Performance analysis of a system during a DDoS attack

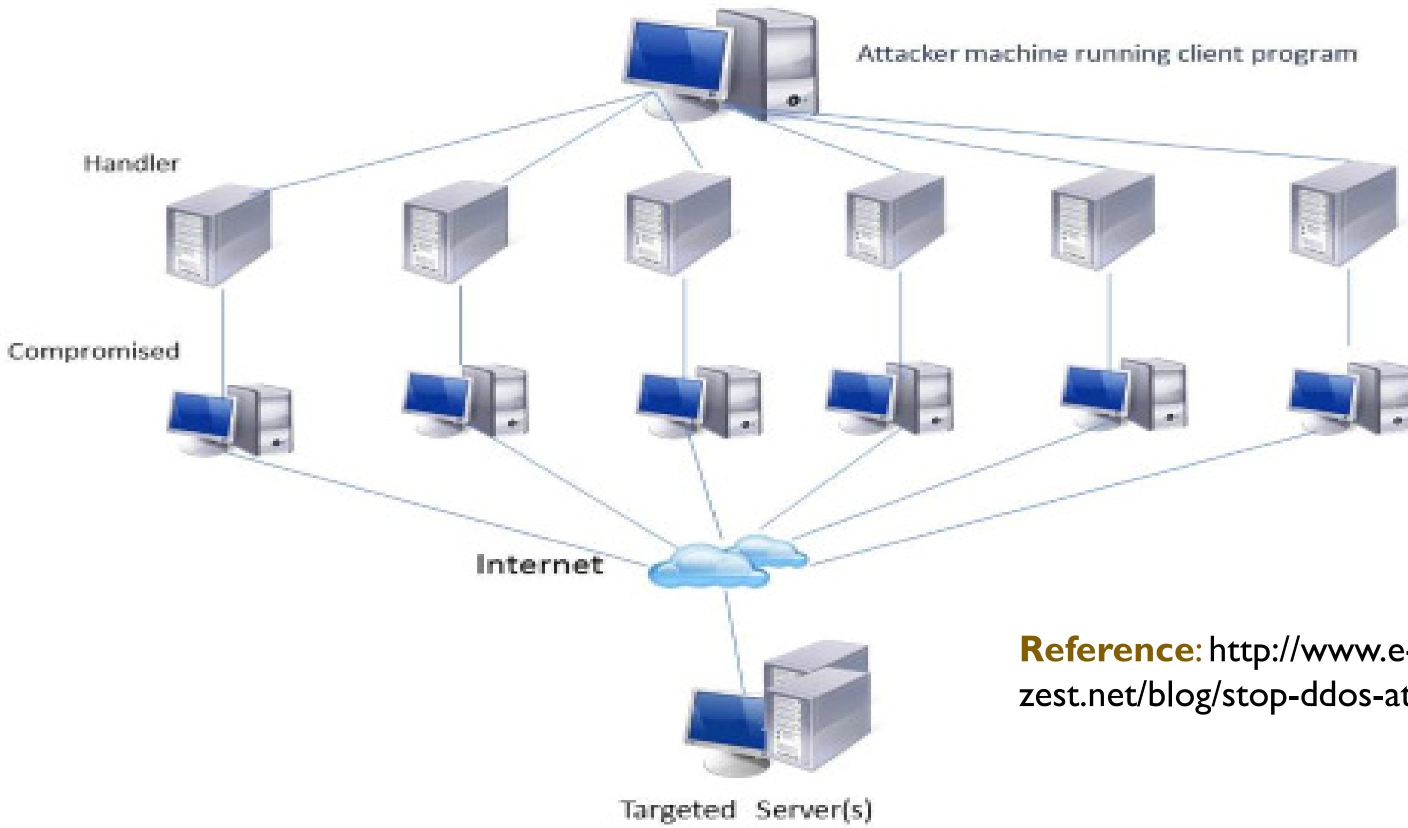
ENSC 427 Communications Network
Spring 2015
Group 8
http://www.sfu.ca/~spc12/

Samuel Chow <spc12 at sfu.ca>
Tenzin Sherpa <tserpa at sfu.ca>
Sam Hoque <shoque at sfu.ca>

What is DDoS?

- **DDoS**: Distributed Denial of Service.
- Denies service to users by interrupting or suspending services of a host connected to the Internet.
- DDoS and DoS are different: DDoS involves multiple attackers while DoS involves one, thus the term "Distributed".
- Attacker employs zombies/botnets (infected computers) to initiate attack.
- More zombies result in larger attacks.

What is DDoS?



Reference: http://www.e-zest.net/blog/stop-ddos-attacks/

Figure 1: A conceptual diagram of a DDoS attack.

Types of DDoS

- **Reflection Attack**: Attacks the challenge-response authentication system (IP spoofing).
- **SYN Flood**: Exploits the vulnerability of 'three-way handshake' principle of a TCP connection.
- **Slowloris**: Holds as many connections to the target web server open for as long as possible by sending partial requests.
- **Zero-day DDoS Attack**: Unknown or new attacks. No prevention technique is known yet. A popular term among the hacking community.

Why is DDoS Important?

- DDoS occurs everyday.
- According to a 2013 Neustar survey result, DDoS attacks cost businesses $100,000 per hour in average.
- This cumulates to an extraordinary $1 million in losses before an internet-reliant company even starts to mitigate the attack.
- Apart from the financial losses, a DDoS attack can lead to erosion of brand value of a company, skyrocketing operational costs, and a need to invest in new people and advance technologies to manage the risk better in the future.

