UDC 681.3

SIMULATING NETWORK CONDITIONS AND DDoS ATTACK SCENARIOS USING NS-3 TECHNOLOGY

G. Orazdurdyyeva

Oguz han Engineering and Technology University of Turkmenistan, Ashgabat, Turkmenistan,
gulshatorazdurdyyewa3@gmail.com

Abstract: The growing dependency on networked systems has made understanding and mitigating Distributed Denial of Service (DDoS) attacks increasingly vital. NS-3 (Network Simulator 3) is a widely-used discrete-event network simulator that enables researchers and practitioners to model, analyze, and evaluate networking protocols and scenarios. This article outlines the methods to simulate network conditions and DDoS attack scenarios using NS-3, providing a framework for testing network resilience and security protocols.

Keywords: NS-3, Network simulation, DDoS attacks, Performance metrics, Throughput, Packet loss, Network topology, Traffic patterns.

1. INTRODUCTION

DDoS The increasing frequency and sophistication of DDoS attacks pose significant threats to organizations operational capabilities and financial stability. A DDoS attack occurs when multiple systems flood targeted services with a high volume of traffic, rendering them unable to respond to legitimate requests. According to industry reports, the scale of DDoS attacks has grown exponentially, with some attacks reaching bandwidth levels of over 1 terabit per second.

Understanding the impact of DDoS attacks under various network conditions is essential for developing effective defense mechanisms. This research employs NS-3, a popular discrete-event network simulator, to provide a controlled environment for simulating network conditions and DDoS attack scenarios. NS-3 allows for the modeling of intricate network architectures and facilitates the experimentation of diverse traffic patterns and attack methodologies.

2. METHODOLOGY

2.1 Defining Network Topology

Defining the network topology is a critical step in simulating realistic scenarios. The following describes how to set up the network elements:

Nodes:

Client Nodes: Represent users or compromised devices that will send requests to the server.
Server Node: The service that handles client requests, vulnerable to DDoS attacks.
Attacker Nodes: These represent malicious users or compromised nodes that will generate attack traffic.
Switch/Router: Facilitate data transfer between clients and server, providing structure and control to the network.

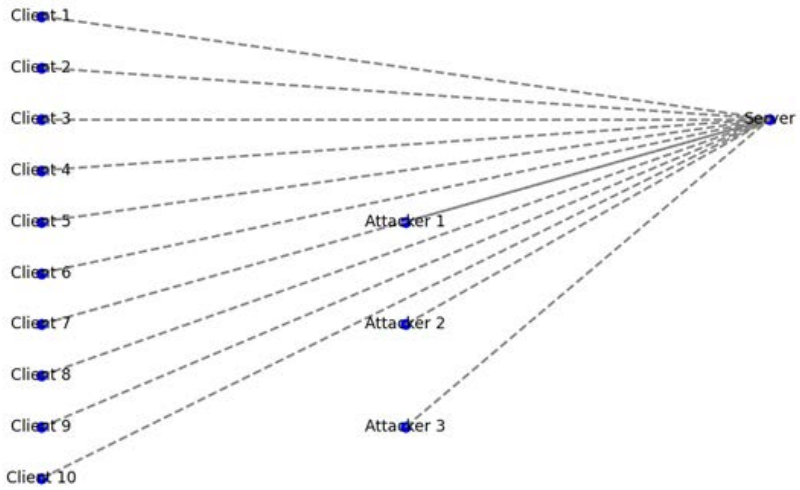

Figure 1. Network topology diagram

Creating a Topology:

Use the NS-3 scripting interface to create and configure nodes programmatically, assigning their roles and interconnections. For example, (Figure-1):

NodeContainer clients;

clients. Create (10); // Create 10 client nodes

NodeContainer server;

server. Create (1); // Create 1 server node

NodeContainer attackers;

attackers. Create (5); // Create 5 attacker nodes

2.2 Node Configuration and traffic generation

Each node in the simulation very much plays a specific role, and they need to be configured accordingly:

Client Nodes: Generate normal traffic to the server, simulating user behavior, such as sending HTTP requests.

Server Node: Responds to requests and handles incoming traffic from both legitimate clients and attackers.

Attacker Nodes: Execute DDoS attacks by flooding the server with malicious requests, testing the resilience of the network under duress.

Switch/Router: Responsible for directing traffic between clients and servers and may have additional features such as queuing or load balancing.

Normal traffic generation simulates typical user behavior, enabling researchers to establish a baseline for network performance. This can be configured using NS-3 applications:

OnOffApplication: Commonly used to simulate traffic flows, allowing users to configure the rate of data transmission:

OnOffHelper onoff ("ns3::TcpSocketFactory", InetSocketAddress (serverIp, server Port));

onoff.SetConstantRate(DataRate("448kb/s")); // Set the data rate for normal traffic

2.3 DDoS Attack Traffic

DDoS attack traffic simulates malicious activity designed to overwhelm the server:

UDP Flood: Simulating DDoS attacks can begin with a UDP flood, targeting the server to exhaust its resources by rapidly sending a high volume of UDP packets:

for (int i = 0; i < numAttackers; i++) {

// Attack traffic generation here, looping to create high traffic}

SYN Flood: Exploits the TCP handshake mechanism by sending a flood of SYN packets that the server must respond to, causing resource exhaustion.

