DDoS

Distributed Denial of Service

Analysis

Group 5
Mohammad Ahmad
Ryadh Almuaili

Outline

- Introduction
- Previous Work
- Approaches
- Design & Implementation
- Results
- Conclusion
- References

WHAT IS DDoS ?

- DDoS: Distributed denial of service attack

- Multiple compromised systems are used to target a single system to disrupt service
- Types of attacks
- Flooding system traffic which leads to service denial to legitimate users
- Connection disruption between two machines, thereby preventing access to a service
- Preventing a particular system or user from accessing a service

WHAT IS DDoS ?

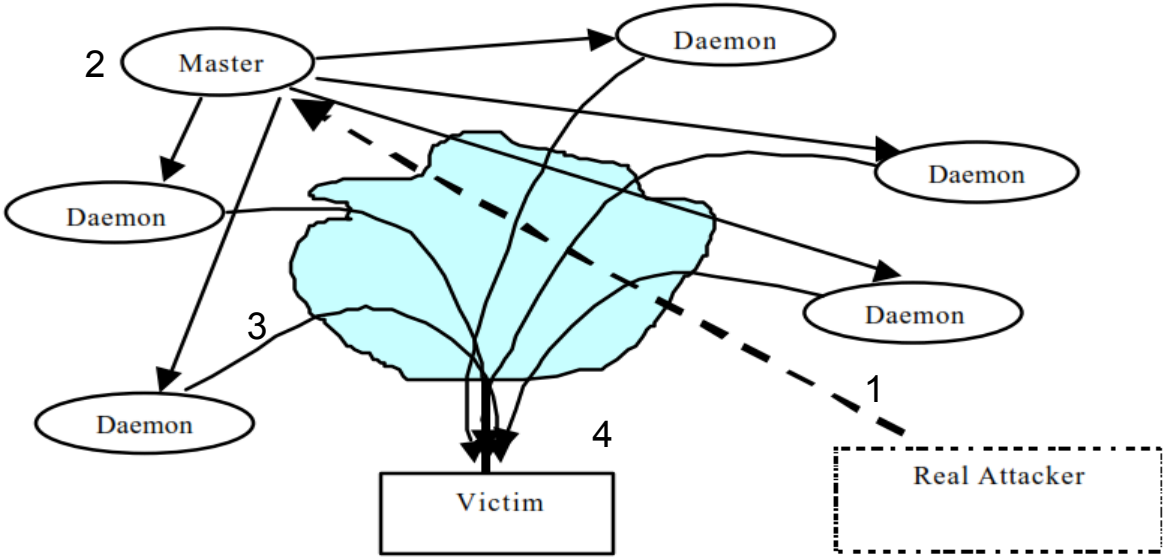


Figure 1: The four components of a distributed denial of service attack: a real attacker, a control master program, attack daemons and the victim

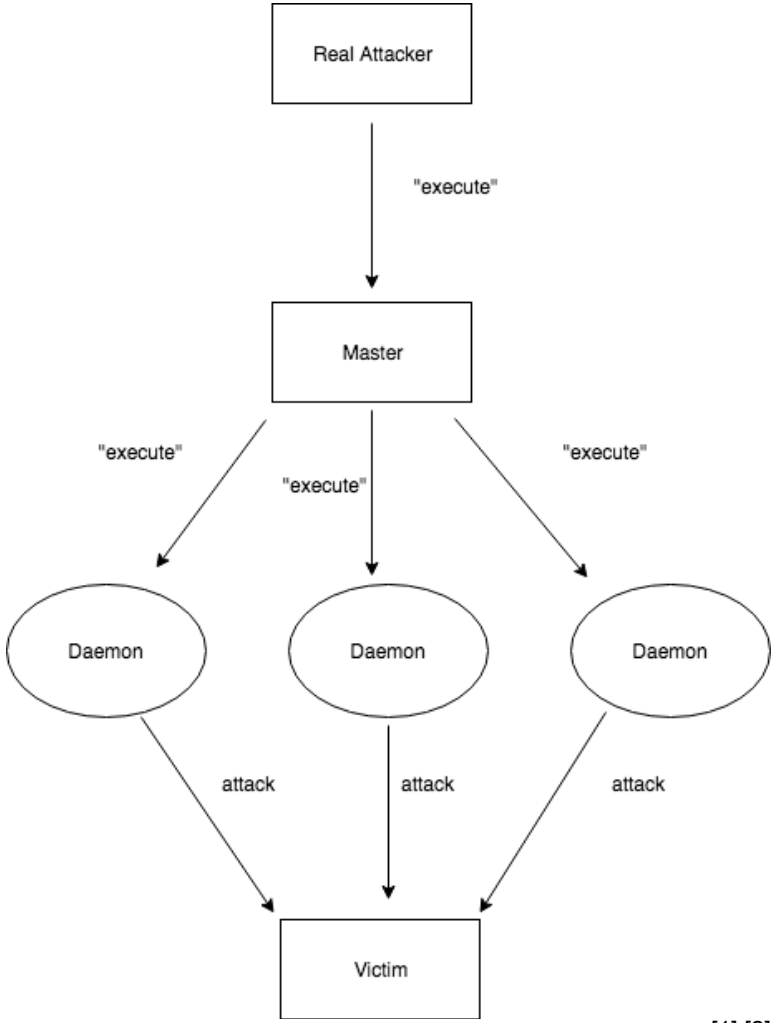
[1] [2]