DDoS example

- Spamhaus (a non-profit anti-spam organization) was under a DDoS attack on March 19, 2013.
- Over 100 Gbps of data were demanded from their servers.
- CloudFlare was asked to help prevent the DDoS attack.
- CloudFlare made heavy use of 'Anycast'. It announced Spamhaus' IP address to 23 worldwide data centers.
- This diluted the attacker's impact and reduced the bottleneck.
- This attack almost took the Email services down.

Prevention Techniques

- **Null route (Black hole)**: Tells the system to drop network communication from a malicious IP addresses.
- **DNSBL**: Publishes lists of IP addresses known to be involved in spamming or potentially harmful activities that can negatively impact a user.
- **SYN Proxy**: All connection requests are screened and only legitimate requests are forwarded.
- **White list, black list**: Based on the location of an IP address on either of these lists, services will be accordingly allowed or denied.

Simulation Scenarios

- **DDoS Attack Type**: Reflection Attack.
- **DDoS Prevention Technique**: DNSBL (DNS Blacklist) and 'Null route'.
- **Platforms**: ns-2, X-graph, Ubuntu 14.04 LTS.
- **Two Scenarios**:

  One: One attacker, three zombies, and six clients.

  Two: One attacker, three zombies, six clients, and one ‘Black hole’.

Simulation Parameters

- **Data Rates**:
  Clients: 50 bytes at 0.5 Mbps
  Zombies: 50 bytes at 5 Mbps
  Attacker: 50 bytes at 0.01 Mbps
- **Agent**: UDP
- **Application**: Constant Bit Rate (CBR)
- **Queue**: Drop tail
- **Delay**: 10 ms
- **Bandwidth**:
  Client to Gateway: 45 Mbps (T3 connection)
  Zombie to Gateway: 45 Mbps (T3 connection)
  Gateway to Server: 12.5 Mbps

ns-2 Simulation Topologies

Scenario 1:

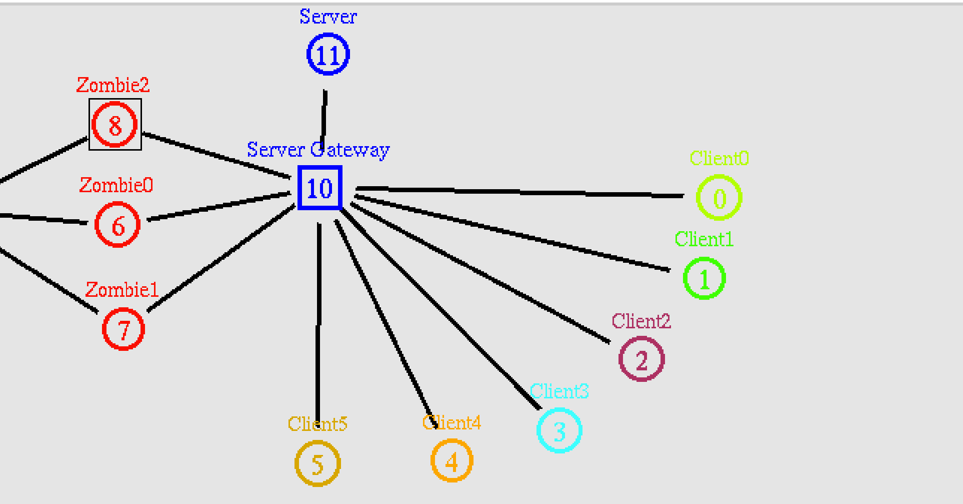


Figure 2: A DDoS attack involving one attacker, three zombies, and six clients.

Scenario 2:

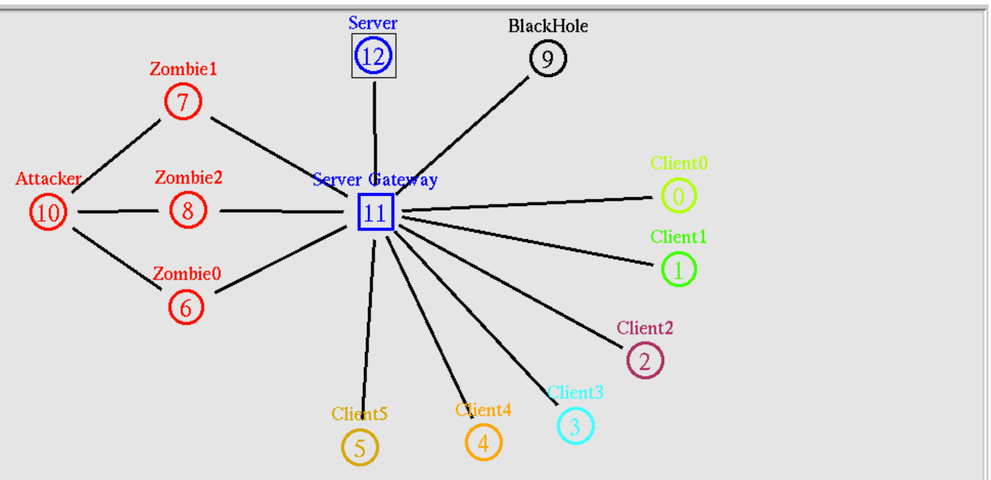


Figure 3: A DDoS attack involving one attacker, three zombies,, six clients, and one 'Black hole'.

Simulation Run Time

- **0s < t < 10s**: No traffic sent.
- **10s < t < 19.9s**: Clients send data to server and data reach server.
- **t = 19.9s**: Attacker sends data to zombies to begin the DDoS attack.
- **20s < t < 40s**: DDoS occurs and clients' data rate drop.
- **t = 39.9s**: Attacker sends data to zombies to stop the DDoS attack.
- **t = 40s**: DDoS stops and clients' data reach the server again.
- **t = 50s**: All traffic stops.

