr 210 ------- 12 17.0 10.1 332 2898
+ 1.26752 13 1 cbr 210 ------- 12 17.0 10.1 332 2898
- 1.26752 13 1 cbr 210 ------- 13 16.0 4.1 332 2897
- 1.26752 0 1 cbr 210 ------- 11 0.0 10.1 338 2949
r 1.26753 6 7 cbr 210 ------- 4 21.0 10.1 332 2895
+ 1.26753 7 8 cbr 210 ------- 4 21.0 10.1 332 2895
r 1.26754 1 8 cbr 210 ------- 12 17.0 10.1 326 2847
+ 1.26754 8 9 cbr 210 ------- 12 17.0 10.1 326 2847
d 1.26754 8 9 cbr 210 ------- 12 17.0 10.1 326 2847
r 1.26758 2 4 cbr 210 ------- 14 15.0 4.1 319 2787
- 1.26766 2 4 cbr 210 ------- 8 18.0 4.1 322 2815
r 1.2677 1 2 cbr 210 ------- 8 18.0 4.1 323 2823
+ 1.2677 2 4 cbr 210 ------- 8 18.0 4.1 323 2823
- 1.26778 1 2 cbr 210 ------- 13 16.0 4.1 326 2846
- 1.26793 11 13 cbr 210 ------- 12 17.0 10.1 335 2922
r 1.26793 7 8 cbr 210 ------- 4 21.0 10.1 328 2861
+ 1.26793 8 9 cbr 210 ------- 4 21.0 10.1 328 2861
d 1.26793 8 9 cbr 210 ------- 4 21.0 10.1 328 2861
r 1.26795 13 1 cbr 210 ------- 12 17.0 10.1 329 2874
+ 1.26795 1 8 cbr 210 ------- 12 17.0 10.1 329 2874
- 1.26795 1 8 cbr 210 ------- 12 17.0 10.1 329 2874
r 1.26825 8 9 cbr 210 ------- 4 21.0 10.1 313 2734
+ 1.26825 9 10 cbr 210 ------- 4 21.0 10.1 313 2734
- 1.26829 8 9 cbr 210 ------- 4 21.0 10.1 315 2751
- 1.26836 13 1 cbr 210 ------- 12 17.0 10.1 332 2898
r 1.26842 2 4 cbr 210 ------- 8 18.0 4.1 319 2790
- 1.2685 2 4 cbr 210 ------- 13 16.0 4.1 322 2813
```

4. DDoS attack

The attack which is performed in this project is Botnet-Driven Distributed Denial-of-Service attack in which bots are used to flood the internet servers. The advantage of using botnets is that it cannot be countered by any of the current Internet defense methods because, it can use valid IP addresses, botnets can flood links without using unwanted traffic (e.g. they can send packets to each other in a way that targets groups of routers.) and a botnet can launch attack with low intensity traffic flows that cross a targeted link at roughly the same time and flood it.

To launch a crossfire attack against a target area, the attacker selects a set of public servers within the target area and a set of decoy servers surrounding the target area. These servers are easily found as they are publicly accessible. The public servers are used to construct an attack topology whereas the decoy servers are used to create attack flows (Paper-1).

Over the course of time, researchers also found out a way to mitigate the crossfire attack. They demonstrated that SDN can be leveraged to enable Moving Target Defense (MTD) to mitigate DDoS attacks. MTD is a concept of introducing dynamic change in a system in order to increase uncertainty and complexity for attackers. The crossfire attack can be prevented by either obfuscating the links during the potential link map creation of the attacker to make it harder to launch the attacks or by detecting and mitigating the network during attacks. These mechanisms rely on the abilities of SDN controller and the OpenFlow protocol (Paper-2).

References:

1. **Paper-1:** https://www.ieee-security.org/TC/SP2013/papers/4977a127.pdf
2. **Paper-2:** https://ieeexplore.ieee.org/abstract/document/7796857/