WHAT IS DDoS ?

- A real attacker deploys daemon attack programs in multiple host computers, and deploys a master program ,that controls and coordinate the daemons, in another host computer.

- How is the attack initiated ?

- When the real attacker wants to launch an attack, an execute command is sent to the control master program which will then execute all the daemons under its control. After that, the daemons will attack the victim



[1] [2]

Previous Work

Two other projects that are comparable to ours are mentioned here.

The first paper [7] is published by professor Ljiljana Trajkovic and her peers in SFU, UoC and SPAWAR systems Center in San Diego, CA. This paper analyzes the attacks using different queueing algorithms.

The second project was done by previous ENSC 427 students, from Spring 2015 [8], where they analyzed the effect of using a black hole on a topology similar to the one used in this project

Attack methods

DoS techniques [2][3]

- Smurf -> ICMP
- SYN Flood -> TCP handshake
- **UDP Flood attack**
  - The attacker uses forged UDP packets to connect attacker and the victim.
  - Implemented exchange rate is designed to deplete the Bandwidth(BW) provided by the victim

DDoS Techniques

- Various methods to communicate between control master program and the attacker
- TFN, ICMP -> (any DoS)
- Stacheldraht, TFN with encrypted TCP in first stage
- **Trinoo**, TCP -> UDP Flood

Other complex variations.

User Datagram Protocol (UDP), Transmission Control Protocol(TCP),Tribe Flood Network(TFN), Internet Control Message Protocol(ICMP)

Prevention Methods

- Filtering Routers: Filtering all packets passing through the network, protects from attacks conducted from neighboring networks, and prevents the network itself from being an unaware attacker [3]
- Disabling IP Broadcasts: By disabling IP broadcasts, host computers can no longer be used as amplifiers in ICMP Flood and Smurf attacks
- Other common ways: [2]
    - Increase the size of the connection queue,
    - decrease the time-out waiting for the three-way handshake, and
    - employ vendor software patches to detect and circumvent the problem.
    - Modifying **queuing algorithm** in routers

Queuing Algorithms

- **DropTail:** Each packet is treated identically and when queue filled to its maximum capacity the newly incoming packets are dropped until queue have sufficient space to accept incoming traffic, finite FIFO. [2]
- **SFQ:** Hash to map traffic to queues. Provide fairness so that each client is able to send data in turn, thus preventing any single user from drowning out the rest. [5]
- **RED:** It operates on the average queue size and drop packets on the basis of statistics information. If the buffer is empty all incoming packets are acknowledged. As the queue size increase the probability for discarding a packet also increase. When buffer is full probability becomes equal to 1 and all incoming packets are dropped. [5]