Scenario One

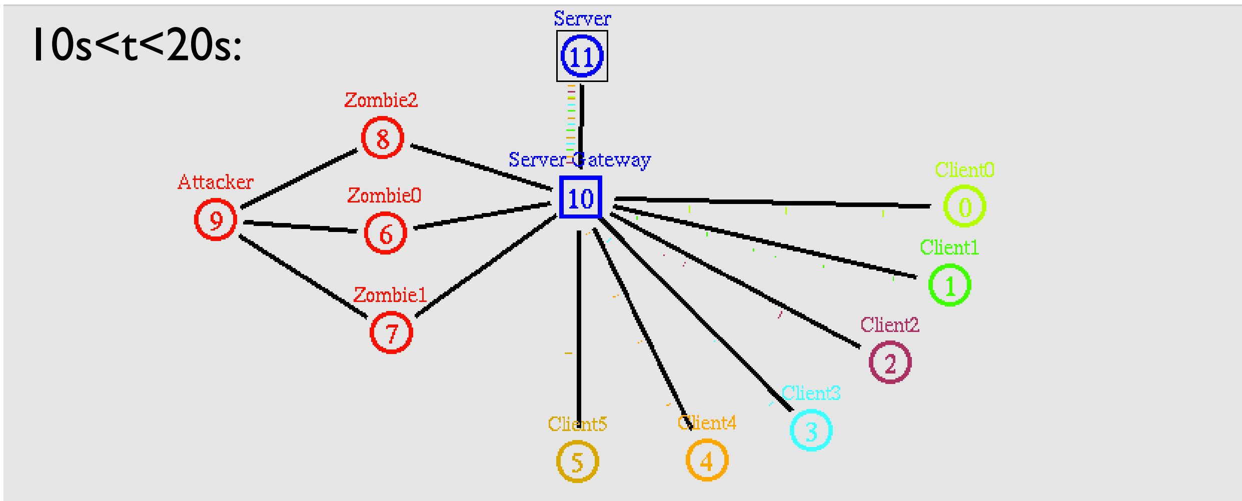


Figure 4: Clients' data flow to the server is successful (10s<t< 20s).

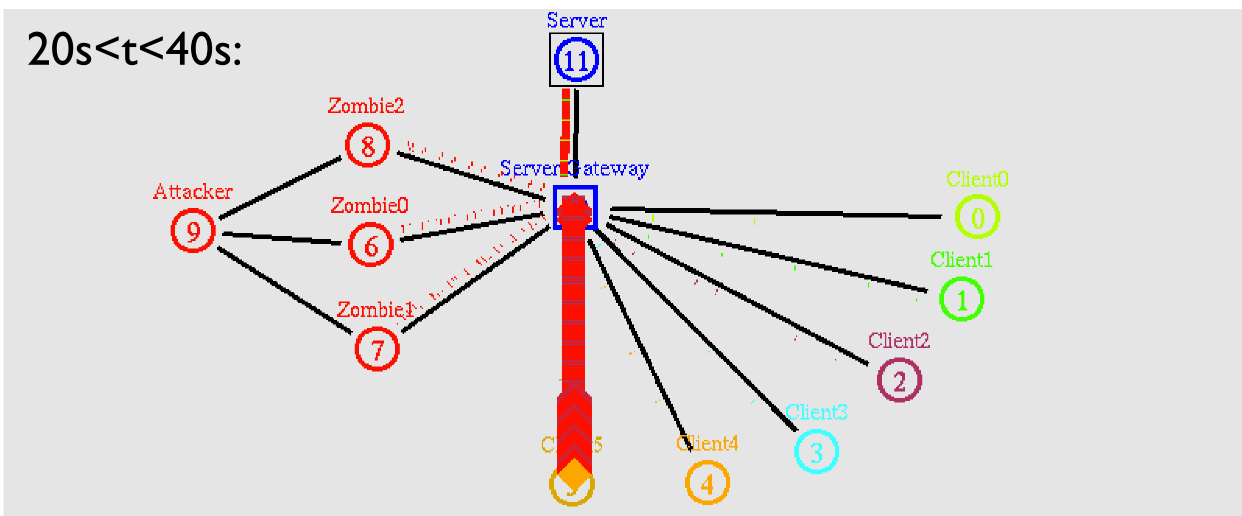


Figure 5: Clients' data flow to the server is unsuccessful (20s<t< 40s).

