DdoS Attack using NS3

Syed Muhammad Hashir	CIIT/FA21-BCE-032/ATD
Muhammad Hassan	CIIT/FA21-BCE-051/ATD
Hafiz Rehmatullah	CIIT/FA21-BCE-061/ATD

Outline

- Introduction
- Literature Review
- Proposed Solution
- Results
- Teamwork / Tasks Division
- Conclusion

Introduction

- This project aims to address this crucial issue by simulating a DDoS attack using the NS-3 network simulator, a versatile tool widely adopted for network research and simulation.
- By leveraging NS-3, we can construct a realistic and controlled network environment to model and analyze the behavior and impact of DDoS attacks.
- The primary goal is to create a simulation that provides deep insights into how these attacks affect network performance and to evaluate potential strategies for mitigating their impact.
- DDoS attacks are a significant threat to network security, where multiple compromised systems flood the targeted system with traffic, overwhelming its resources and causing a denial of service to legitimate users.
- By simulating a DDoS attack in a controlled environment, we can better understand its impact on network performance and explore potential mitigation strategies.

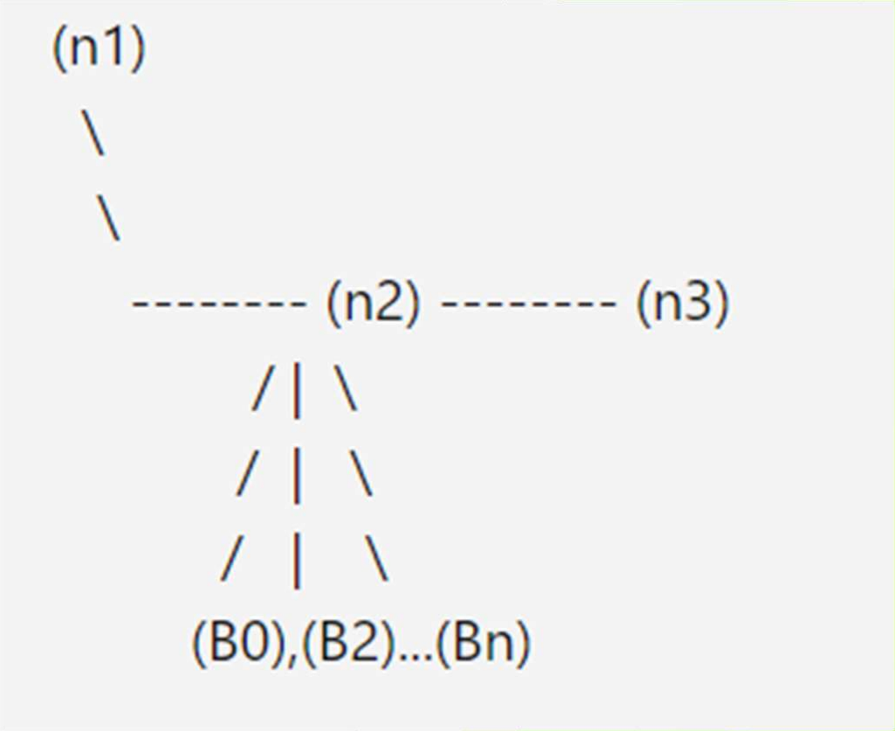
Literature Review

- **Simulation of DDoS Attacks:**
- Numerous studies have been conducted to simulate DDoS attacks and analyze their impact on network performance. Researchers have used various network simulators, including NS-2, NS-3, OMNeT++, and others, to create controlled environments for studying these attacks. These simulations help in understanding the attack dynamics, the extent of damage, and potential mitigation strategies.
- **Mitigation Strategies**
- Several mitigation strategies have been proposed and tested in simulated environments to counter DDoS attacks. These strategies include rate limiting, traffic filtering, anomaly detection, and the use of machine learning algorithms for detecting and mitigating attacks in real-time.

Proposed Solution/Methodology

System Design / Block diagram

- Network Topology:
- The network topology for this simulation consists of three primary nodes
- Client Node (n0):
- Generates legitimate traffic directed towards the server.
- Intermediate Node (n1):
- Routes traffic between the client and the server. This node is the primary target of the DDoS attack.
- Server Node (n2):
- Receives and processes traffic from the client.
- Bot Nodes (B0-Bn):
- A set of nodes generating malicious traffic directed towards the intermediate node.



