ENSC 427: Communication Networks

Spring 2024

Final Project Presentations

A Simulation Study of DDoS Attacks on Networks

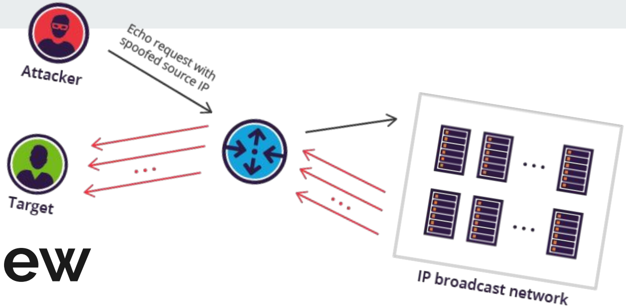
https://elainexluu.github.io/ensc427ddos

Spring 2024

By: Elaine Luu (301392121) - ela64@sfu.ca
Akash Malhi (301393341) - asm19@sfu.ca
Gurnek Ghatarora(301394646) - gghataro@sfu.ca
Group #8

Content

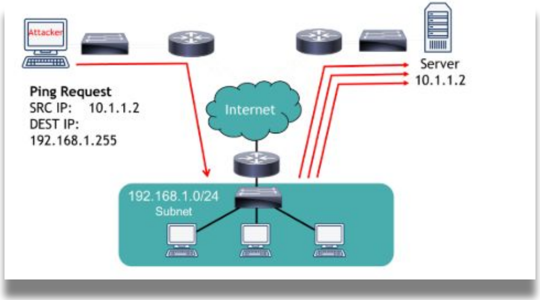
- ➢ Introduction
- ➢ High Level Overview
- ➢ Overview of Related Work
- ➢ Overview of Software Used
- ➢ Implementation
- ➢ Discussion and Limitations
- ➢ Organization and Time Management
- ➢ Contributions



Introduction: Motivation and Overview

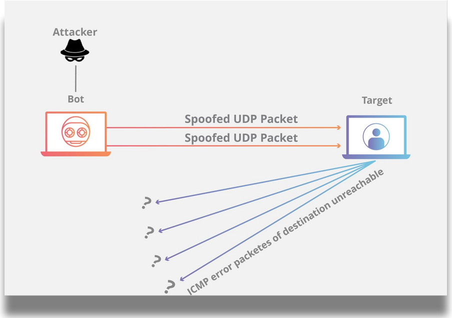
- **Objective**: Simulating a Distributed denial-of-service (DDoS) attack on wired networks
- **Motivation**: Curiosity on how traffic would behave in reaction to DDoS attacks
  - Main scope of project implemented by NS-3 which will be used to simulate DDoS attacks and analyze the negative effects it causes to services for a client
  - Comparisons of performance
- **Overview**: By deliberately creating attacks, different performance measures such as throughput, packet loss, and checksum
  - Acquire insight and create possible countermeasures for the different types of DDoS attacks
  - Efficient algorithms, techniques and procedures can be determined to counteract attacks

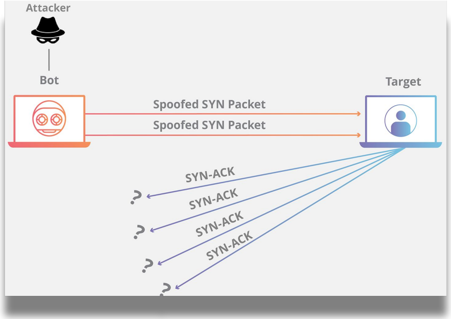
What is DDoS?



- ➢ A Distributed Denial of Service (DDoS) attack is a malicious attempt to disrupt the regular flow of traffic within a server/network by flooding it with a high amount of traffic.

- ➢ DDoS Attack Methods
  - ○ Smurf
  - ○ SYN Flood
  - ○ UDP Flood



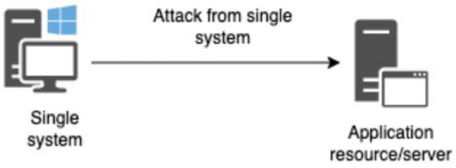


DoS and DDoS Differences

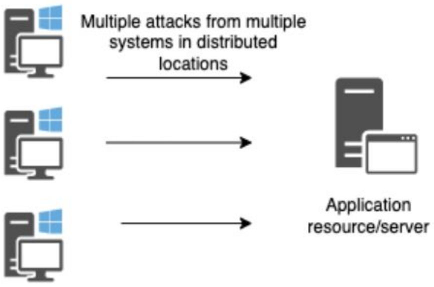
- ➢ DoS and DDoS are both forms of cyber attacks which attempts to intrude the regular flow of traffic within a server/network.