Our Goal

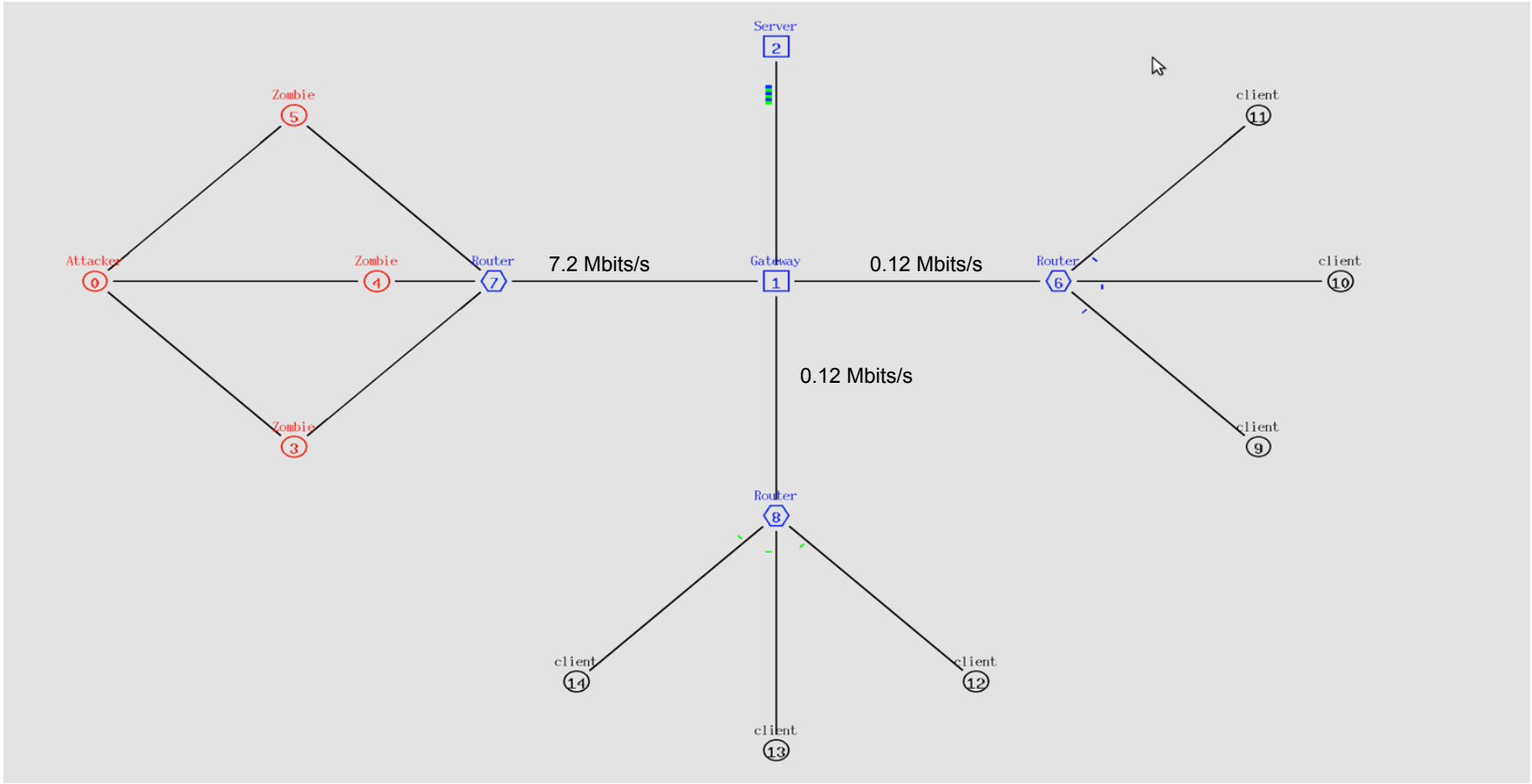
- Simulate a DDoS Scenario
- Software Tool
  - **ns-2** (network simulator)
- Attack Method
  - **UDP Flood**
    - **~Trinoo** DDoS Implementation
- Prevention:
  - Queuing algorithms
    - DropTail
    - SFQ
    - RED

