University of Science and Technology in Zewail City

جـــامعة العلـوم والتكنولوجيـا بمديـنة زويل

Introduction to computer networks (CSAI 252)

Final Project Report **Team: 40**

Team Members:

Sama Mohamed Abdelhamid 202201867

Zeyad Sherif Gamal 202201220

Mohamed Darwish 202201273

Case 1:
window size: 20

Time out:3

The Packet listing windows at the sender side terminal:

```
243     end_time = time.time()
PROBLEMS    OUTPUT    DEBUG CONSOLE    TERMINAL    PORTS

Sent packet with sequence number: 20
Sent packet with sequence number: 21
Sent packet with sequence number: 22
Sent packet with sequence number: 23
Sent packet with sequence number: 24
Sent packet with sequence number: 25
Sent packet with sequence number: 26
Sent packet with sequence number: 27
Sent packet with sequence number: 28
Sent packet with sequence number: 29
Sent packet with sequence number: 30
Sent packet with sequence number: 31
Sent packet with sequence number: 32
Sent packet with sequence number: 33
Sent packet with sequence number: 34
Sent packet with sequence number: 35
Sent packet with sequence number: 36
```

The Packet listing windows at the Receiver side terminal:

```
Packet size: 8192
packet_count: 22
Received packet from: ('192.168.1.113', 59834)
Packet size: 8192
packet_count: 23
Received packet from: ('192.168.1.113', 59834)
Packet size: 8192
packet_count: 24
Received packet from: ('192.168.1.113', 59834)
Packet size: 8192
packet_count: 25
Received packet from: ('192.168.1.113', 59834)
Packet size: 8192
packet_count: 26
Received packet from: ('192.168.1.113', 59834)
Packet size: 8192
packet_count: 27
Received packet from: ('192.168.1.113', 59834)
Packet size: 8192
packet_count: 28
Received packet from: ('192.168.1.113', 59834)
Packet size: 8192
packet_count: 29
Received packet from: ('192.168.1.113', 59834)
Packet size: 8192
packet_count: 30
Received packet from: ('192.168.1.113', 59834)
Packet size: 8192
packet_count: 31
Received packet from: ('192.168.1.113', 59834)
Packet size: 8192
packet_count: 32
```

Display the file transfer information:

```
File transfer information:
Start Time: 1715737815.8020172
End Time: 1715737815.8250835
Elapsed Time (s): 0.023066282272338867
Total Packets Sent: 37
Total Bytes Sent: 303104
Average Transfer Rate (Bytes/sec): 13140565.801688941
Average Transfer Rate (Packets/sec): 1604.072973838982
PS C:\Users\zeyad\Downloads\Draft 2>
```

Case 2:

Window Size:10

Timeout: 5

The Packet listing windows at the sender side terminal:

```
Sent packet with sequence number: 30
Sent packet with sequence number: 31
Sent packet with sequence number: 32
Sent packet with sequence number: 33
Sent packet with sequence number: 34
Sent packet with sequence number: 35
Sent packet with sequence number: 36
```

The Packet listing windows at the Receiver side terminal:

```
packet_count: 28
Received packet from: ('192.168.1.113', 55382)
Packet size: 8192
packet_count: 29
Received packet from: ('192.168.1.113', 55382)
Packet size: 8192
packet_count: 30
Received packet from: ('192.168.1.113', 55382)
Packet size: 8192
```

Display the file transfer information:

```
File transfer information:
Start Time: 1715738463.3934042
End Time: 1715738463.4187512
Elapsed Time (s): 0.025346994400024414
Total Packets Sent: 37
Total Bytes Sent: 303104
Average Transfer Rate (Bytes/sec): 11958183.097231759
Average Transfer Rate (Packets/sec): 1459.7391476112987
PS C:\Users\zeyad\Downloads\Draft 2>
```

Case 3:

Window Size:25

Timeout: 10

The Packet listing windows at the sender side terminal:

```
Sent packet with sequence number: 31
Sent packet with sequence number: 32
Sent packet with sequence number: 33
Sent packet with sequence number: 34
Sent packet with sequence number: 35
Sent packet with sequence number: 36
```

The Packet listing windows at the Receiver side terminal:

```
packet_count: 34
Received packet from: ('192.168.1.113', 62184)
Packet size: 8192
packet_count: 35
Received packet from: ('192.168.1.113', 62184)
Packet size: 8192
packet count: 36
```

Display the file transfer information:

```
File transfer information:
Start Time: 1715738781.0157156
End Time: 1715738781.039642
Elapsed Time (s): 0.0239264965057373O5
Total Packets Sent: 37
Total Bytes Sent: 303104
Average Transfer Rate (Bytes/sec): 12668131.329938717
Average Transfer Rate (Packets/sec): 1546.4027502366598
PS C:\Users\zeyad\Downloads\Draft 2>
```

Discuss how the protocol of this project can be modified for a better performance.