DoS	DDoS
Single, small groups of systems are used as attackers	Multiple, compromised systems are used as attackers
Causes disruption in a smaller scale due to limited resources	Causes disruption at a larger scale
Attacks typically require less preparation and originate from a single source, it may be easier to identify the attacker's IP address	Attacks require more preparation due to their distributed nature. Recovery from DDoS attacks is often more challenging and time-consuming

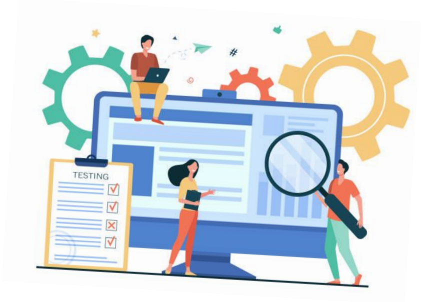
DoS attack

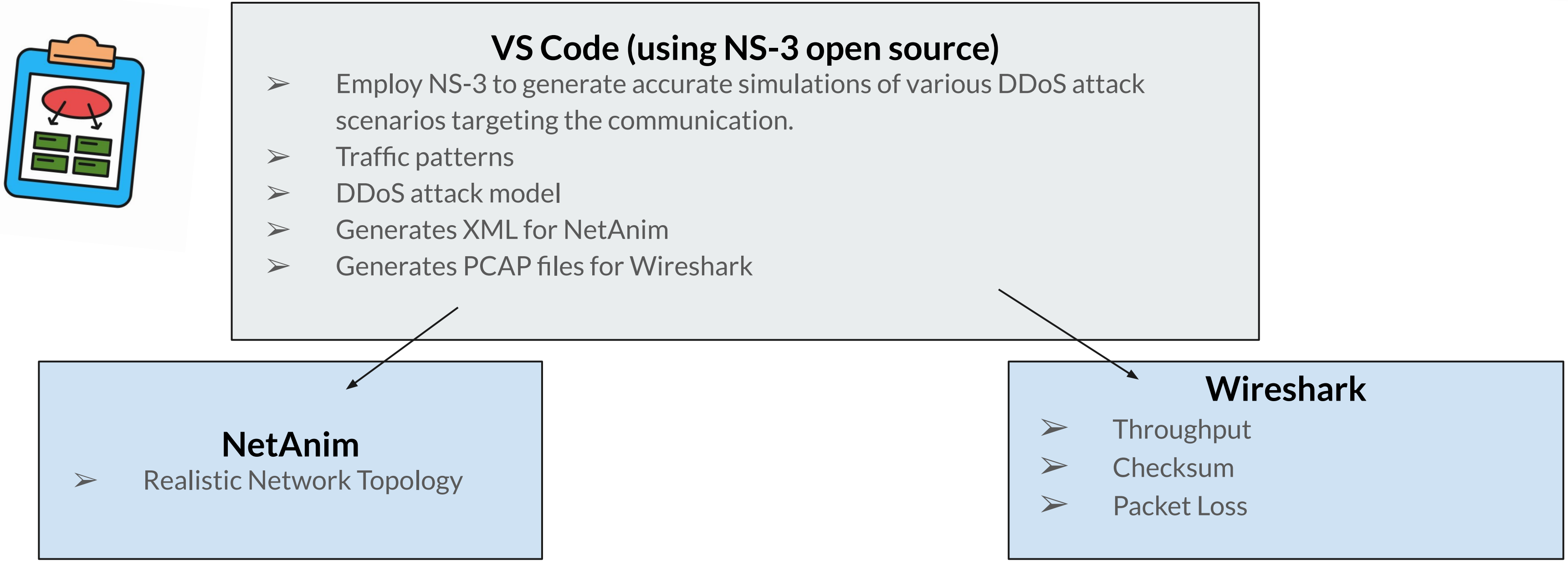


DDoS attack


Multiple attacks from multiple systems in distributed locations
Application resource/server

High Level Overview





VS Code (using NS-3 open source)

- ➢ Employ NS-3 to generate accurate simulations of various DDoS attack scenarios targeting the communication.
- ➢ Traffic patterns
- ➢ DDoS attack model
- ➢ Generates XML for NetAnim
- ➢ Generates PCAP files for Wireshark

NetAnim

- ➢ Realistic Network Topology

Wireshark

- ➢ Throughput
- ➢ Checksum
- ➢ Packet Loss

Overview of Related Work

1. Paper: Using Graphic Network Simulator 3 for DDoS Attacks Simulation
   a. Discusses the applications of a specific approach to simulating the performance of an HTTP server within a typical enterprise network under DDoS attack using Graphical Network Simulator-3.
   b. Focuses on understanding how an HTTP server behaves and performs under adverse conditions, allowing for the evaluation of potential vulnerabilities and the effectiveness of mitigation strategies
2. Paper: Modeling distributed denial of service attack in advanced metering infrastructure
   a. Explores the idea of a DDoS cyber attack on an advanced metering infrastructure (AMI). AMI essentially allows two-way communication between utilities and users, and allows remote communication between smart household appliances and these utilities, and here the
   b. Authors analyze the effect on the latency, throughput, and response times under different attack scenarios. The results give insight on the pros and cons of the different wireless protocols used in AMI.

Example of Real Life Problem

- Online gaming servers are vulnerable to UDP flood attacks due to the real-time nature of gaming communication and the reliance on UDP for its low-latency characteristics.
  - Real-time Communication
  - Gameplay Interruption
  - Downtime
  - Competitive Disadvantage
  - Loss of Revenue
- Overall, UDP flood attacks pose a significant threat to the stability and performance of online gaming servers, impacting both players and service providers.