Implementation

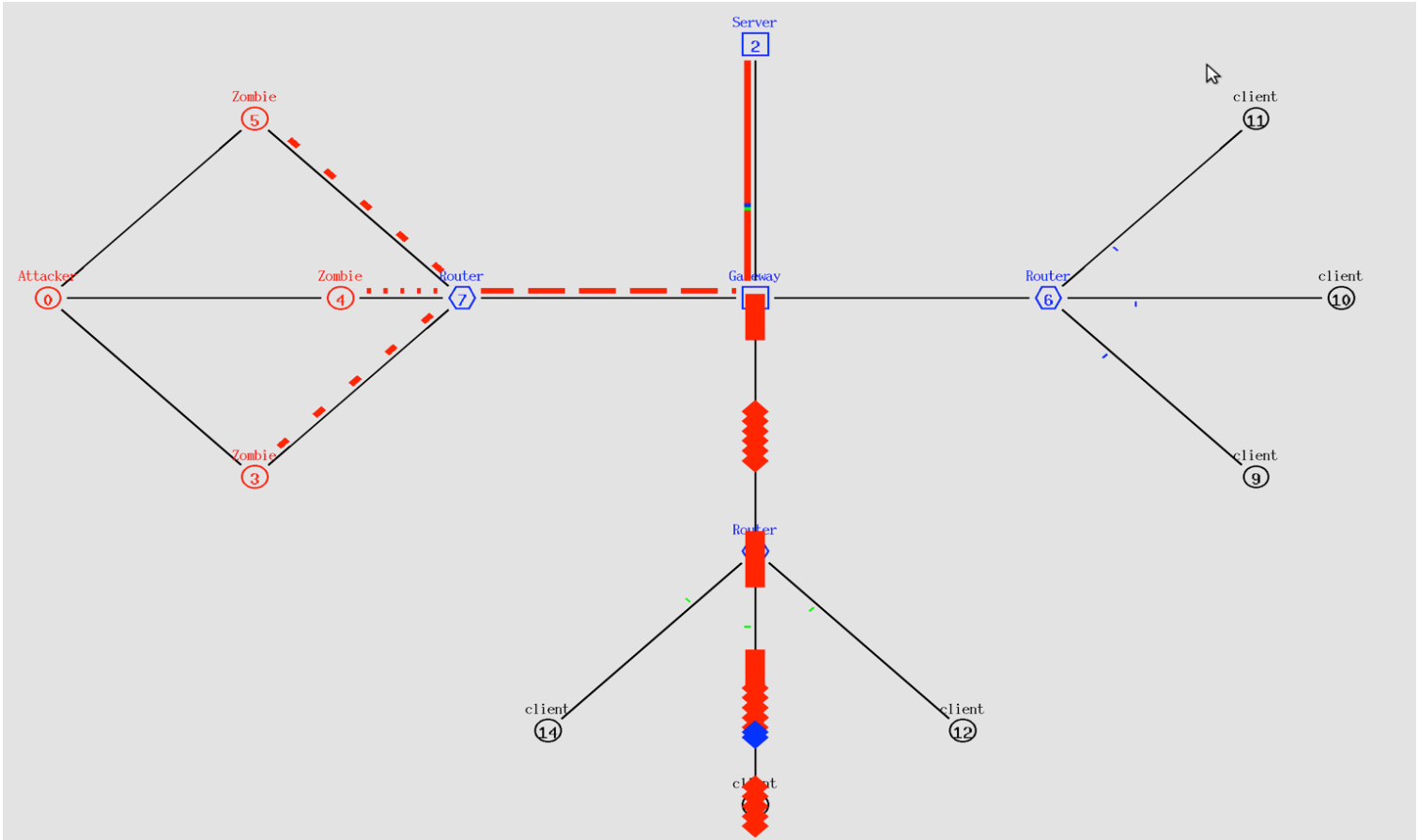
3 clusters of clients

- 1 Attacking
  - 1 Attacker
  - 3 Zombies (Daemons)
  - Rate: 2.4Mbps / Zombie: 7.2 Mbps total (Zombies -> Gateway)
  - Interval: 20ms
- 2 legitimate Clients
  - 3 each, 6 total
  - Rate: 0.04Mbps / client: 0.24 Mbps total (Clients-> Gateway)
  - Interval: 200ms
- Routers: 3 routers used to bridge the connection between clusters -> gateway
- Links
  - 100ms delay on 10Mbps all except gateway to server, 5Mbps