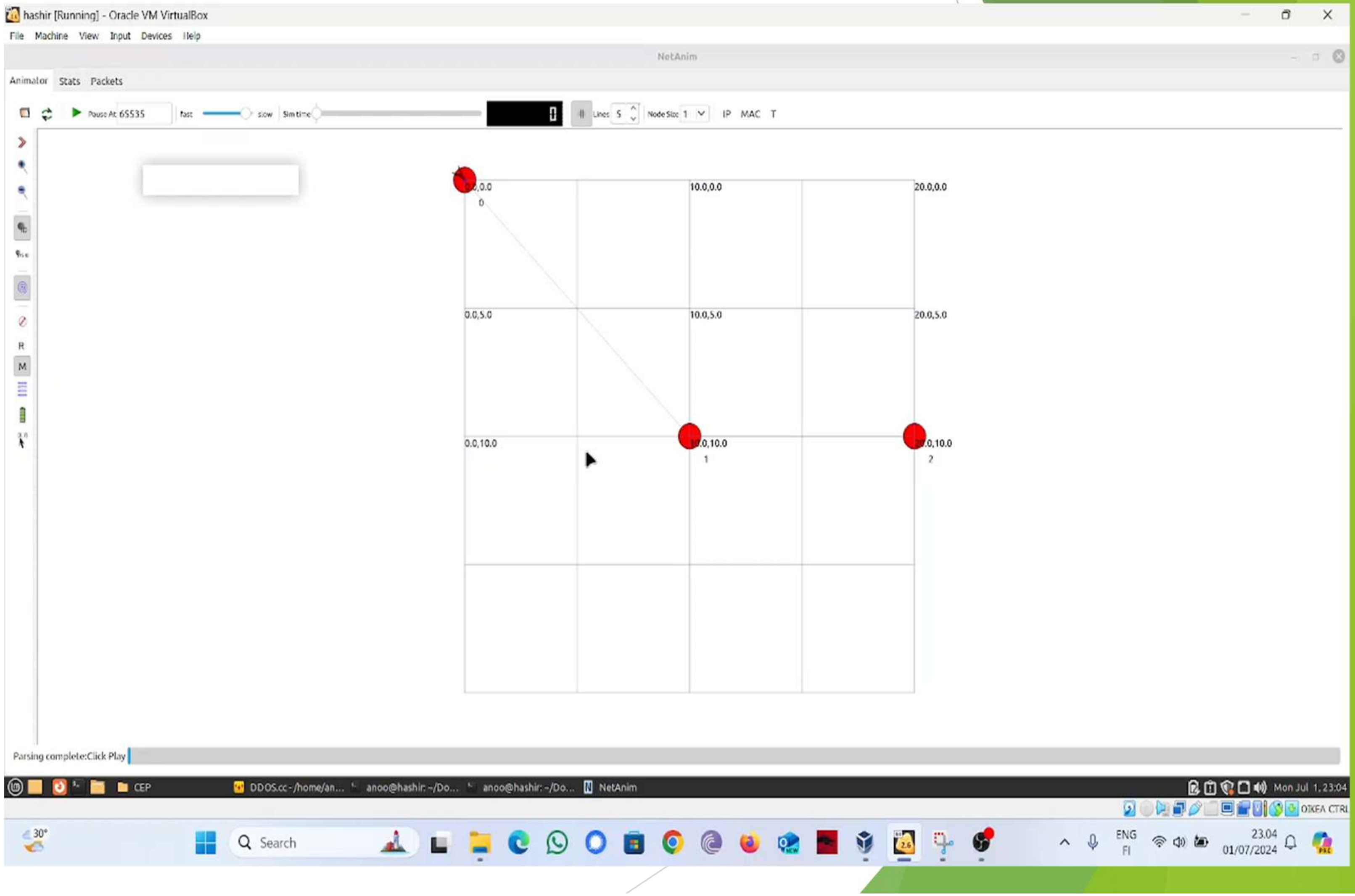
```
(n1)
 \
  \
    -------- (n2) -------- (n3)
              /|\
             / | \
            /  |  \
       (B0),(B2)...(Bn)
```

Proposed Solution/Methodology

Simulation:

Below simulation is for simple network when bots are still not connected.