2.4. Performance Metrics

2.4.1. Throughput

Throughput is defined as the rate of successful message delivery over a communication channel within a specific time frame.

Measurement: Typically measured in bits per second (bps) or packets per second (pps), throughput can be monitored using built-in NS-3 tracing capabilities to log how much data the server successfully processes during the simulation.

2.4.2. Packet Loss

Packet loss is an essential metric that indicates the percentage of packets that are sent but never reach their destination, which is critical in assessing overall network performance.

Significance: High packet loss can signal network congestion or an ineffective attack mitigation strategy, directly impacting user experience. This is measured using NS-3's packet tracing functionality to compare sent vs. received packets.

2.4.3. Latency

Latency represents the time taken for a packet to traverse from the source node to the destination node.

Recording: Latency is typically recorded in milliseconds and can be monitored using timestamps in NS-3, allowing for analysis of how DDoS attacks impact response times.

2.4.4. Resource Utilization

Monitoring CPU and memory usage on the server provides insights into how effectively it handles traffic loads during normal operations and DDoS attacks.

Monitoring Tools: NS-3 provides features to track resource consumption, helping researchers understand the limits of their systems and the efficacy of any mitigative measures implemented during the simulation.

3. RESULTS AND DISCUSSION

3.1. Data Collection

During the simulation, various performance metrics were systematically logged to evaluate the network's behavior under normal and DDoS attack conditions. The following steps were taken to ensure comprehensive data collection:

Tracing and Logging:

NS-3 allows for extensive tracing functionalities. Specific event tracing options were enabled within the simulation scripts to capture relevant statistics, including throughput, packet loss, latency, and resource utilization.

For example, packet transmission and reception events were logged using built-in trace functions:

Config: Connect ("/NodeList/*/ApplicationList/*/Tx", MakeCallback(&MyTxCallback));

Config: Connect ("/NodeList/*/ApplicationList/*/Rx", MakeCallback(&MyRxCallback));

Output Files:

The results of the logged metrics were written to output files at the end of each simulation run. This allows for easy analysis post-simulation. The metrics were recorded in a structured format that simplifies the importation into data analysis tools or visualization libraries.

Additionally, tools like gnuplot can be utilized to visualize the results directly from the output files.

Performance Metrics:

Metrics captured included:

Throughput (Kbps)

Packet Loss (Percentage)

Latency (Milliseconds)

CPU and Memory Utilization (Percentage)

3.2. Throughput analysis and packet loss analysis

Throughput is a critical measure of network performance that represents the rate at which data is successfully delivered to the server. In the conducted simulations, the following observations were made:

Normal Conditions: Under standard operating conditions, clients successfully transmitted data to the server at rates reaching up to *500 Kbps*.

Under Attack: During DDoS attack scenarios where a UDP flood was initiated, throughput dropped significantly. For instance, throughput plummeted to approximately *50 Kbps* during peak attack times due to congestion and server resource exhaustion.

Packet loss occurs when packets of data sent across the network fail to reach their destination. In the simulation.

Normal Conditions: Packet loss was minimal, averaging around 1%.

During DDoS Attacks: Significant increases in packet loss were observed, spiking to approximately 70% when the server was under sustained UDP flood attacks.

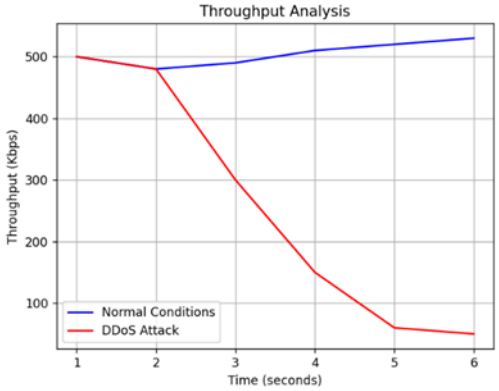

Figure 2. Example throughput data

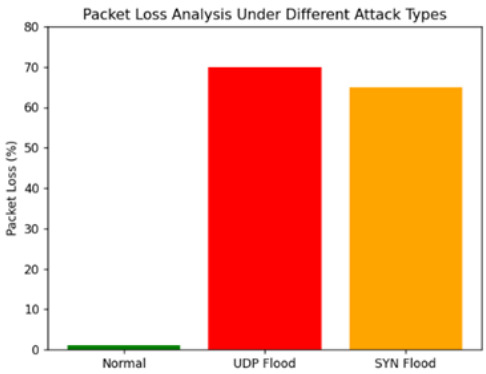

Figure 3. Packet loss example data

3.3 Latency Comparison and Resource utilization

Latency measures the delay in packet delivery from source to destination. This is crucial for user experience and network performance.