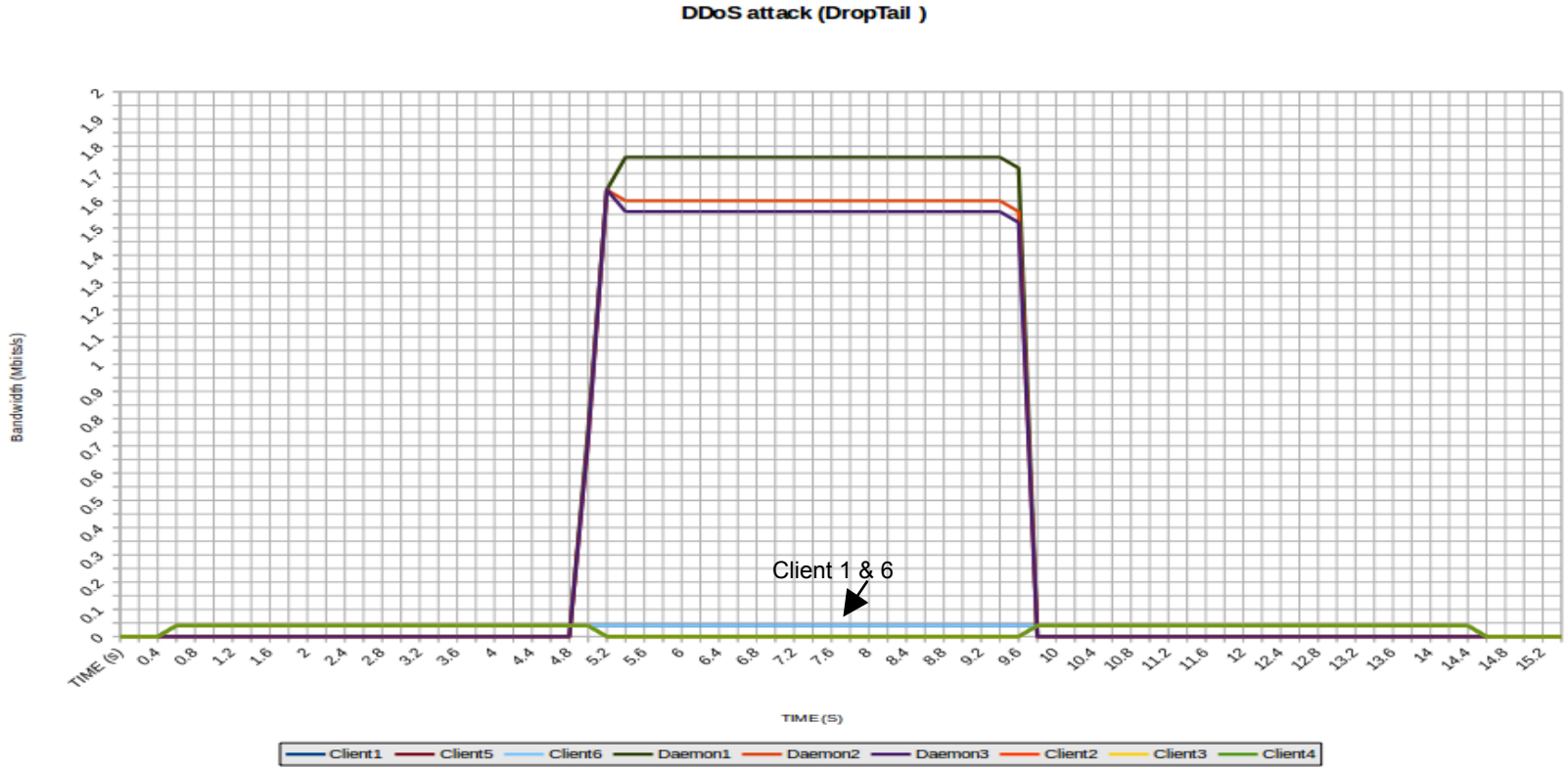
Topology (Before attack)



Topology (During attack)