Implementation: Simulation (NS-3)

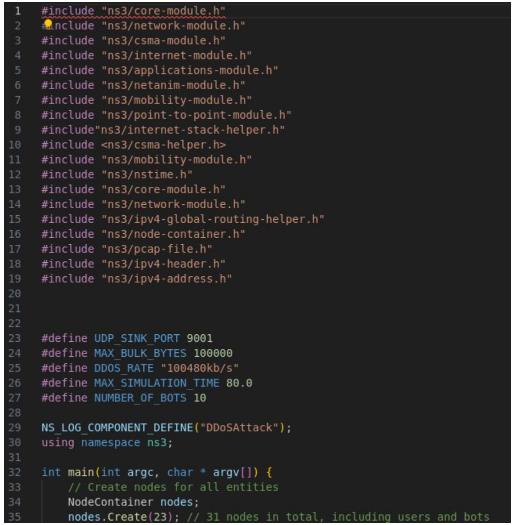
- Open-source platform simulator
- Provides a wide range of network protocols (TCP/IP, Wi-Fi, LTE, Bluetooth etc).
- Aims to provide realistic network simulations through detailed models of network components such as nodes, links and protocols
- Allows users to easily customize functionalities to specifically fit research needs

Implementation: Wireshark

- Open-source packet analyzer
- Displays all network traffic
- Supports hundreds of protocols and provides detail information about each packet:
  - Source and Destination
  - Protocol Type
  - Payload Content
- Commonly used by network administrators, developers to
  - Analyze network performance
  - Detect security threats
  - Debug network protocols and applications

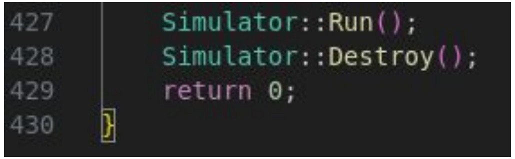
High Level Pseudo Code

1. Define all required header files by ns3
2. Define number of Users, Bots, and Network (Server) nodes
3. Create Networks and assign nodes
4. Generate IP addresses for each node
5. Assign attack parameters (DDoS rate, packet size, etc.)
6. Launch attack on target.



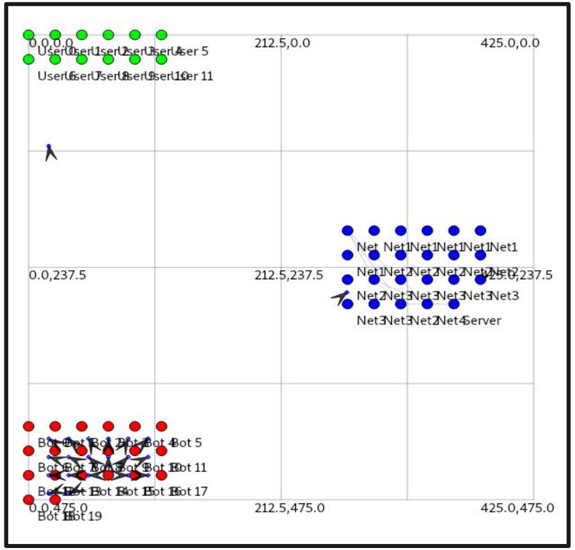
```
#include "ns3/core-module.h"
#include "ns3/network-module.h"
#include "ns3/csma-module.h"
#include "ns3/internet-module.h"
#include "ns3/applications-module.h"
#include "ns3/netanim-module.h"
#include "ns3/mobility-module.h"
#include "ns3/point-to-point-module.h"
#include"ns3/internet-stack-helper.h"
#include <ns3/csma-helper.h>
#include "ns3/mobility-module.h"
#include "ns3/nstime.h"
#include "ns3/core-module.h"
#include "ns3/network-module.h"
#include "ns3/ipv4-global-routing-helper.h"
#include "ns3/node-container.h"
#include "ns3/pcap-file.h"
#include "ns3/ipv4-header.h"
#include "ns3/ipv4-address.h"



#define UDP_SINK_PORT 9001
#define MAX_BULK_BYTES 100000
#define DDOS_RATE "100480kb/s"
#define MAX_SIMULATION_TIME 80.0
#define NUMBER_OF_BOTS 10

NS_LOG_COMPONENT_DEFINE("DDoSAttack");
using namespace ns3;

int main(int argc, char * argv[]) {
    // Create nodes for all entities
    NodeContainer nodes;
    nodes.Create(23); // 31 nodes in total, including users and bots
```

● ● ● ●

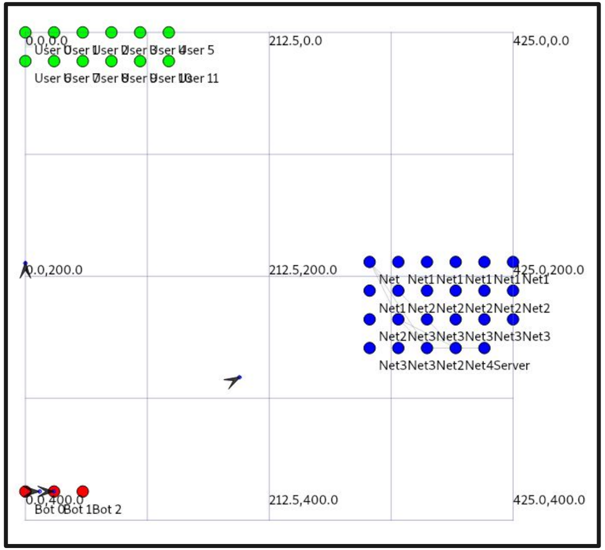


```
        Simulator::Run();
        Simulator::Destroy();
        return 0;
}
```

