A

MAJOR PROJECT-III REPORT

on

Traceback Mechanisms for Malicious Traffic Detection: An NS-3 Simulation Approach

Submitted by:

Meka Jeyadev (210274)
Gopika (210365)
Shivangi (210366)
Rishit Chowdary (210197)
Shaik Mahmmad Nazir (210326)

under
mentorship of

Dr. Abhishek Jain(Assistant Professor)
Dr. Nikhil (Assistant professor)

Department of Computer Science Engineering
School of Engineering and Technology
BML MUNJAL UNIVERSITY, GURUGRAM (INDIA)

May 2024

TABLE OF CONTENT

I. CANDIDATE'S DECLARATION

I hereby certify that the work on the project entitled, **"Project Name - Traceback Mechanisms for Malicious Traffic Detection: An NS-3 Simulation Approach**", in partial fulfillment of requirements for the award of Degree of **Bachelor of Technology** in School of Engineering and Technology at BML Munjal University, is an authentic record of the work carried out during a period from 27th January 2024 to 17th May2024 under the supervision of Dr. Abhishek Jain & Dr. Nikhil.

1) Meka Jeyadev – (210274)
2) Gopika (210365)
3) Shivangi (210366)
4) Rishit Chowdary (210197)
5) Shaik Mahmmad Nazir (210326)

SUPERVISOR'S DECLARATION

This is to certify that the above statement made by the candidate is correct to the best of my knowledge.

Faculty Supervisor Name: Dr. Abhishek Jain
Faculty Supervisor Name: Dr. Nikhil

Signature:

II. Acknowledgement

I am highly grateful to Dr. Abhishek Jain, Assistant Professor, Dr. Nikhil, Assistant Professor, BML Munjal University,

Gurugram, for providing supervision to carry out the seminar/case study from July December 2022.

Dr. Abhishek Jain & Dr. Nikhil has provided great help in carrying out my work and is acknowledged with reverential thanks. Without wise counsel and able guidance, it would have been impossible to complete the training in this manner.

I would like to express thanks profusely to Dr. Abhishek Jain, for stimulating me from time to time. I would also like to thank the entire team at BML Munjal University. I would also thank my friends who devoted their valuable time and helped me in all possible ways toward successful completion.

III. List of Figures

IV. List of Tables

V. List of Abbreviation

NS3	Network Simulator 3
DDoS	Distributive Denial of Services
NetAnim	Network Animator
IDS	Intrusion Detection System
WSNs	Wireless Sensor Networks
IoT	Internet of Things
VANETs	Vehicular Ad-hoc Networks
P2P	Peer-to-Peer
SDN	Software Defined Networking
TCP	Transmission Control Protocol
SVM	Support Vector Machine
UDP	User Datagram Protocol.

1. Abstract

This project explores cybersecurity within the NS-3 simulation environment on Ubuntu, divided into four sections. In Section 1, an 8-node network is established, simulating packet transmission using C++ scripts. Section 2 introduces a malicious node triggering a simulated DDoS attack, flooding packets towards a designated endpoint. Section 3 focuses on identifying the attacker through traffic analysis, showcasing a novel method for DDoS detection in simulated environments. Finally, Section 4 addresses mitigating the DDoS attack by isolating the attacker and victim nodes while preserving the functionality of other network segments. Utilizing the NetAnim tool, this project underscores the necessity of proactive cybersecurity measures in mitigating evolving threats.

1.1 Motivation

In today's hyper-connected digital landscape, where information flows seamlessly across global networks, the integrity and security of these networks stand as paramount concerns. Cyber threats, ranging from subtle infiltration attempts to full-scale attacks, pose significant risks to individuals, organizations, and even nations. Among these threats, Distributed Denial of Service (DDoS) attacks emerge as particularly insidious, capable of crippling vital network infrastructures and disrupting essential services. The motivation behind our project stems from a deep-seated recognition of the critical importance of cybersecurity in preserving the functionality and stability of modern networks. As aspiring cybersecurity professionals, we are driven by a shared commitment to understanding and combating these threats through innovative research and practical solutions.

By focusing our efforts on the detection and mitigation of DDoS attacks within the NS-3 simulation environment, we aim to address a pressing need for proactive cybersecurity measures. Through our project, we seek to unravel the complexities of DDoS attack vectors, identify vulnerabilities within network architectures, and develop effective countermeasures to neutralize these threats. Furthermore, our motivation extends beyond academic curiosity to real-world implications. As cyber threats continue to evolve in sophistication and scale, the need for robust cybersecurity frameworks becomes increasingly urgent. By gaining insights into the dynamics of DDoS attacks and honing our skills in threat detection and mitigation, we hope to contribute to the ongoing efforts to safeguard digital ecosystems against malicious incursions.

Ultimately, our project serves as a testament to our unwavering dedication to the principles of cybersecurity and our steadfast commitment to ensuring the resilience and security of network infrastructures in the face of emerging threats.

2. Introduction

In an era dominated by digital interconnectedness, cybersecurity stands as a cornerstone in safeguarding the integrity and functionality of network infrastructures. As cyber threats continue to evolve in complexity and sophistication, the need for robust defensive measures becomes increasingly paramount. In response to this pressing demand, our project embarks on a comprehensive exploration of cybersecurity principles within the Network Simulator 3 (NS3) environment, operating on the Ubuntu platform.