Scenario One

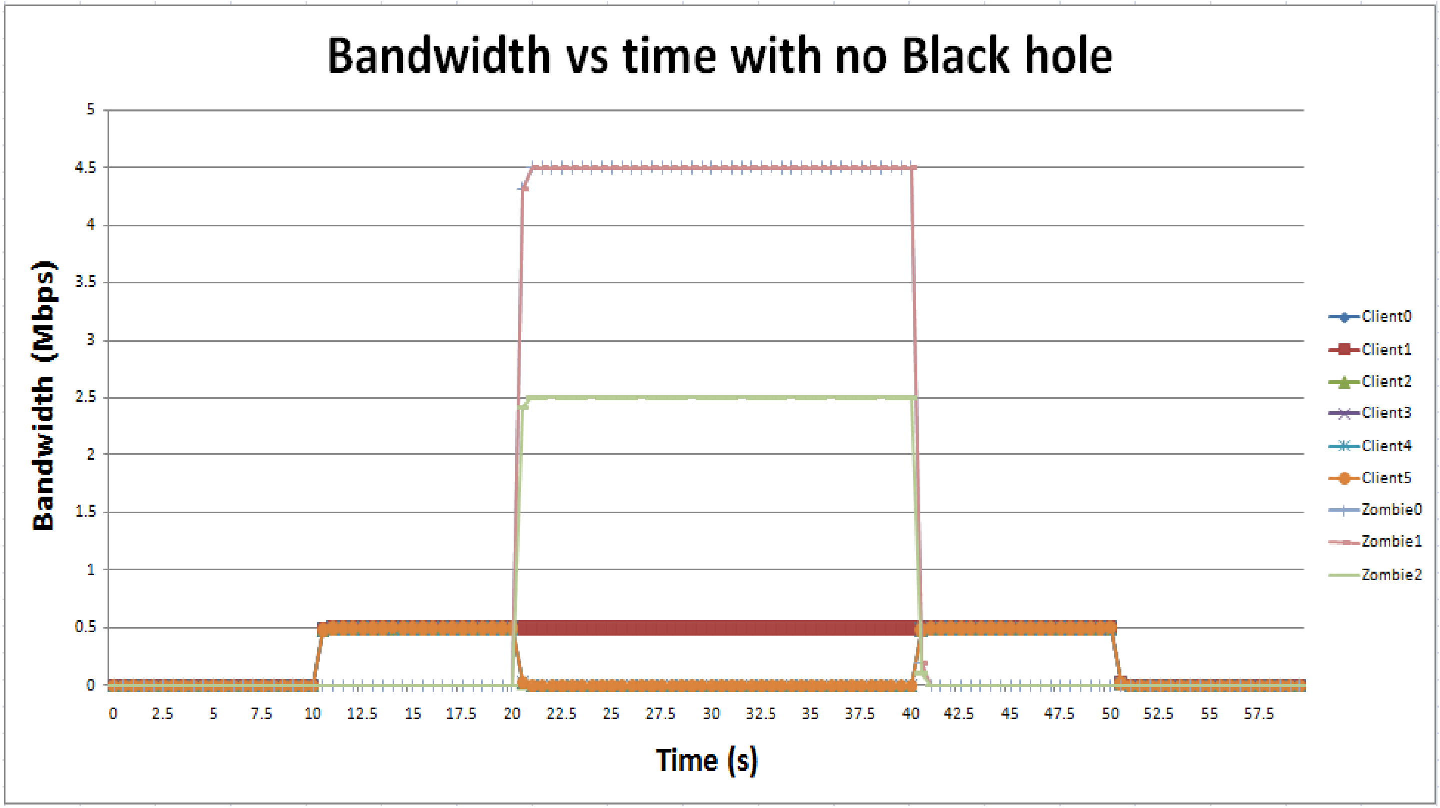


Figure 6: 'Bandwidth vs. time' graph of a DDoS attack (0s<t<60s).