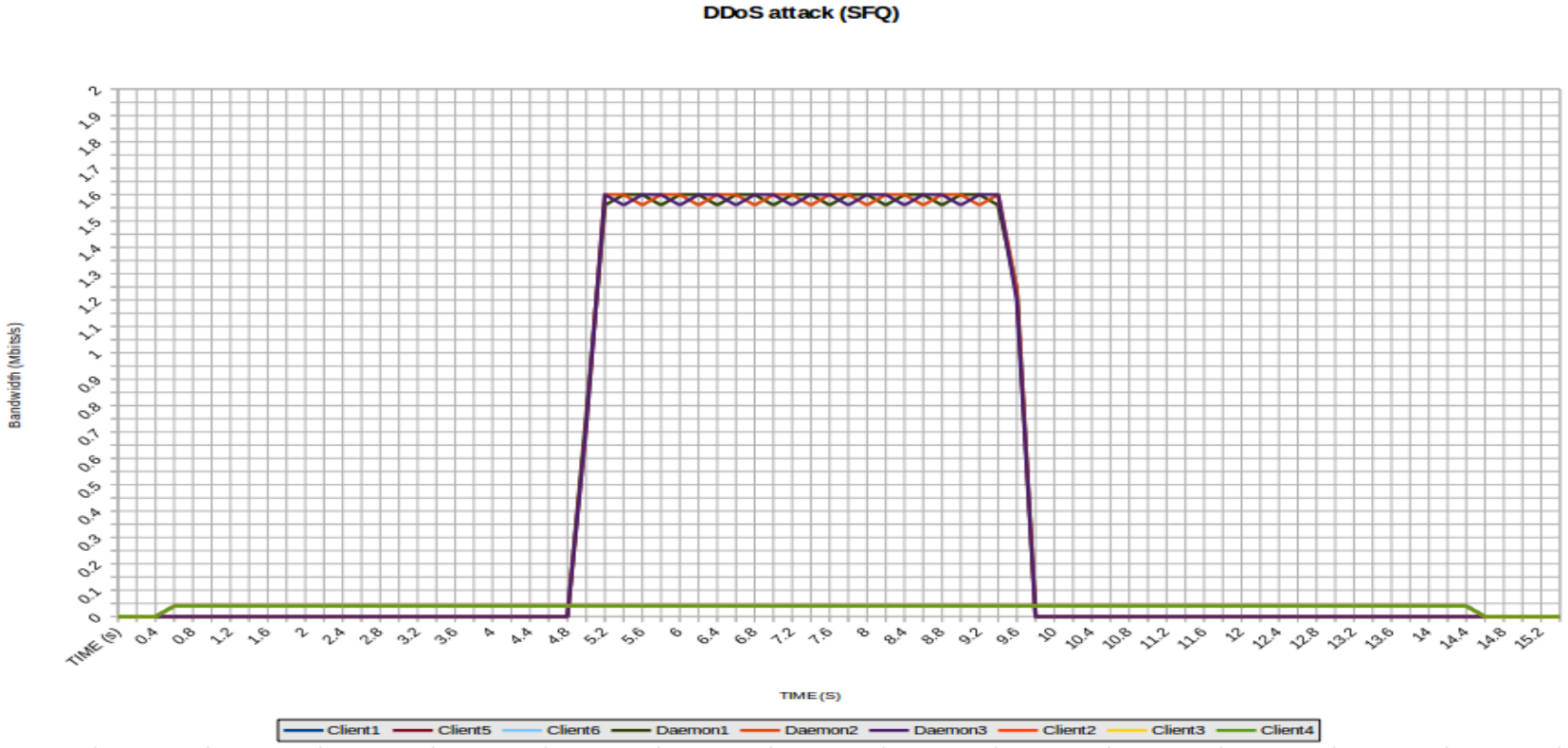


Results (QUEUE TYPE : DropTail)