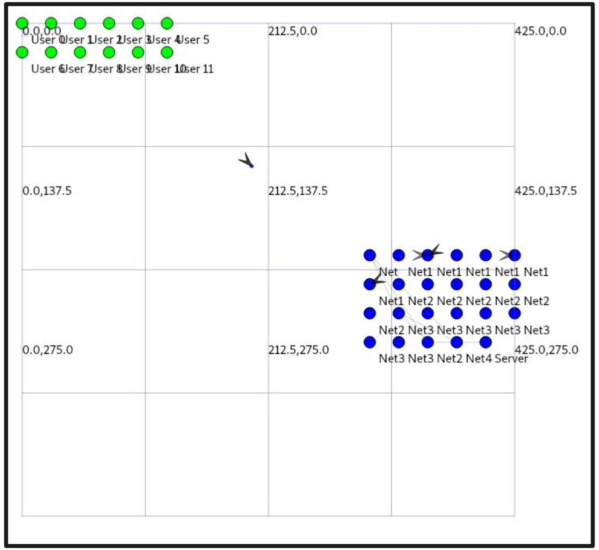
Problem Description: Technical Details (Topology)



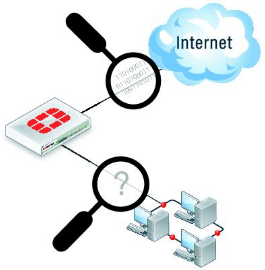
20 bots


0.0,0.0
User 0 User 1 User 2 User 3 User 4 User 5
User 6 User 7 User 8 User 9 User 10 User 11
212.5,0.0
425.0,0.0
0.0,200.0
212.5,200.0
425.0,200.0
Net Net1 Net1 Net1 Net1 Net1
Net1 Net2 Net2 Net2 Net2 Net2
Net2 Net3 Net3 Net3 Net3 Net3
Net3 Net3 Net2 Net4 Server
0.0,400.0
Bot 0 Bot 1 Bot 2
212.5,400.0
425.0,400.0

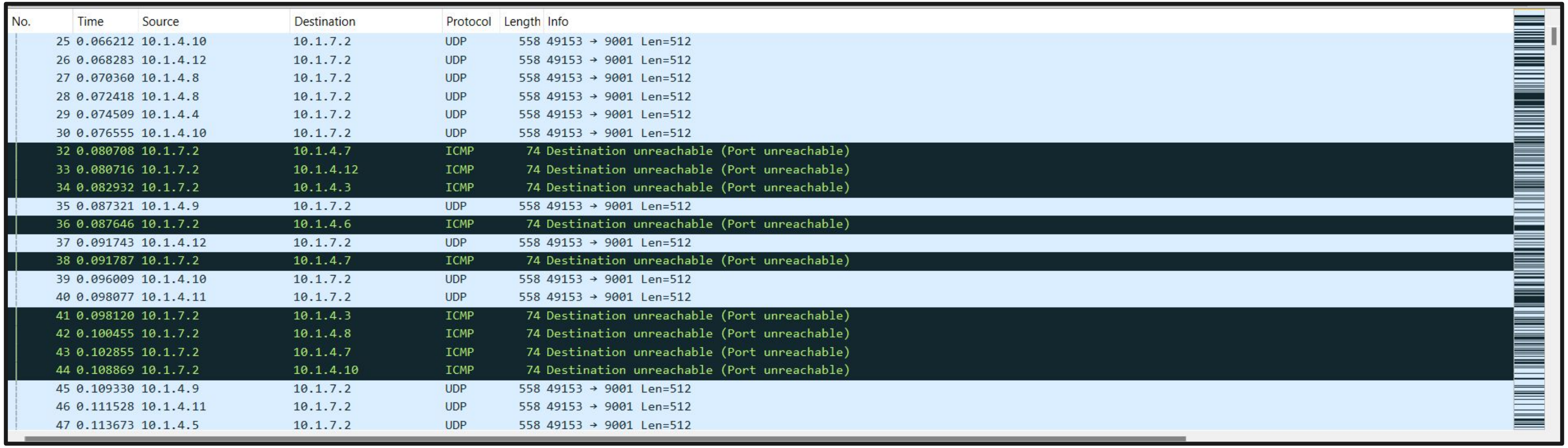
3 bots


0.0,0.0
User 0 User 1 User 2 User 3 User 4 User 5
User 6 User 7 User 8 User 9 User 10 User 11
212.5,0.0
425.0,0.0
0.0,137.5
212.5,137.5
425.0,137.5
Net Net1 Net1 Net1 Net1 Net1
Net1 Net2 Net2 Net2 Net2 Net2
Net2 Net3 Net3 Net3 Net3 Net3
Net3 Net3 Net2 Net4 Server
0.0,275.0
212.5,275.0
425.0,275.0