Scenario One

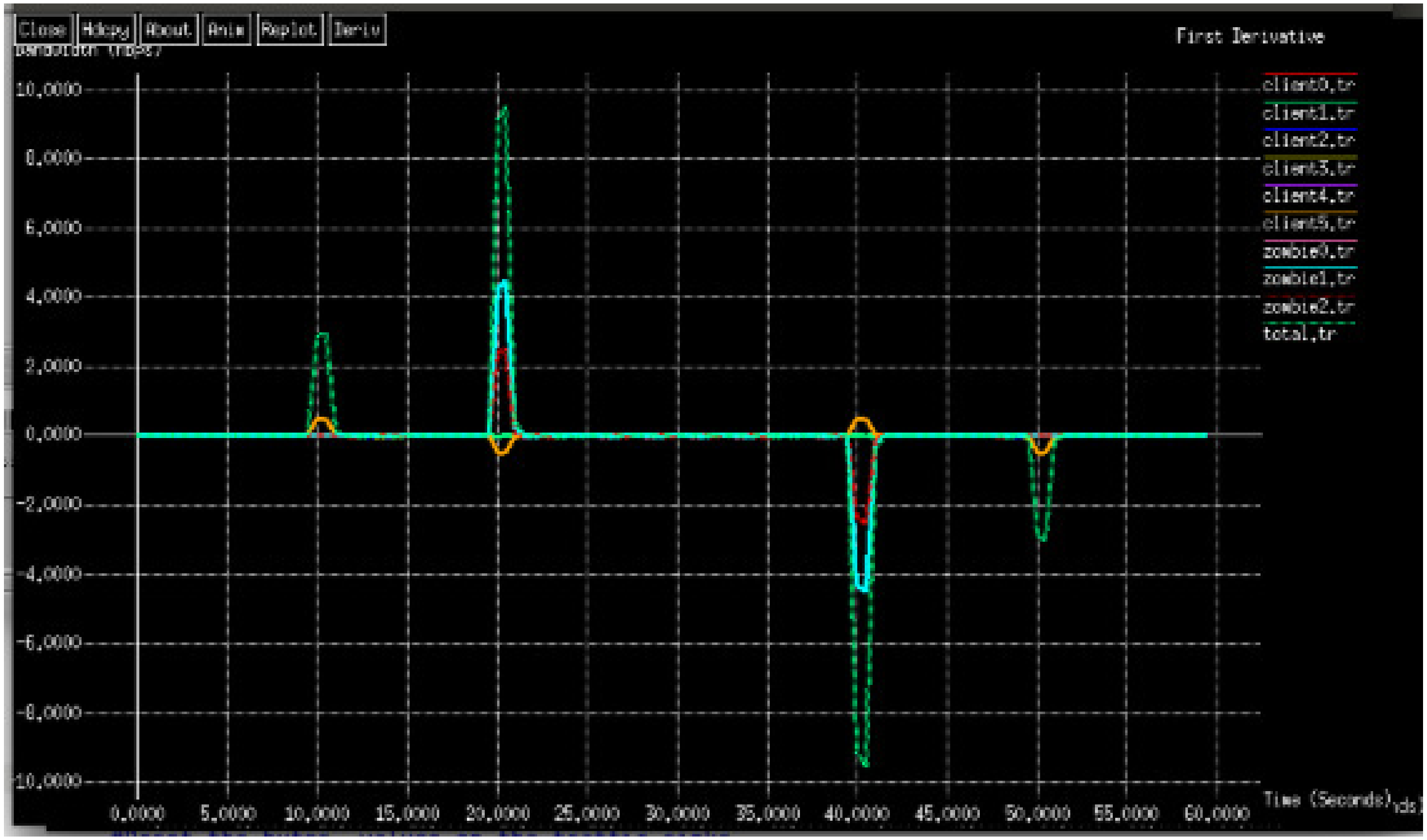


Figure 6: First derivative of the 'bandwidth vs. time' graph of a DDoS attack (0s<t<60s).

Scenario Two

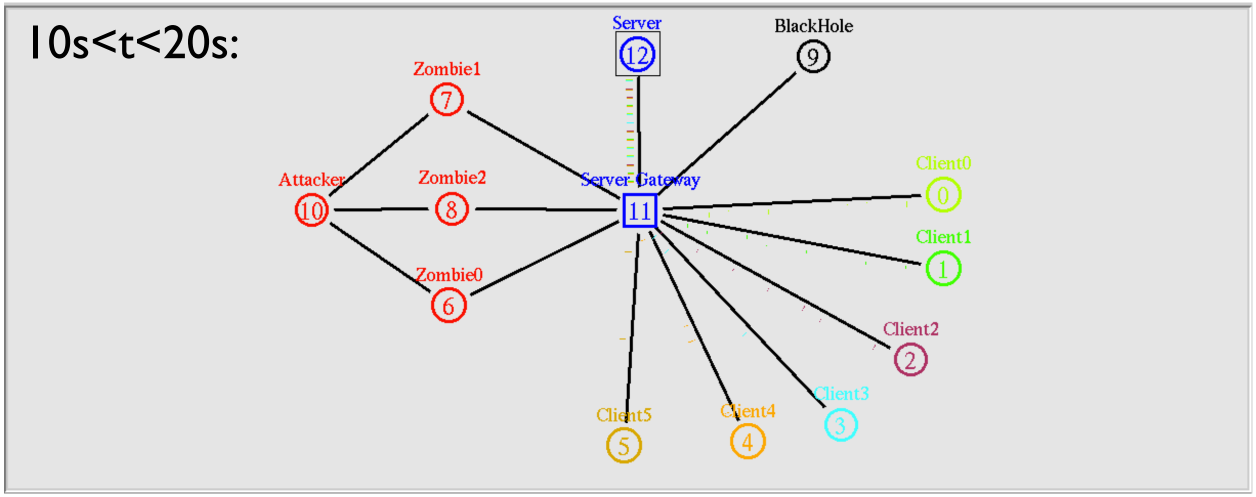


Figure 7: System with 'Black hole' prevention technique (10s<t< 20s).

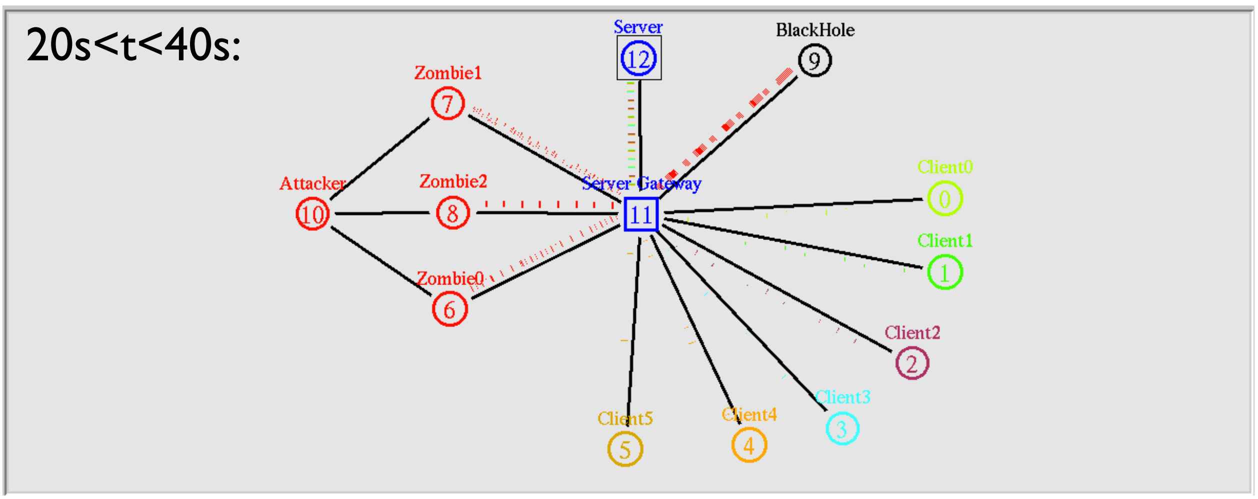


Figure 8: Successful prevention of DDoS attack using a 'Black hole' (20s<t<40s).