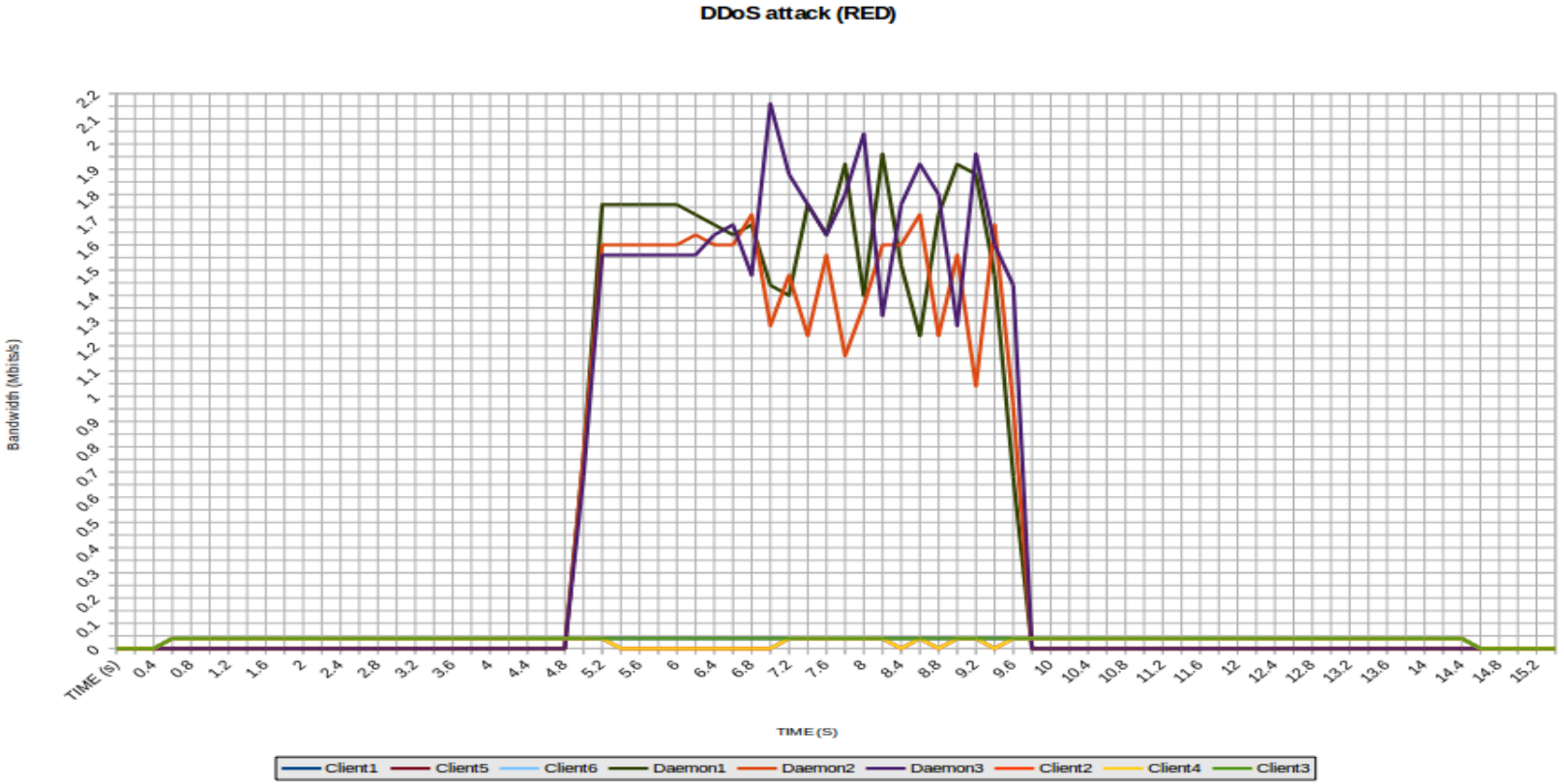
Attack : 4.8s < t < 9.4s

Results (QUEUE TYPE : SFQ)