Divided into four distinct sections, our project navigates the intricate terrain of network dynamics and security vulnerabilities, offering valuable insights into the detection and mitigation of Distributed Denial of Service (DDoS) attacks. Beginning with the establishment of an 8-node network, we meticulously simulate packet transmission akin to real-world scenarios, laying the groundwork for subsequent analyses.

With the introduction of a malicious node, our project pivots towards the examination of DDoS attack vectors within simulated environments. Through systematic observation and analysis, we endeavor to identify the malevolent actors orchestrating these assaults, shedding light on novel methodologies for threat detection.

Building upon our findings, we delve into the development and implementation of countermeasures aimed at neutralizing DDoS threats. By strategically isolating the attacker and victim nodes, we aim to mitigate the impact of malicious incursions while preserving the functionality of unaffected network segments.

Through simulation using the NetAnim tool, our project not only provides a platform for experimentation and analysis but also underscores the urgency of proactive cybersecurity measures in safeguarding network integrity. As we navigate through the intricacies of network security, our project serves as a beacon of innovation and resilience in the face of evolving cyber threats.

2.1 Existing Systems

Existing systems for combating DDoS attacks encompass a range of techniques and technologies aimed at detecting, mitigating, and preventing such malicious activities. Traditional approaches often rely on firewalls, intrusion detection systems (IDS), and load balancers to filter and monitor network traffic, attempting to identify and block suspicious or anomalous behavior. Additionally, specialized DDoS mitigation services and appliances offer targeted solutions for mitigating large-scale attacks by diverting and scrubbing malicious traffic. More advanced strategies involve the use of machine learning algorithms and behavioral analysis techniques to proactively identify and respond to DDoS threats in realtime. Despite these existing systems' efficacy to some extent, the evolving nature of DDoS attacks necessitates ongoing research and innovation to stay ahead of emerging threats and bolster network defenses.

2.2 User Requirement Analysis

To begin the user requirement analysis for our project focused on combating DDoS attacks within the NS-3 environment, it's essential to understand the stakeholders and their specific needs and expectations. The primary stakeholders in this context include:

- **Cybersecurity Researchers:** These individuals are primarily interested in developing and validating innovative techniques for detecting, mitigating, and preventing DDoS attacks within simulated environments. They require a platform that facilitates experimentation and analysis, enabling them to assess the effectiveness of various defense mechanisms and strategies.
- **Network Administrators:** Network administrators are responsible for maintaining the integrity and functionality of network infrastructures. They seek solutions that can effectively detect and mitigate DDoS attacks in real-time, minimizing disruption to network services and ensuring continuous availability for end-users.
- **Educational Institutions:** Educational institutions may use the NS-3 platform for teaching and research purposes in cybersecurity and network engineering courses. As such, they require a user-friendly environment that allows students to gain hands-on experience with DDoS detection and mitigation techniques, enhancing their understanding of cybersecurity principles.

Based on the needs of these stakeholders, the user requirements for our project can be outlined as follows:

- **Simulation Environment:** The NS-3 simulation environment should be robust, flexible, and easy to use, allowing researchers and students to create and manipulate network topologies, simulate DDoS attacks, and analyze network behavior.
- **DDoS Attack Scenarios:** The platform should support the simulation of various DDoS attack scenarios, including volumetric attacks, protocol attacks, and application-layer attacks, enabling users to explore different attack vectors and their impact on network performance.
- **Detection Mechanisms:** Users should have access to a range of DDoS detection mechanisms, such as anomaly detection, signature-based detection, and machine learning-based detection, allowing them to evaluate the effectiveness of different detection techniques in identifying malicious traffic.
- **Mitigation Strategies:** The platform should provide tools for implementing and testing DDoS mitigation strategies, such as traffic filtering, rate limiting, and traffic diversion, enabling users to assess the efficacy of different mitigation approaches in mitigating DDoS attacks.

By addressing these user requirements, our project aims to provide a comprehensive platform for researching, teaching, and experimenting with DDoS detection and mitigation techniques within the NS-3 environment, ultimately contributing to the advancement of cybersecurity knowledge and practices.

3. Literature Review

[1] Scans and blocks infected nodes, while IPS nodes monitor and block misbehaving nodes. Effectively prevents DDoS attacks and enhances network security. It employs a two-pronged approach: identifying and blocking infected nodes through scanning algorithms and utilizing Intrusion Prevention System (IPS) nodes to monitor and block misbehaving nodes within their radio range.[2] Reviews approaches to detect and defend against DDOS attacks in WSNs. Evaluates existing mechanisms considering resource constraints.[3] Detects and mitigates attacks in IoT networks using CoAP and DTLS protocols. Provides early-stage detection and outperforms existing methods. This approach reportedly outperforms existing methods.[4] This paper investigates jamming attacks, a specific type of DoS attack, in Vehicular Ad-hoc Networks (VANETs). It proposes a method to identify and isolate multiple malicious nodes, thereby enhancing network security and overall performance.