Scenario Two

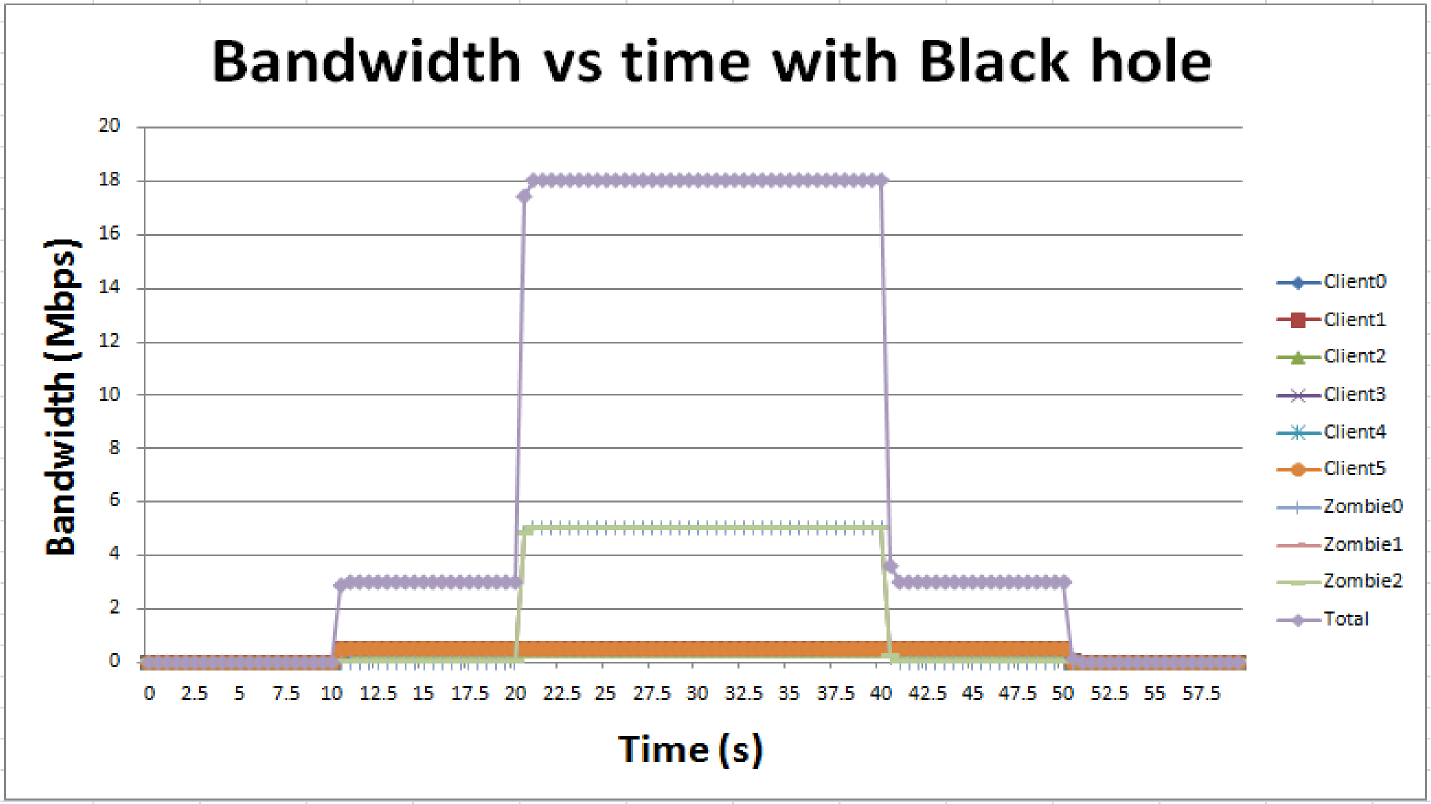


Figure 9: 'Bandwidth vs. time' graph using 'Black hole' prevention technique (0s<t<60s).