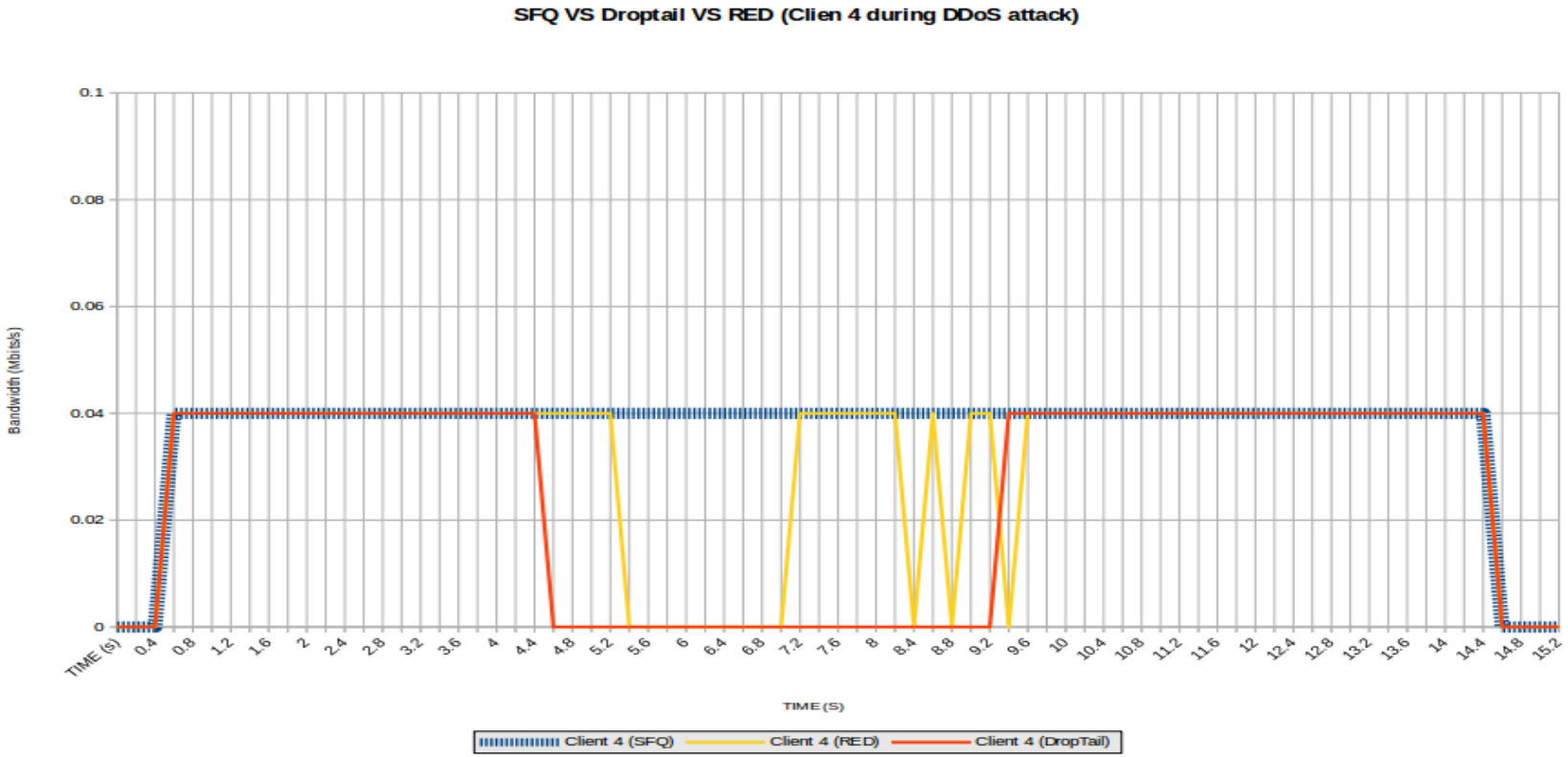
Attack : 4.8s < t < 9.4s

Results (QUEUE TYPE : RED)



Attack : 4.8s < t < 9.4s

Results (SFQ VS RED VS DropTail)



Attack : 4.8s < t < 9.4s

Scope of Future Work

- Simulate larger network with more realistic components.
- Implement different types of DDoS attacks.
- Implement different preventions techniques and determine which once are more useful to implement in a giving application.

Conclusion

- We tested three different queueing algorithms.
- Worst to Best:
  - Droptail: Queue filled up very quickly, and it drop all incoming packets.
  - RED: Sporadic bandwidth to users, significant improvement over Droptail.
  - SFQ: Best queue so far, no measurable drops in BW for any of the connected users.

References

- [1]S. Bellovin, “Distributed denial of service attacks,” Feb. 2000,http://www.research.att.com/~smb/talks
- [2]F. Lau, S. H. Rubin, M. H. Smith, and Lj. Trajkovic, "Distributed denial of service attacks," (invited paper) in Proc. IEEE Int. Conf. on Systems, Man, and Cybernetics, SMC 2000, Nashville, TN, Oct. 2000, pp. 2275-2280
- [3]D. Dittrich, “The DoS project's ‘Trinoo’ distributed denial of service attack tool,” Oct. 1999; “The ‘Stacheldraht’ distributed denial of service attack tool,” Dec. 1999; “The ‘Tribe Flood Network’ distributed denial of service attack tool,” Oct. 1999, http://www.washington.edu/People/dad.
- [4] P. Ferguson and D. Senie, “RFC 2267: Network ingress filtering: defeating denial of service attacks which employ IP source address spoofing,” Jan. 1998, http://info.internet.isi.edu/innotes/rfc/files/rfc2267.txt
- [5] Kuznetsov, Alexey. "Tc-Sfq(8) - Linux Man Page". *Linux man page*. N.p., 2017. Web. 3 Apr. 2017.
- [6] "Working Mechanism Of FQ, RED, SFQ, DRR And Drop-Tail Queues - Network Technologies (TCP/IP Suite)". *Sites.google.com*. N.p., 2017. Web. 3 Apr. 2017.

References

- [7] F. Lau, S. H. Rubin, M. H. Smith, and Lj. Trajkovic, "Distributed denial of service attacks," (invited paper) in Proc. IEEE Int. Conf. on Systems, Man, and Cybernetics, SMC 2000, Nashville, TN, Oct. 2000, pp. 2275-2280

- [8] S. Chow, T. Sherpa and S. Hoque, “Performance analysis during a DDoS attack”, http://www.ensc.sfu.ca/~ljilja/ENSC427/Spring15/Projects/team8/ENSC427_team8_report.pdf, April 2015.