[5] This research presents a technique that combines stateful and stateless signatures for early detection and prevention of DoS attacks. This method offers an efficient and scalable defense mechanism.[6][7] Swiftly identifies malicious nodes in P2P live streaming. Enhances system efficiency and security.[8][15] Safeguards critical servers from DDoS attacks using TCP probing and bloom filter trust model. Ensures continuous server availability and high-quality service provision.[9][16] Efficiently detects and counters DDoS attacks in IoT networks and SDNs. Ensures normal network operation and protects against Botnet exploitation. [10] This research leverages Mininet, a network emulator, to monitor traffic statistics and mitigate DDoS attacks in SDN environments. By enabling efficient attack detection and prevention, this approach bolsters network security.[11] This paper proposes a technique for mitigating Interest Flooding Attacks, a specific type of DDoS attack, in Named Data Networking (NDN). This approach offers security enhancements with minimal overhead on the network.[12] This paper proposes a technique for mitigating Interest Flooding Attacks, a specific type of DDoS attack, in Named Data Networking (NDN). This approach offers security enhancements with minimal overhead on the network.[13] This paper proposes a technique for mitigating Interest Flooding Attacks, a specific type of DDoS attack, in Named Data Networking (NDN). This approach offers security enhancements with minimal overhead on the network.

[14][17] Develops a trust-based framework to detect DDoS attacks. Enhances security and optimizes bandwidth utilization. [18] Introduces a scheme for early detection of DDoS attacks in WSNs. Enhances network security and conserves energy.[19] Proposes separation concept to prevent DDoS attacks. Enhances security and warrants further study.[20] Employs Hadoop for rapid detection of DDoS attacks. Enables swift blocking of malicious IPs and substantial traffic reduction.

Table 3.1 Literature Review

Year	Author	Title	Methodology	Conclusion
2017 [1]	Surendra Nagar; Shyam Singh Rajput; Avadesh Kumar Gupta; Munesh Chandra Trivedi	Secure routing against DDoS attack in wireless sensor network	Proposed secure routing protocol scans and blocks infected nodes, while IPS nodes monitor and block misbehaving nodes in WSNs.	The scheme effectively prevents DDoS attacks, enhances network security, and improves performance in WSNs.
2016 [2]	Taranpreet Kaur; Krishan Kumar Saluja; Anuj Kumar Sharma	DDOS attack in WSN: A survey	Paper reviews approaches to detect and defend against DDOS attacks in WSNs considering resource constraints.	Developing a security model for WSNs to combat DDOS attacks is a challenging task, and the paper evaluates existing mechanisms based on various parameters.
2018 [3]	Shruti Kajwadkar; Vinod Kumar Jain	A Novel Algorithm for DoS and DDoS attack detection in Internet of Things	Proposed algorithm detects and mitigates DoS and DDoS attacks in resource constrained IoT networks using CoAP and DTLS protocols.	Algorithm provides effective early-stage detection and mitigation of DoS and DDoS attacks in IoT, outperforming existing methods.
2018 [4]	Sushil Kumar; Kulwinder Singh Mann	Detection of Multiple Malicious Nodes Using Entropy for Mitigating the Effect of Denial-of-Service Attack in VANETs	The algorithm detects jamming attacks in VANETs by isolating multiple malicious and irrelevant nodes, ensuring timely dissemination of critical information and enhancing network availability.	The proposed algorithm enhances VANET security by isolating malicious nodes, boosting network performance metrics over existing methods.
2005 [5]	John Haggerty, Qi Shi, Madjid Merabti	Early detection and prevention of denialof-service attacks: a novel mechanism with propagated traced-back attack blocking	Combine stateful and stateless signatures, employ domainbased approach, gradually propagate blockage, confine attacks, simplify tracing back attack sources.	Efficient and scalable solution for DOS attacks, enhances network security, minimizes overload, streamlined tracing, improved defense in the information economy.

2010 [6]	Qiyan Wang; Long Vu; Klara Nahrstedt; Himanshu Khurana	MIS: Malicious Nodes Identification Scheme in Network-CodingBased Peer-to-Peer Streaming	Efficiently mitigate pollution attacks in P2P live streaming systems by swiftly identifying malicious nodes via hash computations, minimizing computational latency and space overhead.	Proposed scheme surpasses prior methods, ensuring live streaming system efficiency with rapid malicious node detection, validated via simulations on actual PPLive channel overlays.
2015 [7]	Abdul Quyoom; Raja Ali; Devki Nandan Gouttam; Harish Sharma	A novel mechanism of detection of denial-ofservice attack (DoS) in VANET using Malicious and Irrelevant Packet Detection Algorithm (MIPDA)	Implement MIPDA to detect and mitigate DoS attacks in VANET.	MIPDA enhances VANET security by reducing network overload and ensuring availability of critical information.
2019 [8]	Pedro Manso, José Moura and Carlos Serrão	SDN-Based Intrusion Detection System for Early Detection and Mitigation of DDoS Attacks	Implement a Software-Defined IDS to detect and counter DDoS attacks in IoT networks.	Our IDS efficiently mitigates DDoS attacks, ensuring normal network operation and protecting against Botnet exploitation.
2019 [9]	Nisha Ahuja1, Gaurav Singal2	DDOS Attack Detection & Prevention in SDN using OpenFlow Statistics	Utilize Mininet to monitor traffic statistics and detect DDoS attacks in Software Defined Networks. Prevent attacks by adjusting switch forwarding logic.	Our method efficiently detects and mitigates DDoS attacks in Software Defined Networks, bolstering network security.