0 bots

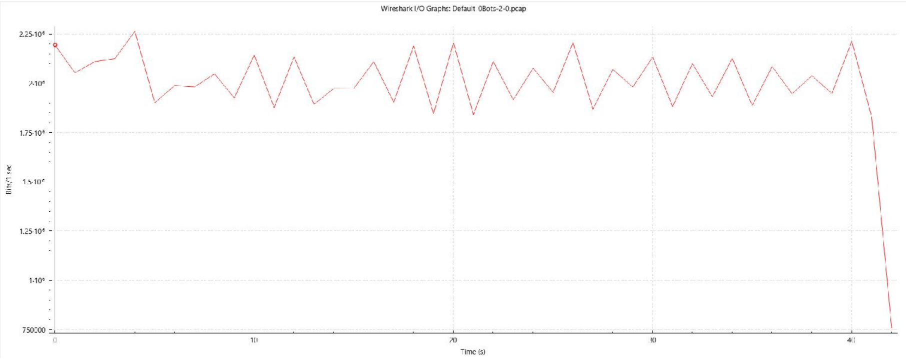


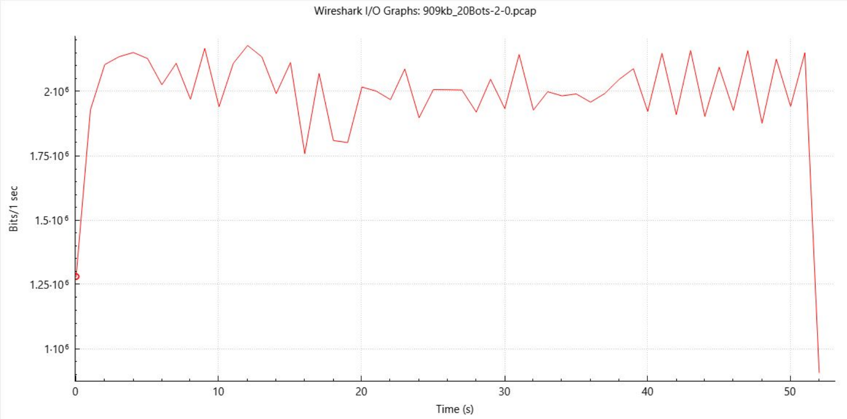
Wireshark Packet Capture



No.	Time	Source	Destination	Protocol	Length	Info
25	0.066212	10.1.4.10	10.1.7.2	UDP	558	49153 → 9001 Len=512
26	0.068283	10.1.4.12	10.1.7.2	UDP	558	49153 → 9001 Len=512
27	0.070360	10.1.4.8	10.1.7.2	UDP	558	49153 → 9001 Len=512
28	0.072418	10.1.4.8	10.1.7.2	UDP	558	49153 → 9001 Len=512
29	0.074509	10.1.4.4	10.1.7.2	UDP	558	49153 → 9001 Len=512
30	0.076555	10.1.4.10	10.1.7.2	UDP	558	49153 → 9001 Len=512
32	0.080708	10.1.7.2	10.1.4.7	ICMP	74	Destination unreachable (Port unreachable)
33	0.080716	10.1.7.2	10.1.4.12	ICMP	74	Destination unreachable (Port unreachable)
34	0.082932	10.1.7.2	10.1.4.3	ICMP	74	Destination unreachable (Port unreachable)
35	0.087321	10.1.4.9	10.1.7.2	UDP	558	49153 → 9001 Len=512
36	0.087646	10.1.7.2	10.1.4.6	ICMP	74	Destination unreachable (Port unreachable)
37	0.091743	10.1.4.12	10.1.7.2	UDP	558	49153 → 9001 Len=512
38	0.091787	10.1.7.2	10.1.4.7	ICMP	74	Destination unreachable (Port unreachable)
39	0.096009	10.1.4.10	10.1.7.2	UDP	558	49153 → 9001 Len=512
40	0.098077	10.1.4.11	10.1.7.2	UDP	558	49153 → 9001 Len=512
41	0.098120	10.1.7.2	10.1.4.3	ICMP	74	Destination unreachable (Port unreachable)
42	0.100455	10.1.7.2	10.1.4.8	ICMP	74	Destination unreachable (Port unreachable)
43	0.102855	10.1.7.2	10.1.4.7	ICMP	74	Destination unreachable (Port unreachable)
44	0.108869	10.1.7.2	10.1.4.10	ICMP	74	Destination unreachable (Port unreachable)
45	0.109330	10.1.4.9	10.1.7.2	UDP	558	49153 → 9001 Len=512
46	0.111528	10.1.4.11	10.1.7.2	UDP	558	49153 → 9001 Len=512
47	0.113673	10.1.4.5	10.1.7.2	UDP	558	49153 → 9001 Len=512

Implementation: Results (Wireshark Analysis)