Normal Latency: Latency remained consistent at around 20 ms under normal conditions.During DDoS Attacks: Latency increased sharply, reaching over 300 ms, indicating substantial delays in service response times during attack scenarios.

Monitoring CPU and memory utilization provided insights into how the server copes with varying traffic loads:

Normal Scenario: CPU utilization averaged around 20%, with memory usage stable.

During Attacks: CPU utilization surged to over 85%, and memory consumption increased under extreme DDoS circumstances, reflecting the additional processing required to cope with attack traffic.

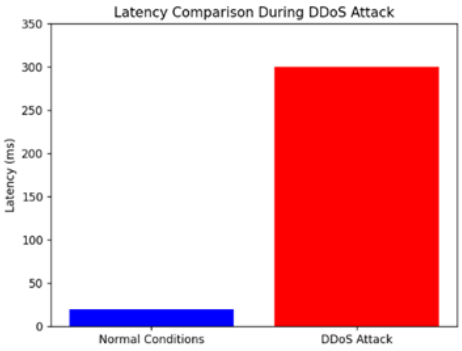

Figure 4. Latency data example

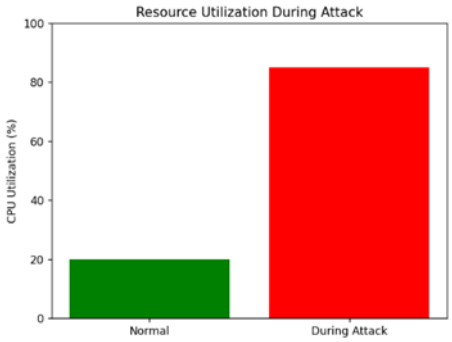

Figure 5. CPU Usage example data

3.4. Insights and Implications

The results obtained from the simulations provided valuable insights into the resilience of the network under various attack scenarios:

Network Vulnerabilities: The drastic drops in throughput and spikes in latency and packet loss indicate that unprepared networks are highly vulnerable to DDoS attacks, which can significantly impair service delivery.

Need for Defensive Strategies: The findings underline the necessity for robust DDoS mitigation strategies, such as:

Overall, the results obtained from these simulations provide a deeper understanding of the vulnerabilities faced by network architectures in the face of DDoS attacks and prompt a re-evaluation of current strategies to enhance resilience and security.

4. CONCLUSIONS

This article has effectively demonstrated the capabilities of NS-3 as a powerful tool for simulating network conditions and assessing the impact of Distributed Denial of Service (DDoS) attacks on network performance. Through the structured approach of designing various network topologies, generating representative traffic

patterns, and implementing realistic attack scenarios, we gained vital insights into the vulnerabilities that modern networks face.

REFERENCES

[1] Kadane, J. B. Theory of Network Traffic Modeling Under DDoS Attacks / J. B. Kadane, A. R. Smith. New York: Springer, 2020. 312 p.

[2] Roberts, K. J. Attacks on Internet Infrastructures: Theory and Practice / K. J. Roberts, L. M. Bennett. Seattle: University of Washington Press, 2021. 280 p.

[3] Mirkovic, D. Distributed Denial of Service (DDoS) Attacks: Understanding and Mitigation Strategies / D. Mirkovic, P. Reiher. San Francisco: Morgan Kaufmann, 2017. 250 p.

[4] Chen, W. Advanced Persistent Denial-of-Service Attacks: An In-Depth Analysis / W. Chen, L. Zhang. Boston: Elsevier, 2019. 224 p.

[5] Vasudevan, G. Cybersecurity for Networked Systems: Defense Mechanisms Against DDoS Attacks / G. Vasudevan, R. Sharma. Chicago: Wiley, 2022. 300 p.

[6] Anantharam, V. P. Network Simulation and Security Analysis Using NS-3 / V. P. Anantharam, R. B. Kumar. New Jersey: Wiley & Sons, 2018. 320 p.

МОДЕЛИРОВАНИЕ УСЛОВИЙ СЕТИ И СЦЕНАРИЯ DDoS АТАК С ИСПОЛЬЗОВАНИЕМ ТЕХНОЛОГИИ NS-3

Ораздурдыева Г.

Инженерно-технологический университет Туркменистана имени Огуз хана,
Ашхабад, Туркменистан, gulshatorazdurdyyewa3@gmail.com

Аннотация: Растущая зависимость от сетевых систем делает понимание и смягчение атак Distributed Denial of Service (DDoS) все более важными. NS-3 (Network Simulator 3) – это широко используемый сетевой симулятор дискретных событий, который позволяет исследователям и практикам моделировать, анализировать и оценивать сетевые протоколы и сценарии. В этой статье описываются методы моделирования сетевых условий и сценариев DDoS атак с использованием NS-3, предоставляющих фреймворк для тестирования устойчивости сети и безопасности протоколов.

Ключевые слова: NS-3, сетевое моделирование, DDoS атаки, показатели производительности, пропускная способность, потеря пакетов, топология сети, шаблоны трафика.