2020 [10]	Vassilios G. Vassilakis, Bashar A. Alohali, Ioannis D. Moscholios, Michael D. Logothetis	Mitigating Distributed Denial-of-Service Attacks in Named Data Networking	Assess vulnerability to Interest Flooding Attacks (IFA) and propose a mitigation technique.	The proposed scheme effectively enhances security with minimal overhead.
2020 [11]	Mochamad Teguh Kurniawan; Setiadi Yazid	Mitigation and Detection Strategy of DoS Attack on Wireless Sensor Network Using Blocking Approach and Intrusion Detection System	Implement signature-based IDS in WSN to detect DoS attacks and block attacker packets.	Blocking approach effectively mitigates DoS attacks in WSN, ensuring network reliability and security.
2014 [12]	B.S. Kiruthika Devi; G. Preetha; G.Selvaram;	An impact analysis: Real time DDoS attack detection and mitigation using machine learning.	Develop an OMS for real-time impact measurements, incorporate HCF and SVM for spoofed traffic detection, and implement IBRL for traffic rate limiting.	The proposed model effectively detects and mitigates DDoS attacks with high accuracy and reduced false positives.
2012 [13]	Saravanan Kumarasamy, Asokan Ramasamy	Distributed Denial of Service (DDoS) Attacks Detection Mechanism	Deploy Efficient Spoofed Mitigation Scheme (ESMS) to protect critical servers from DDoS attacks, using TCP probing and the bloom filter trust model.	ESMS accurately detects and controls spoofed packets during DDoS attacks, ensuring seamless server availability and high Quality of Service (QoS) for customers
2018 [14]	Ademola P. Abidoye, Ibidun C. Obagbuwa	DDoS attacks in WSNs: detection and countermeasures	Propose a message analyzer scheme for WSNs to detect compromised SNs and	The proposed scheme effectively detects and defends against DDoS attacks in WSNs.

			messages, compared with related protocols.	

2017 [15]	L. Kavisankar; C. Chellappan; S. Venkatesan; P. Sivasankar	Efficient SYN Spoofing Detection and Mitigation Scheme for DDoS Attack	Utilize Efficient Spoofed Mitigation Scheme (ESMS) with TCP probing and bloom filter trust model to safeguard critical servers from DDoS attacks.	ESMS effectively detects and controls spoofed packets during DDoS attacks, ensuring continuous server availability and highquality service provision.
2020 [16]	Rana Abubakar; Abdul aziz Aldegheishem; Muhammad Faran Majeed	An Effective Mechanism to Mitigate Real-Time DDoS Attack	Integrate optimized SVM with SNORT IPS for DDoS detection and mitigation, identifying attack routes and initiating early-stage mitigation.	Outperforming traditional methods, our approach achieves 97% accuracy in detecting and mitigating DDoS attacks, enhancing network security against evolving threats.
2020 [17]	I. Sumantra; S. Indira Gandhi	DDoS attack Detection and Mitigation in Software Defined Networks	Utilize SDN for DDoS attack detection by analyzing network flow data and implementing mitigation strategies in the POX controller, evaluated via Mininet emulation	The proposed scheme effectively detects and mitigates DDoS attacks in SDN, improving attack detection time, reducing delay for legitimate requests, and optimizing CPU utilization.
2019 [18]	M. Poongodi; Mounir Hamdi; Ashutosh Sharma Maode Ma	DDoS Detection Mechanism Using Trust-Based Evaluation System in VANET	Develop a trust-based framework to detect DDoS attacks in VANETs, utilizing trust elements and clustering methods for efficient attacker identification and detection cost reduction.	The proposed mechanism enhances VANET security by effectively detecting DDoS attacks, optimizing bandwidth utilization, and safeguarding network nodes.

2016 [19]	Kanchan Kaushal Varsha Sahni	Early Detection of DDoS Attack in WSN	Introduce a new scheme for early detection of DDoS attacks in WSNs to prevent data loss and conserve energy.	The proposed scheme enhances network security by detecting DDoS attacks early, preventing data loss and conserving energy.
2013 [20]	Hongbin Luo; Yi Lin; Hongke Zhang; Moshe Zukerman	Preventing DDoS attacks by identifier/locator separation	Identify issues, introduce separation concept, detail mapping, discuss DDoS challenges, and analyze impact with real data.	Separation enhances security, is crucial for Internet resilience, warrants further study, has practical applications, and underscores ongoing need for innovation
2018 [21]	Vishal Maheshwari; Ashutosh Bhatia; Kuldeep Kumar	Faster detection and prediction of DDoS attacks using MapReduce and time series analysis.	Employ Hadoop for parallel log file processing and propose time series-based prediction for rapid DDoS attack detection.	Hadoop-driven processing enables swift detection within minutes, aiding in prompt blocking of malicious IPs and substantial traffic reduction.
2020 [22]	Ahmed Benmoussa Aflou Abdou el Karim Tahari Chaker Abdelaziz Kerrache Nasreddine Lagraa	MSIDN: Mitigation of Sophisticated Interest flooding-based DDoS attacks in Named Data Networking	Propose MSIDN for mitigating interest flooding-based DoS and DDoS attacks in NDN, focusing on precise rate-limiting and source-based blocking without harming legitimate users.	MSIDN demonstrates effectiveness in NDN, as evidenced by simulations showing robust attack mitigation while preserving legitimate traffic flow.
2019 [23]	G Ajeetha; G Madhu Priya	Machine Learning Based DDoS Attack Detection	Utilize feature analysis and classifiers (Naive Bayes, Random Forest) to detect DDoS attacks from traffic flow traces.	Proposed method offers promising detection capabilities, with Naive Bayes outperforming Random Forest, crucial for mitigating risks and safeguarding against DDoS attacks in cyber security.