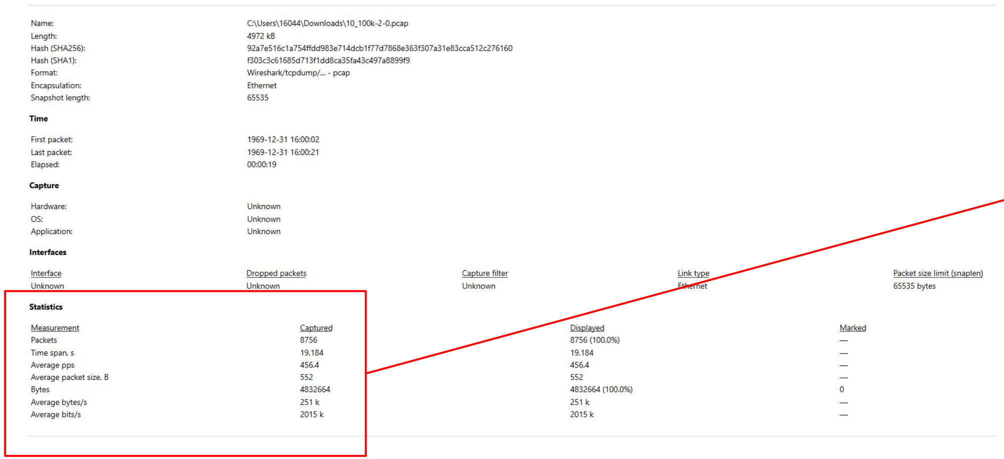
I/O Graph

- ➢ 1 sec: 2.056x10^6 bps
- ➢ 6 sec: 1.991x10^6 bps
- ➢ 11 sec: 1.879x10^6 bps
- ➢ 15 sec: 1.976x10^6 bps

I/O Graph

- ➢ 1 sec: 1.9x10^6 bps
- ➢ 6 sec: 1.971x10^6 bps
- ➢ 11 sec: 1.759x10^6 bps
- ➢ 15 sec: 1.899x10^6 bps

Implementation: Results (Wireshark Analysis)



Name:	C:\Users\16044\Downloads\10_100k-2-0.pcap
Length:	4972 kB
Hash (SHA256):	92a7e516c1a754ffdd983e714dcb1f77d7868e363f307a31e83cca512c276160
Hash (SHA1):	f303c3c61685d713f1dd8ca35fa43c497a8899f9
Format:	Wireshark/tcpdump/... - pcap
Encapsulation:	Ethernet
Snapshot length:	65535

Time

First packet:	1969-12-31 16:00:02
Last packet:	1969-12-31 16:00:21
Elapsed:	00:00:19

Capture

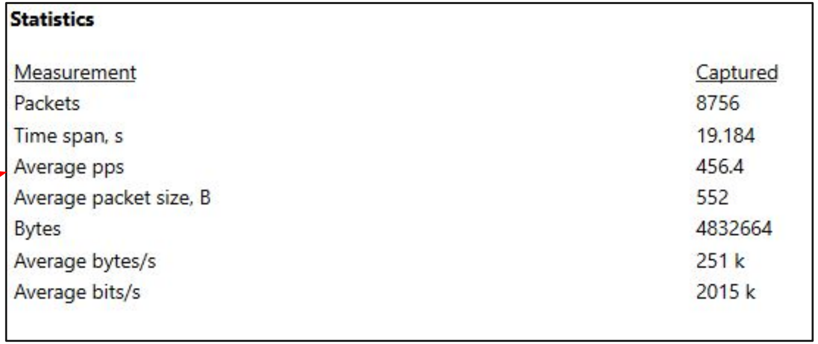
Hardware:	Unknown
OS:	Unknown
Application:	Unknown

Interfaces

Interface	Dropped packets	Capture filter	Link type	Packet size limit (snaplen)
Unknown	Unknown	Unknown	Ethernet	65535 bytes

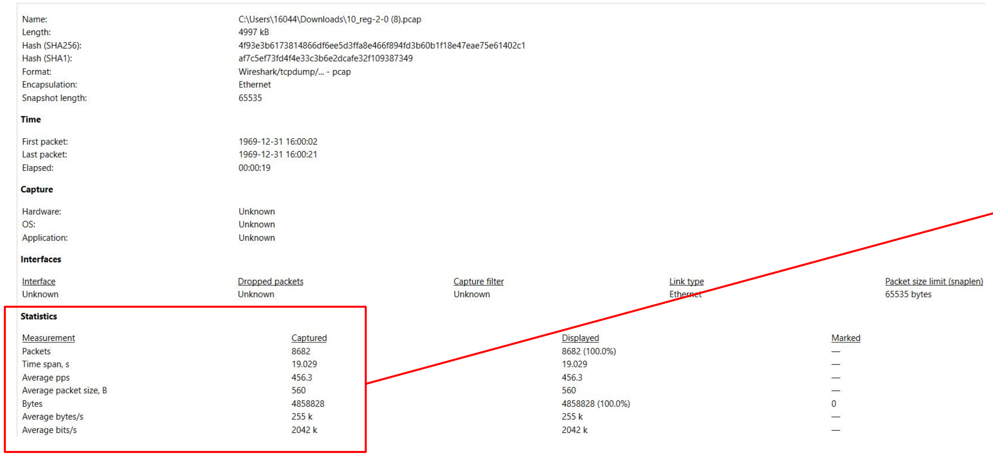
Statistics

Measurement	Captured	Displayed	Marked
Packets	8756	8756 (100.0%)	—
Time span, s	19.184	19.184	—
Average pps	456.4	456.4	—
Average packet size, B	552	552	—
Bytes	4832664	4832664 (100.0%)	0
Average bytes/s	251 k	251 k	—
Average bits/s	2015 k	2015 k	—