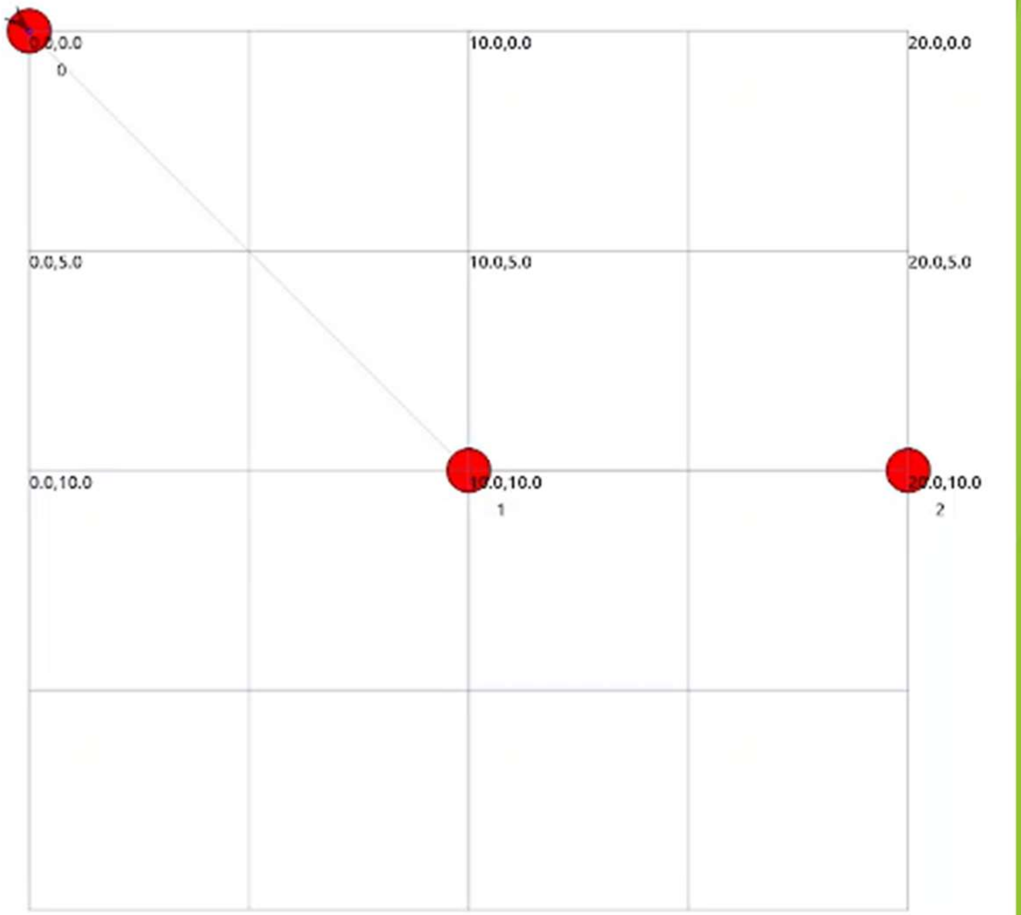
As we can see traffic is normal and client (n0) request is being fulfilled by server application (n2) and this is passed through an intermediate node (n1).



Parsing complete:Click Play

Proposed Solution/Methodology

- **Simulation diagram:**
- As we can see traffic is normal and client (n0) request is being fulfilled by server application (n2) and this is passed through an intermediate node (n1).