2003 [24]	Abraham Yaar Adrian Perrig Dawn Song	Pi: a path identification mechanism to defend against DDoS attacks	Introduce Pi, a packet marking approach enabling per-packet path identification despite source IP spoofing, facilitating proactive defense against DDoS attacks.	Pi's lightweight design proves effective in mitigating large-scale DDoS attacks, showcasing its resilience and efficacy in real Internet simulations.
2019 [25]	Mauro Conti, Chhagan Lal, Reza Mohammadi & Umashankar Rawat	Lightweight solutions to counter DDoS attacks in software defined networking	Propose lightweight countermeasures for Route Spoofing and Resource Exhaustion DDoS attacks in SDN networks, validated through simulations showing reduced bandwidth consumption, processing delay, and improved packet delivery rate.	Countermeasures effectively mitigate DDoS threats in SDN, enhancing network performance with accurate detection rates.

3.1 Problem Statement:

In the face of escalating cyber threats, our project within the Network Simulator 3 (NS-3) environment on Ubuntu seeks to develop effective defense mechanisms against Distributed Denial of Service (DDoS) attacks. With the prevalence of DDoS incidents impacting network infrastructures worldwide, there is an urgent need to enhance our ability to detect, mitigate, and prevent such malicious activities. By exploring innovative approaches within a simulated environment, we aim to contribute to the advancement of cybersecurity research and bolster network resilience against evolving threats.

4. Methodology

4.1 Introduction to Network Simulation Tools (NS-3 and NetAnim):

NS-3 (Network Simulator 3) is an open-source network simulation framework widely used for research and education in the field of computer networking. It provides a comprehensive set of libraries and modules for simulating various network protocols, devices, and scenarios. NS-3 allows users to create complex network topologies, model packet transmission and routing behaviors, and analyze network performance under different conditions. NetAnim, a visualization tool integrated with NS-3, enables users to visualize network simulations in realtime, facilitating the visualization of network topologies, packet movements, and traffic flows.

4.2 Programming Languages and Tools:

For our project, we primarily utilize C++ programming language for scripting network behaviors within the NS-3 environment. C++ offers robust capabilities for low-level network programming, allowing us to define the behavior of individual network nodes, simulate packet transmission, and implement DDoS attack scenarios. Additionally, we leverage Python scripting language for auxiliary tasks and automation within the project. Python's versatility and extensive libraries make it well-suited for tasks such as data analysis, visualization, and script automation, complementing the capabilities of C++ within the NS-3 framework.

4.3 User Characteristics:

The target users of our project include cybersecurity researchers, network administrators, and educational institutions. Cybersecurity researchers aim to utilize the project for experimenting with DDoS detection and mitigation techniques within simulated network environments. Network administrators seek practical insights and strategies for defending against DDoS attacks in real-world network infrastructures. Educational institutions utilize the project for teaching and learning purposes, providing students with hands-on experience in cybersecurity research and network simulation.

4.4 Constraints:

Several constraints influence the development and implementation of our project. These include resource constraints, such as limited computational resources and hardware capabilities available for conducting simulations. Time constraints also play a significant role, requiring efficient project management and prioritization of tasks to meet project deadlines. Additionally, technical limitations inherent to the NS-3 simulation environment may impose constraints on the complexity and scalability of network simulations, influencing the scope and design of the project.

4.5 Use Case Model/Flow Chart:

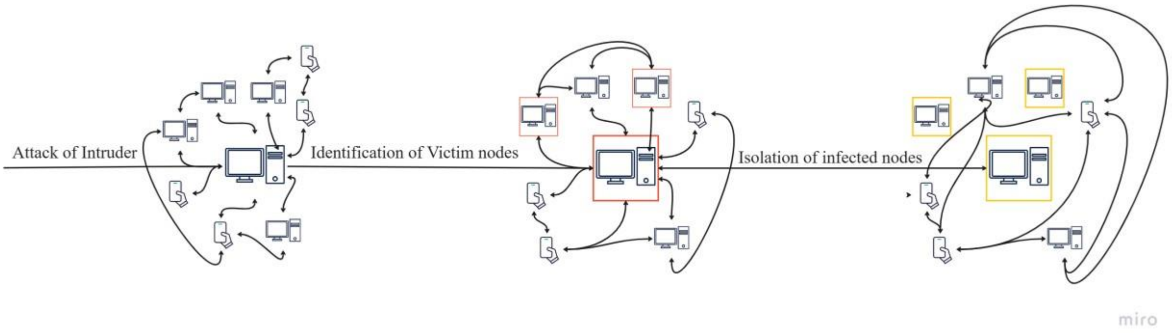


Fig 4.1: Flow Chart of Malicious Nodes Detection

4.6 Network Topology Design:

The network topology for our project consists of eight interconnected nodes, representing a simplified yet realistic network environment. Each node in the topology is configured to simulate specific network devices, such as routers, switches, or end hosts, depending on the requirements of the scenario. The topology is designed to facilitate packet transmission and interaction between nodes, enabling the simulation of various network protocols and behaviors. Nodes are strategically placed and interconnected to emulate typical network architectures and scenarios encountered in real-world deployments. By designing the network topology appropriately, we ensure that the simulation accurately reflects the complexities and challenges of real-world network environments, providing a robust platform for experimenting with DDoS detection and mitigation techniques.