Scenario Two

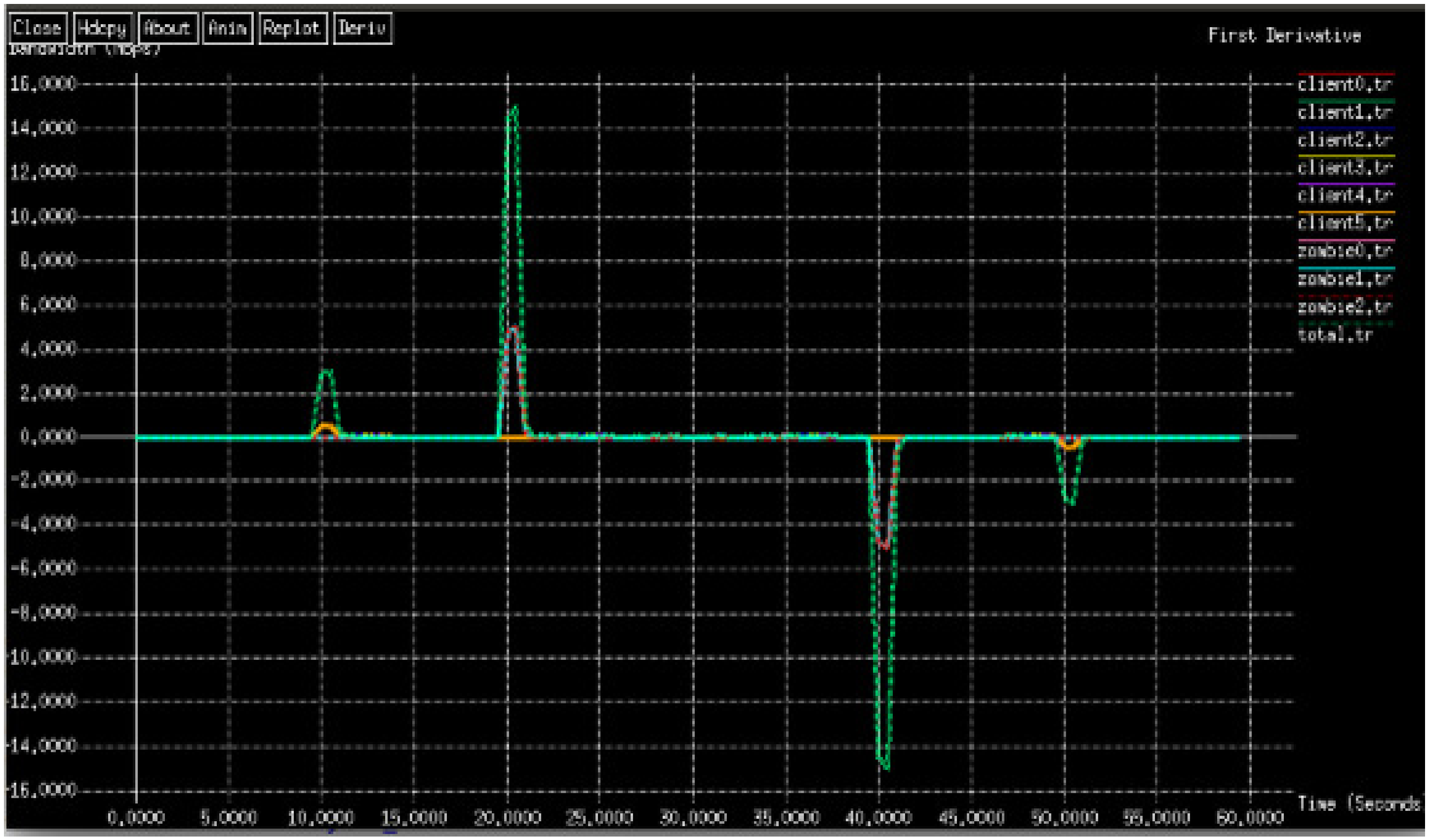


Figure 10: First derivative of the 'Bandwidth vs. time' graph using 'Black hole' prevention technique (0s<t<60s).

Comparison of Drop tail and SFQ

- **SFQ**: Stochastic Fair Queuing method.
- **Definition**: Uses a hashing algorithm to divide the traffic over a limited number of FIFO queues while being almost perfectly fair.
- **Simulation**: Keeping the same topologies of one attacker, three zombies, six clients, we simulated the DDoS attack again using SFQ method. The run times were also kept exactly the same.

Comparison of Drop tail and SFQ

- **Data Rates**:

  Clients 0: 50 bytes at 0.1 Mbps
  Clients 1: 50 bytes at 0.2 Mbps
  Clients 2: 50 bytes at 0.3 Mbps
  Clients 3: 50 bytes at 0.4 Mbps
  Clients 4: 50 bytes at 0.5 Mbps
  Clients 5: 50 bytes at 0.6 Mbps
  Zombie 0: 50 bytes at 4.0 Mbps
  Zombie 1: 50 bytes at 5.0 Mbps
  Zombie 2: 50 bytes at 6.0 Mbps
  Attacker: 50 bytes at 0.01 Mbps

Comparison of Drop tail and SFQ

- **Agent**: UDP
- **Application**: Constant Bit Rate (CBR)
- **Queue**: SFQ
- **Delay**: 10 ms
- **Bandwidth**:
  Client to Gateway: 45 Mbps (T3 connection)
  Zombie to Gateway: 45 Mbps (T3 connection)
  Gateway to Server: 12.5 Mbps