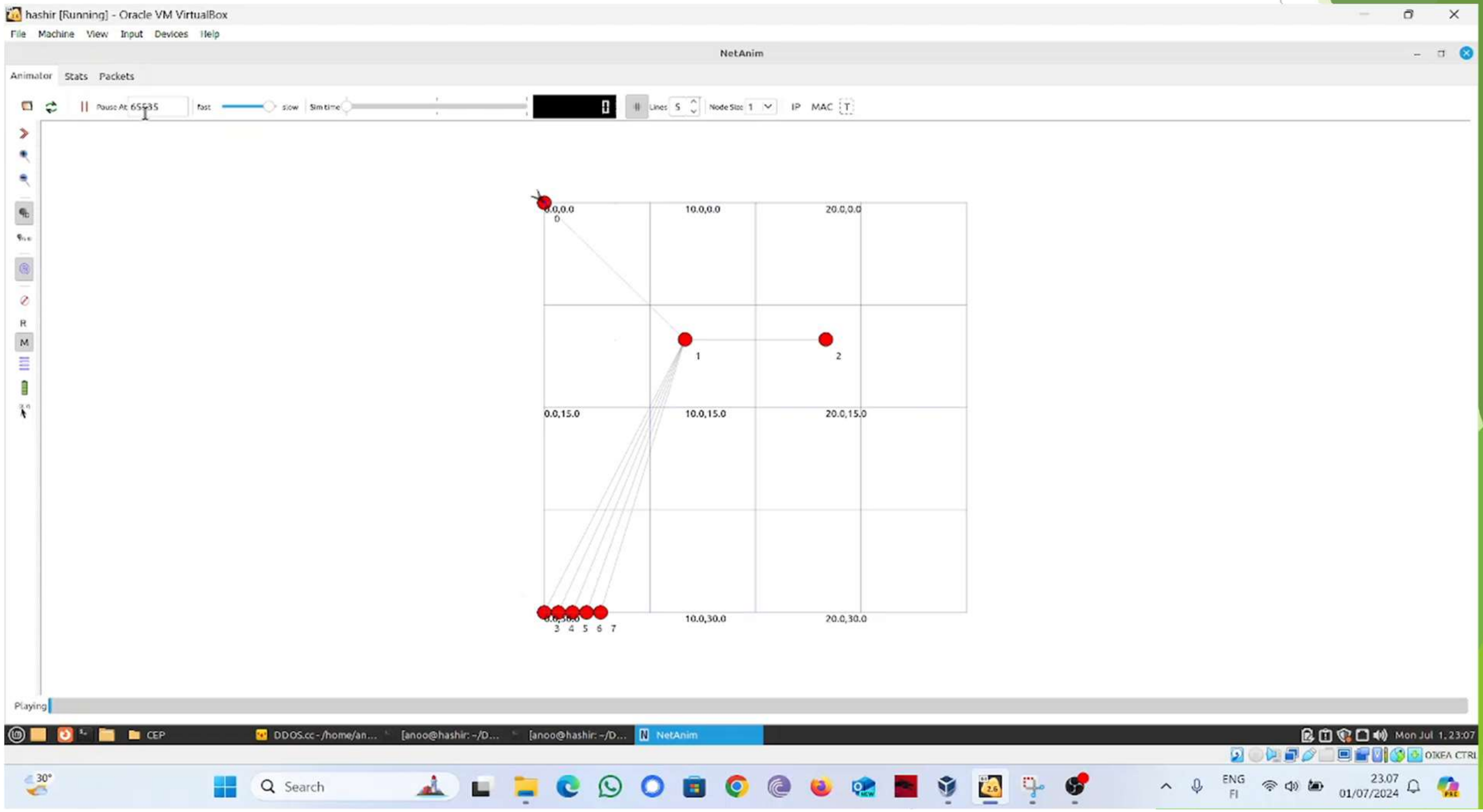
Proposed Solution/Methodology

- **Algorithm:**
- The provided program simulates a Denial-of-Service (DoS) attack using ns-3. Here's the algorithm breakdown:
- 1. Setup:
- 2. IP Address Assignment:
- 3. DDoS Application Configuration:
- 4. Legitimate Traffic Configuration:
- 5. Sink Applications:
- 6. Routing and Network Animation:
- 7. Simulation Execution:

Results

▶ Software simulation 1 results:

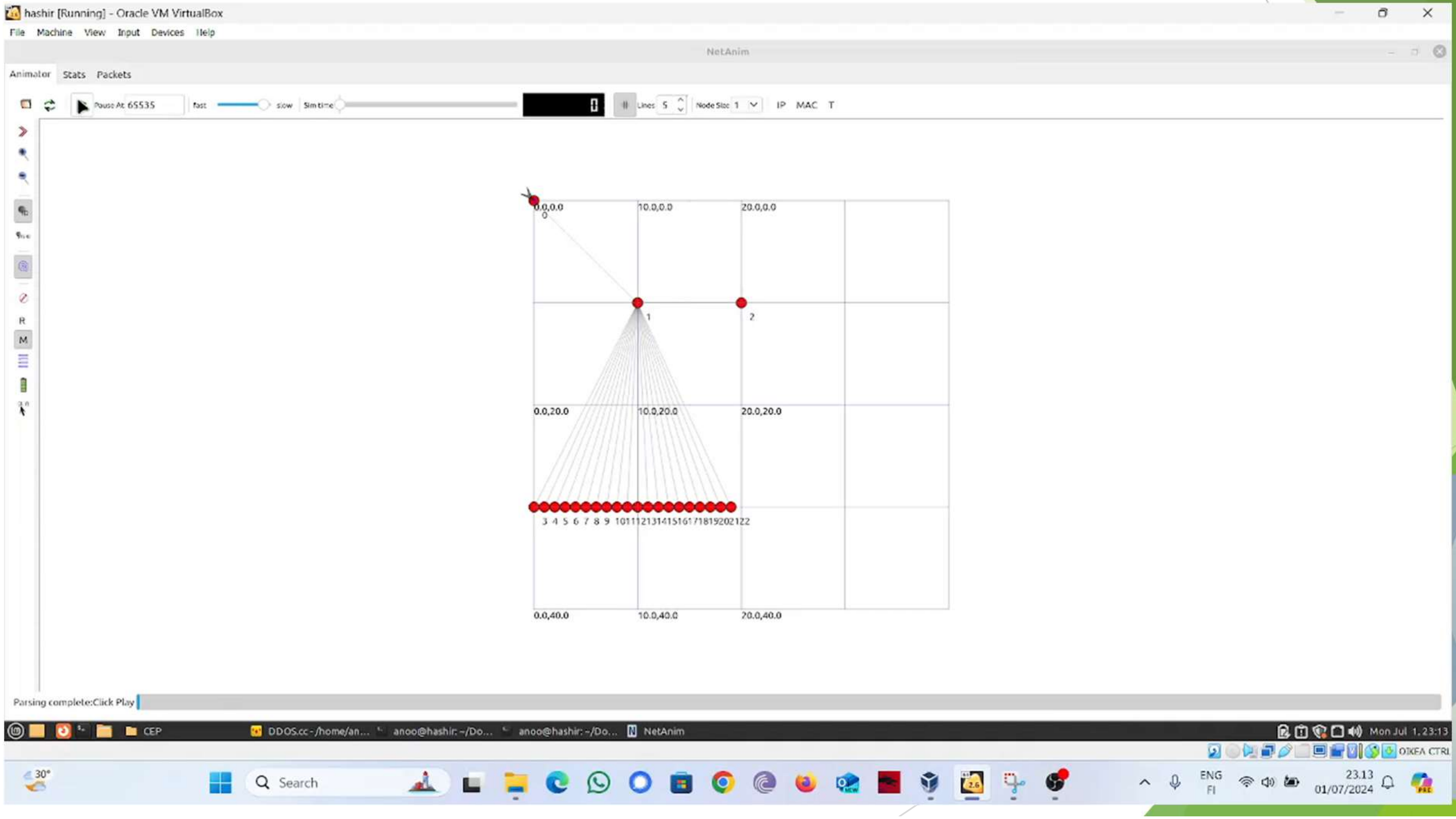
we have connected 5 bots. Requests from the client are properly going to the server application (first image) but response from the server side is slow which can be seen in the second image



Results:

Software simulation 2 results:

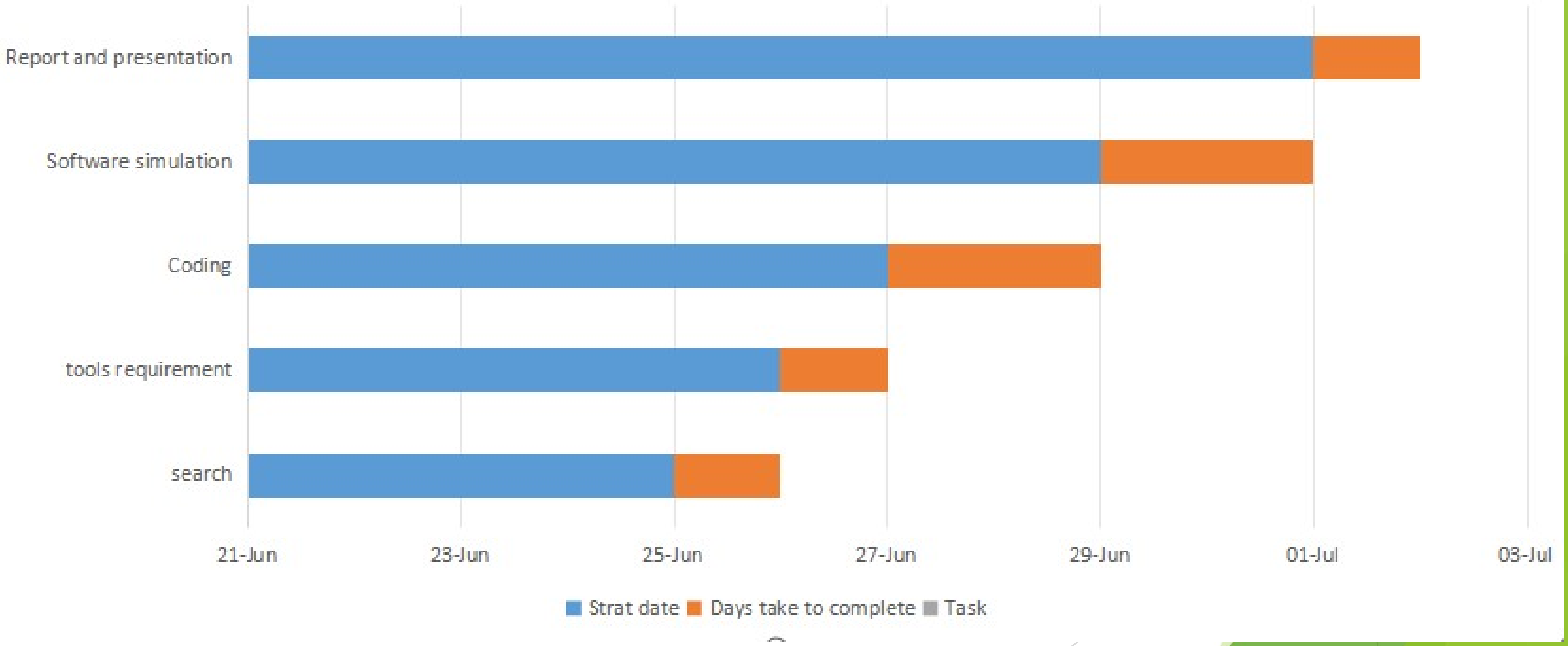
we have used 20 bots. Requests from the client are properly going to the server application (first image) but response from the server side is very slow because now we have used more number of bots which can be seen in the second image.



Results:

- **Design/simulation parameters**
- 1 .Network Topology:
- 2. Network Configuration:
- 3. Attack Parameters:
- 4. Application Behavior:
- 5. Simulation Environment:
- **Discussions**
- 1 .Effectiveness of DDoS Attack:
- 2. Impact on Server Application:
- 3. Simulation Limitations and Future Enhancements:

Teamwork


Report and presentation
Software simulation
Coding
tools requirement
search
21-Jun
23-Jun
25-Jun
27-Jun
29-Jun
01-Jul
03-Jul
Strat date
Days take to complete
Task

Conclusion

- In conclusion, this project simulated a Distributed Denial of Service (DDoS) attack using NS-3, focusing on understanding its impact and exploring mitigation strategies in network security. The simulation employed a network topology with nodes representing legitimate clients, an intermediate node, and a server application, along with bots simulating the attackers. Through general parameterization of network configurations, attack characteristics, and simulation environments, the study observed significant disruptions caused by the DDoS attack. Discussions highlighted the effectiveness of DDoS attacks in compromising network performance and the importance of implementing robust defense mechanisms such as rate limiting and traffic filtering to mitigate their impact. Future research could enhance simulation realism and explore advanced defense strategies to bolster network resilience against such kind of attacks.