4.7 Attack Simulation and Traffic Generation:

In our project, we simulate a Distributed Denial of Service (DDoS) attack by introducing a malicious node into the network topology. The malicious node is programmed to continuously transmit a large volume of data packets towards a target node, thereby flooding the target node with excessive traffic and disrupting its normal operation. The attack traffic generated by the malicious node is designed to mimic the characteristics of real-world DDoS attacks, such as high packet rates, varying packet sizes, and randomized source IP addresses. Additionally, we employ traffic generation techniques to simulate legitimate network traffic within the topology, providing a realistic background against which the DDoS attack can be detected and mitigated.

4.8 Detection and Mitigation Mechanisms:

To detect and mitigate the DDoS attack, we implement a combination of detection and mitigation mechanisms within the NS-3 environment. Detection mechanisms aimed at identifying patterns indicative of malicious activity in network traffic. Mitigation mechanisms encompass traffic filtering, rate limiting, and traffic diversion techniques, designed to mitigate the impact of the DDoS attack and restore normal network operation. These mechanisms are integrated into the network simulation to enable real-time monitoring and response to DDoS attacks, enhancing the resilience of the network against malicious incursions.

4.9 Implementation and Testing:

The implementation of DDoS detection and mitigation mechanisms within the NS-3 environment involves several steps, including scripting network behaviors, configuring detection algorithms, and implementing mitigation strategies. Each step is carefully executed to ensure the accuracy and effectiveness of the implemented mechanisms in detecting and mitigating DDoS attacks. Testing is conducted to validate the functionality and performance of the implemented mechanisms under various scenarios and conditions. Test scenarios include different types of DDoS attacks, varying network traffic loads, and different network topologies. Through rigorous testing and evaluation, we aim to verify the efficacy of the implemented mechanisms in defending against DDoS attacks and ensuring the resilience of network infrastructures.

Node no:	Counter no:	Traffic Encountered
7	1	84
7	2	87
7	3	78
7	4	16
7	5	94

Table 4.1 Traffic at Node 7(Victim Node)

Average Traffic at victim node	71.8
Minimum Traffic at victim node	16
Maximum Traffic at victim node	94
Standard Deviation at victim node	28.3718

Table 4.2 Observations made at Node 7(Victim Node)

5. Results

Our project successfully simulated a DDoS attack and implemented a isolated strategy to backoff DDoS attack in the NS-3. The results at each stage are listed below:

Stage 1: Network Creation & Malicious Node introduction

- We successfully created a network with eight nodes. C++ scripts effectively handled normal packet transmission between the nodes, confirming our ability to simulate network Communication.
- Introducing the malicious node (node 3) resulted in a surge of data packets directed towards node 7.

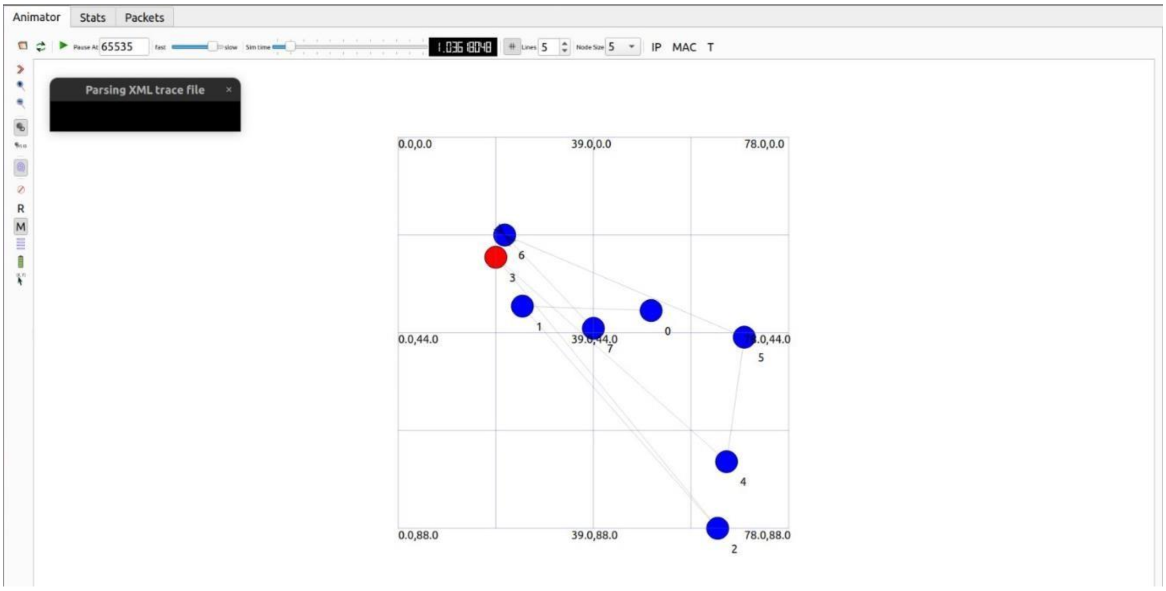
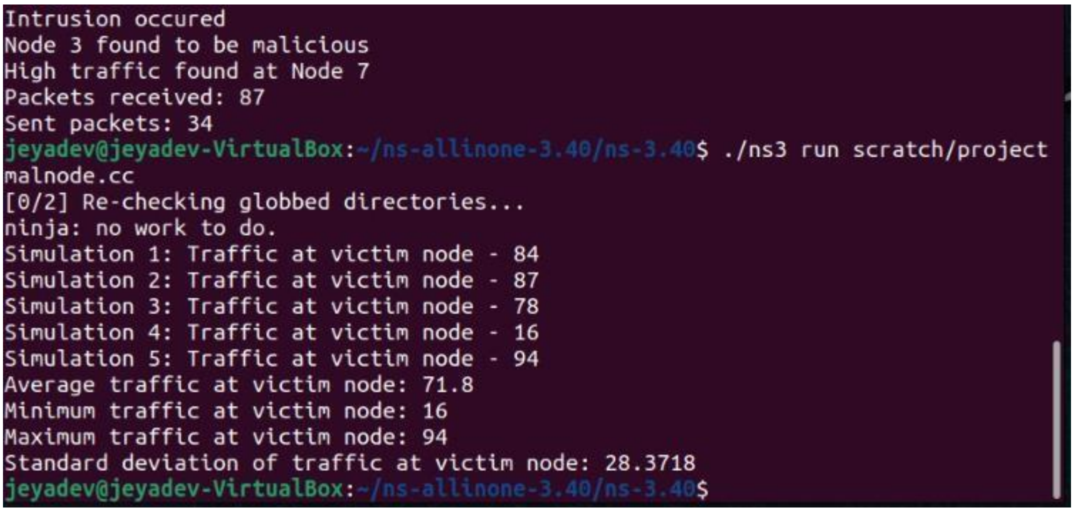