Comparison of Drop tail and SFQ

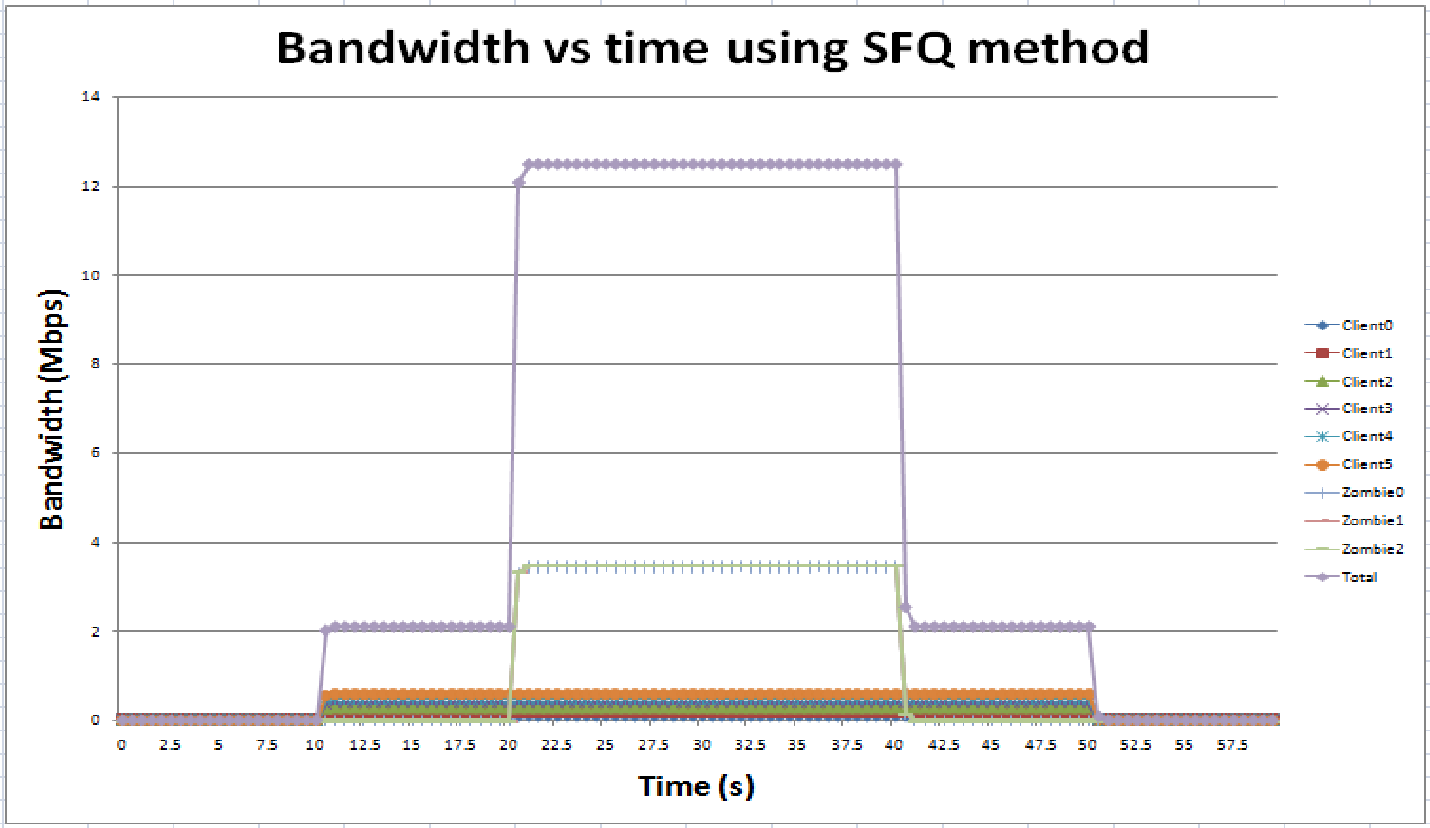


Figure 11: 'Bandwidth vs. time' graph using SFQ method (0s<t<60s).

Scope of future work

- Using Drop tail queuing method, change the data rates of the clients and observe their effects on the DDoS attack with and without a 'Black hole‘.
- Using SFQ queuing method, change the data rates of the clients and zombies and observe their effects on the DDoS attack.
- Using SFQ queuing method, initiate data transfer from a client after the DDoS attack to verify FIFO mechanism.
- Complete writing of C++ code in ns-2 to create a new agent/application model of DDoS attacks.

Scope of future work

- Simulate larger, more realistic models of DDoS attacks using more network components.
- Simulate different DDoS attacking methods and compare their impacts.
- Compare the effectiveness of other prevention techniques.
- Create scenarios with other queuing disciplines and compare their performances.

Conclusion

- We identified what a DDoS attack is and the numerous varieties of a DDoS attack.
- We simulated a simple Reflection method DDoS attack on a client-server model in ns-2 and noted its effects.
- 'Black hole' prevention technique was a robust measure in nullifying the threat of this DDoS attack.
- We also compared Drop tail and SFQ methods and their impacts on a DDoS attack.
- Our research has paved the way for more future work in this field.

References

[1] 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.

[2] X. Rui, M. W. Li, and Z. W. Ling, "SYN flooding detecting using negative selection algorithm based on eigen value sets," May 2009, [Online]. Available: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=5138099

[3] M. Blagov, "DDoS Definition," [Online]. Available: https://www.incapsula.com/ddos/ddos-attacks/

[4] M. Greis, "Tutorials for the Network Simulator 'ns'," [Online]. Available: http://www.isi.edu/nsnam/ns/tutorial/

[5] P. White, "How much traffic can a single server handle," Mar. 2011, [Online]. Available: http://blog.whitesites.com/How-much-traffic-can-a-single-server-handle__634363981032706250_blog.htm

[6] M. Prince, "The DDoS that knocked SpamhausOffline (And how we mitigated it)," Mar. 2013, [Online]. Available: https://blog.cloudflare.com/the-ddos-that-knocked-spamhaus-offline-and-ho/

[7] A. S. Tanenbaum, "Authentication Protocols" in*Computer Networks*, 4th edition, New Jersey, Prentice Hall, 2003, ch.*8*, sec. *7*, pp. 787-790.

References

[8] Computer Emergency Response Team (CERT) for the Software Engineer Institute, "Denial of Service Attacks," 1997, [Online]. Available: https://www.cert.org/information-for/denial_of_service.cfm?

[9] The Anti-Abuse Project, "DNS blacklists," [Online]. Available: http://www.anti-abuse.org/dns-blacklists/

[10] B. Cane, "Mitigating DoS attacks with a null (or black hole) route on Linux," Jan. 2013, [Online]. Available: http://bencane.com/2013/01/14/mitigating-dos-attacks-with-a-null-or-blackhole-route-on-linux/

[11] Global Dots, "DDoS mitigation," [Online]. Available: http://www.globaldots.com/knowledge-base/ddos-mitigation/

[12] E. Ahmed, "Working Mechanism of FQ, RED, SFQ, DRR and Drop-Tail Queues," [Online]. Available: https://sites.google.com/a/seecs.edu.pk/network-technologies-tcp-ip-suite/home/performance-analysis-of-impact-of-various-queuing-mechanisms-on-mpeg-traffic/working-mechanism-of-fq-red-sfq-drr-and-drop-tail-queues

[13] US Department of Homeland Security, "DDoS quick guide," Jan. 2014, [Online]. Available: https://www.us-cert.gov/sites/default/files/publications/DDoS%20Quick%20Guide.pdf