Statistics

Measurement	Captured
Packets	8756
Time span, s	19.184
Average pps	456.4
Average packet size, B	552
Bytes	4832664
Average bytes/s	251 k
Average bits/s	2015 k



Name:	C:\Users\16044\Downloads\10_reg-2-0 (8).pcap
Length:	4997 kB
Hash (SHA256):	4f93e3b6173814866df6ee5d3ffa8e466f894fd3b60b1f18e47eae75e61402c1
Hash (SHA1):	af7c5ef73fd4f4e33c3b6e2dcafe32f109387349
Format:	Wireshark/tcpdump/... - pcap
Encapsulation:	Ethernet
Snapshot length:	65535

Time

First packet:	1969-12-31 16:00:02
Last packet:	1969-12-31 16:00:21
Elapsed:	00:00:19

Capture

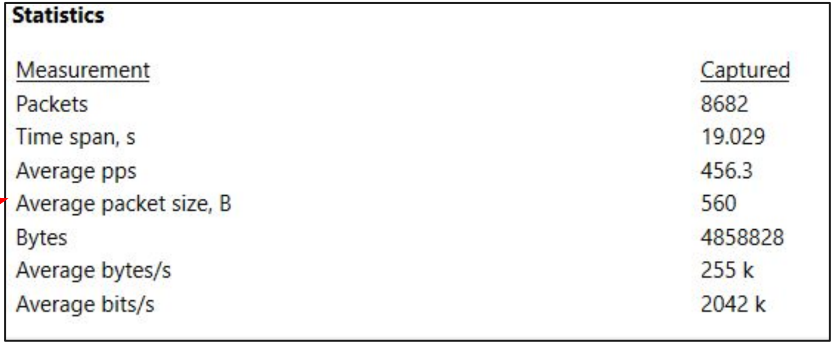
Hardware:	Unknown
OS:	Unknown
Application:	Unknown

Interfaces

Interface	Dropped packets	Capture filter	Link type	Packet size limit (snaplen)
Unknown	Unknown	Unknown	Ethernet	65535 bytes

Statistics

Measurement	Captured	Displayed	Marked
Packets	8682	8682 (100.0%)	—
Time span, s	19.029	19.029	—
Average pps	456.3	456.3	—
Average packet size, B	560	560	—
Bytes	4858828	4858828 (100.0%)	0
Average bytes/s	255 k	255 k	—
Average bits/s	2042 k	2042 k	—

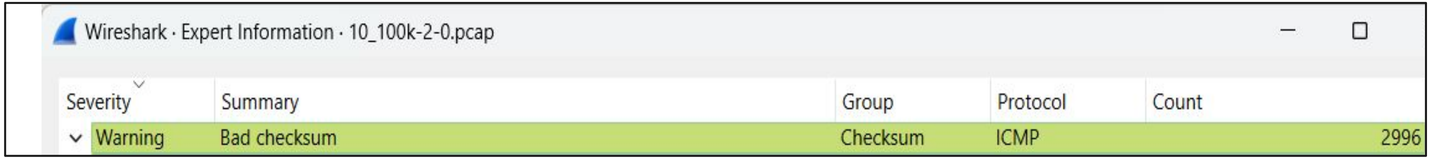


Statistics

Measurement	Captured
Packets	8682
Time span, s	19.029
Average pps	456.3
Average packet size, B	560
Bytes	4858828
Average bytes/s	255 k
Average bits/s	2042 k

Implementation: Results (Packet Loss Analysis)

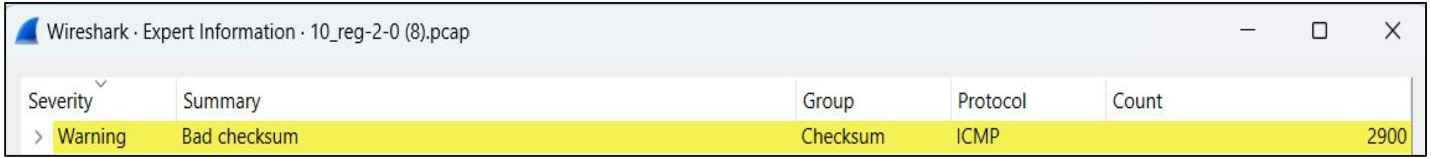
Packet Loss (%)