Fig-5.1: Introduction of Malicious node

Stage 2: Attack identification:

- By monitoring traffic at node 7, we observed a significant increase in data packets compared to normal operation.
- Running the script multiple times ensured the consistency of the observed behaviour, strengthening the evidence of a DDoS attack. Node 3, constantly transmitting data packets to node 7, became a strong suspect as the attacker.



```
Intrusion occured
Node 3 found to be malicious
High traffic found at Node 7
Packets received: 87
Sent packets: 34
jeyadev@jeyadev-VirtualBox:~/ns-allinone-3.40/ns-3.40$ ./ns3 run scratch/project
malnode.cc
[0/2] Re-checking globbed directories...
ninja: no work to do.
Simulation 1: Traffic at victim node - 84
Simulation 2: Traffic at victim node - 87
Simulation 3: Traffic at victim node - 78
Simulation 4: Traffic at victim node - 16
Simulation 5: Traffic at victim node - 94
Average traffic at victim node: 71.8
Minimum traffic at victim node: 16
Maximum traffic at victim node: 94
Standard deviation of traffic at victim node: 28.3718
jeyadev@jeyadev-VirtualBox:~/ns-allinone-3.40/ns-3.40$
```

Fig 5.2 Identification of Attack

Stage 3: Attack Mitigation

- Isolating nodes 3, 4, 5, 6, and 7 effectively stopped the flow of malicious packets from the attacker (node 3) to the victim (node 7).
- Nodes 0, 1, and 2 continued normal communication, demonstrating that our mitigation strategy protected unaffected parts of the network.

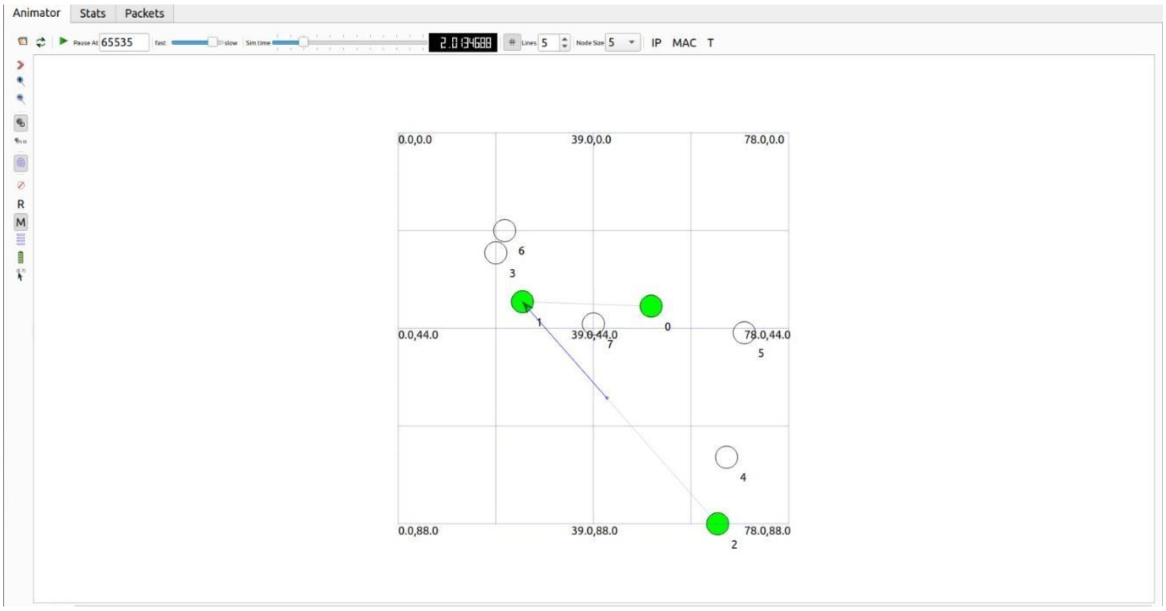


Fig 5.3 Attack Mitigation

6. Conclusion & Future Scope

6.1 Conclusion

This project successfully simulated a DDoS attack and mitigation strategy in NS-3. We achieved the following:

- Built a functional network with controllable packet transmission.
- Introduced a malicious node and observed its impact through simulated DDoS attack.
- Developed a strategy to identify and isolate the attack, protecting the victim node and unaffected parts of the network.
- Visualized the attack and mitigation process using NetAnim for better understanding. These results showcase the potential of NS-3 for simulating cybersecurity threats like DDoS attacks. It provides a valuable platform for students and researchers to explore various attack scenarios and develop mitigation techniques.