Ensuring reliable data transfer across unreliable networks poses a core dilemma in computer networking. While the Go-Back-N protocol tackles this issue by permitting the transmission of multiple packets without awaiting acknowledgments, there remains room for refinement. Taking from the TCP protocol standard, integrating congestion control mechanisms into the Go-Back-N protocol holds promise for notable performance upgrades.

TCP's congestion control mechanisms, including features such as slow start, congestion avoidance, fast retransmit, and fast recovery, aim to adaptively regulate the transmission rate in response to network conditions. This approach optimizes throughput while safeguarding against network congestion.

Modify the sender in a way that exploits any weakness in the protocol specifications to maliciously disrupt the receiver.

Within the sender of the Go-Back-N (GBN) protocol, a potential Weakness exists that could be exploited maliciously to disrupt the receiver's functionality.

Attack Method:

A malicious sender could intentionally manipulate the timeout mechanism to flood the network with unnecessary retransmissions. By artificially delaying acknowledgment responses or by sending acknowledgments for packets that were never received, the sender can trigger frequent timeouts at the receiver. This flood of retransmissions overwhelms the receiver, leading to increased network congestion and potentially causing denial of service.

Mitigation Methods:

1- Timeout Backoff Mechanism: Add a backoff system to the sender. If timeouts happen one after the other, make the waiting time longer each time. This slows down retransmissions and makes it harder for someone to mess with the timeouts on purpose.

2- Duplicate Acknowledgment Detection: Improve the receiver to spot and get rid of duplicate acknowledgments, which might suggest someone is up to no good. By getting rid of these fake acknowledgments, the receiver can lessen the impact of acknowledgment tricks.

Protocol Updates for Enhanced Security:

1- Sequence Number Validation: Incorporate a check in the receiver to confirm that the packets received are in the right order. This helps prevent attacks where someone sends packets out of order to mess up the communication.

2- Checksum Verification: Integrate checksum verification in the receiver to detect packet tampering or corruption. By verifying the integrity of received packets, the protocol can mitigate the impact of packet alteration attacks.

Legal Implications:

In Egypt, cybercrimes and unauthorized network interference are regulated under Law No. 175 of 2018 on Combating Information Technology Crimes (commonly known as the Cybercrime Law) with penalty starts from 7 years of prison. This law criminalizes a range of cyber activities, including unauthorized access to computer systems and networks, data interception, and the dissemination of malicious software. Penalties under this law can include fines and imprisonment.

Internationally, Multiple conventions and treaties exist to combat cybercrime and unauthorized network interference. One prominent instance is the Budapest Convention on Cybercrime, also

recognized as the Council of Europe Convention on Cybercrime. This agreement sets up legal structures for member states to tackle diverse cybercrimes, such as unauthorized access to computer systems, data tampering, and disruption of networks. Penalties for breaches of the Budapest Convention can differ based on the jurisdiction of the member state.

Discuss the possible economic and societal impact of freely spreading tools that can disrupt network communication.

Financial Losses: The operational success of businesses greatly depends on reliable network communication. Any interruption caused by readily accessible tools can lead to notable financial setbacks due to periods of inactivity, reduced efficiency, and the risk of tarnishing their reputation. Furthermore, sectors like finance, healthcare, and e-commerce are especially susceptible to such disruptions, amplifying the overall economic impact.

National Security Risks: The widespread distribution of disruptive tools carries substantial risks to national security. Malicious individuals, including cybercriminals and state-sponsored actors, could exploit these tools to initiate cyberattacks aimed at critical infrastructure, government networks, and defense systems. Such actions could jeopardize national security and stability.

Social Disruption: Disruptions in network connectivity have the potential to interfere with vital services like healthcare, education, and emergency response systems, which directly affect the safety and welfare of communities. Furthermore, extensive disruptions may worsen existing social disparities, disproportionately affecting marginalized groups that have limited access to alternative resources.