Wireshark · Expert Information · 10_100k-2-0.pcap

Severity	Summary	Group	Protocol	Count
Warning	Bad checksum	Checksum	ICMP	2996

34.2%



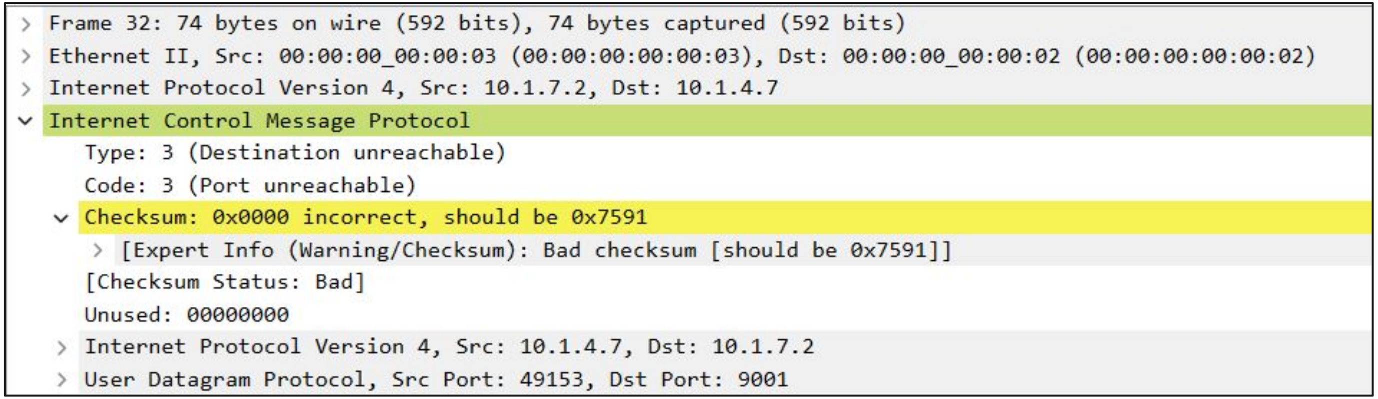
Wireshark · Expert Information · 10_reg-2-0 (8).pcap

Severity	Summary	Group	Protocol	Count
Warning	Bad checksum	Checksum	ICMP	2900

33.4%

Implementation: Checksum

- The sender computes the checksum for the UDP segment data.
- The computed checksum is then stored in the checksum field within the UDP header.
- Upon receiving the segment, the recipient computes the checksum based on the received data and compares it with the checksum stored in the header to detect data corruption.



```
> Frame 32: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
> Ethernet II, Src: 00:00:00_00:00:03 (00:00:00:00:00:03), Dst: 00:00:00_00:00:02 (00:00:00:00:00:02)
> Internet Protocol Version 4, Src: 10.1.7.2, Dst: 10.1.4.7
v Internet Control Message Protocol
    Type: 3 (Destination unreachable)
    Code: 3 (Port unreachable)
  v Checksum: 0x0000 incorrect, should be 0x7591
    > [Expert Info (Warning/Checksum): Bad checksum [should be 0x7591]]
    [Checksum Status: Bad]
    Unused: 00000000
  > Internet Protocol Version 4, Src: 10.1.4.7, Dst: 10.1.7.2
  > User Datagram Protocol, Src Port: 49153, Dst Port: 9001
```

Discussion and Limitations

Challenges	Trivial	Alternative
➢ Initial project proposal was to implement DDoS on Wireless networks ○ Segfaults ○ Spent too much time debugging ➢ Creating a realistic scenario	➢ Many open sources files ➢ Easily change different variables and settings in code ➢ Creating PCAP files to use in Wireshark	➢ Use a different software ➢ Build up from a smaller project

Organization and Time Management

- January 14th - January 29th
  - Project Proposal
- January 30th - February 25th
  - Designed web page including project title, abstract, and a list of five references
- February 26th - March 10th
  - Interim Report
  - Started looking into NS-3 header files and resources
- March 10th - April 9th
  - Continued to write the final report
  - Finished presentation slides
  - Coding the final project

Contributions

	Akash Malhi	Gurnek Ghatarora	Elaine Luu
References and Literature Review	⅓	⅓	⅓
Project Website	⅓	⅓	⅓
Simulation scenarios, implementation, analysis, and discussion of simulation result	⅓	⅓	⅓
Project Presentation	⅓	⅓	⅓
Written final report	⅓	⅓	⅓

References

[1] A. Balyk, et al., “Using graphic network simulator 3 for DDoS attacks simulation.” *International Journal of Computing.*16.4 (2017): 219-225 [accessed Feb. 23, 2024].

[2] Y. Guo et al., “Modeling distributed denial of service attack in advanced metering infrastructure.” *IEEE Xplore.* https://ieeexplore.ieee.org/abstract/document/7131828/authors [accessed Mar. 20, 2024].

[3] Cloudflare, "What is a DDoS attack? " cloudflare, https://www.cloudflare.com/en-ca/learning/ddos/what-is-a-ddos-attack/ [accessed Feb. 23, 2024].

[4] FORTINET, “What is a DDoS Attack?” Fortinet, https://www.fortinet.com/resources/cyberglossary/ddos-attack [accessed Feb. 23, 2024].

[5] I. Kotenko and A. Ulanov, “Simulation of Internet DDoS Attacks and Defense.” *Information Security*, https://doi.org/10.1007/11836810_24. [accessed Feb. 23, 2024].

[6] L. Arockiam Lawrence and B. Vani, "A Survey of Denial of Service Attacks and its Countermeasures on Wireless Network." *International Journal on Computer Science and Engineering*. https://www.researchgate.net/publication/49965401_A_Survey_of_Denial_of_Service_Attacks_and_it%27s_Countermeasures_on_Wireless_Network [accessed Feb. 23, 2024].

[7] M. Poongothai and M. Sathyakala, “Simulation and analysis of DDoS attacks.” *IEEE Xplore.* https://ieeexplore.ieee.org/abstract/document/6513885 [accessed Feb. 23, 2024].

Thank You!