6.2 Future Scope

Our project lays a solid foundation for further exploration. Here are some exciting possibilities for future development:

- **Advanced Attack Scenarios:** We can incorporate more sophisticated DDoS attacks, like reflection attacks or amplification attacks, to test the resiliency of the network and mitigation strategies.
- **Scalability Testing:** We can increase the network size and observe the impact on attack effectiveness and mitigation efficiency. This can provide valuable insights into real-world large-scale network scenarios.
- **Machine Learning Integration:** Machine learning algorithms can be integrated to analyze network traffic patterns and automatically identify and respond to DDoS attacks.
- **Real-World Network Implementation:** While this project focused on simulation, the knowledge gained can be applied to develop and test mitigation strategies for realworld networks.

By continuing research and development in these areas, we can create more robust and secure networks that can effectively defend against evolving cyber threats.

7. References/Bibliography

[1] Abubakar, R., Aldegheishem, A., & Majeed, M. F. (n.d.). An Effective Mechanism to Mitigate Real-Time DDoS Attack. doi:10.1109/ACCESS.2020.2995820

[2] Ademola P. Abidoye, I. C. (n.d.). DDoS attacks in WSNs: detection and countermeasures. doi:https://doi.org/10.1049/iet-wss.2017.0029

[3] Ahmed Benmoussa, A. e. (n.d.). MSIDN: Mitigation of Sophisticated Interest floodingbased DDoS attacks in Named Data Networking. doi:10.1016/j.future.2020.01.043

[4] Ajeetha, G., & Priya, G. M. (n.d.). Machine Learning Based DDoS Attack Detection. doi:10.1109/i-PACT44901.2019.8959961

[5] arXiv. (n.d.). Distributed Denial of Service (DDOS) Attacks Detection Mechanism. doi:10.5121/ijcseit.2011.1504

[6] Devi, B. K., Preetha, G., Selvaram, G., & Shalinie, S. M. (n.d.). An impact analysis: Real time DDoS attack detection and mitigation using machine learning. doi:10.1109/ICRTIT.2014.6996133

[7] Kajwadkar, S., & Jain, V. K. (n.d.). A Novel Algorithm for DoS and DDoS attack detection in Internet Of Things. From https://ieeexplore.ieee.org/document/8722397

[8] Kanchan Kaushal, V. S. (n.d.). Early Detection of DDoS Attack in WSN. doi:10.5120/ijca2016908117

[9] Kaur, T., Saluja, K. K., & Sharma, A. K. (n.d.). DDOS attack in WSN: A survey. From https://ieeexplore.ieee.org/document/7939566

[10] Kavisankar, L., Chellappan, C., Venkatesan, S., & Sivasankar, P. (n.d.). Efficient SYN Spoofing Detection and Mitigation Scheme for DDoS Attack. doi:10.1109/ICRTCCM.2017.55

[11] Kumar, S., & Mann, K. S. (n.d.). Detection of Multiple Malicious Nodes Using Entropy for Mitigating the Effect of Denial of Service Attack in VANETs. From https://ieeexplore.ieee.org/document/8611036

[12] Kurniawan, M. T., & Yazid, S. (n.d.). Mitigation and Detection Strategy of DoS Attack on Wireless Sensor Network Using Blocking Approach and Intrusion Detection System. doi:10.1109/ICECCE49384.2020.9179255

[13] Luo, H., Lin, Y., Zhang, H., & Zukerman, M. (n.d.). Preventing DDoS attacks by identifier/locator separation. doi:10.1109/MNET.2013.6678928

[14] Maheshwari, V., Bhatia, A., & Kumar, K. (n.d.). Faster detection and prediction of DDoS attacks using MapReduce and time series analysis. doi:10.1109/ICOIN.2018.8343180

[15] Mauro Conti, C. L. (n.d.). Lightweight solutions to counter DDoS attacks in software defined networking. From https://link.springer.com/article/10.1007/s11276019-01991-y

[16] Nagar, S., Rajput, S. S., Gupta, A. K., & Trivedi, M. C. (n.d.). Secure routing against DDoS attack in wireless sensor network.

[17] Nisha Ahuja1, G. S. (n.d.). DDOS Attack Detection & Prevention in SDN. From https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8971596

[18] Pedro Manso 1, J. M. (n.d.). SDN-Based Intrusion Detection System for Early Detection and Mitigation of DDoS Attacks. doi:https://doi.org/10.3390/info10030106

[19] Poongodi, M., Hamdi, M., Sharma, A., Ma, M., & Kumar, P. (n.d.). DDoS Detection Mechanism Using Trust-Based Evaluation System in VANET. doi:10.1109/ACCESS.2019.2960367

[20] Qi Shi, M. M. (n.d.). Early detection and prevention of denial-of-service attacks: A novel mechanism with propagated traced-back attack blocking. doi:10.1109/JSAC.2005.854123

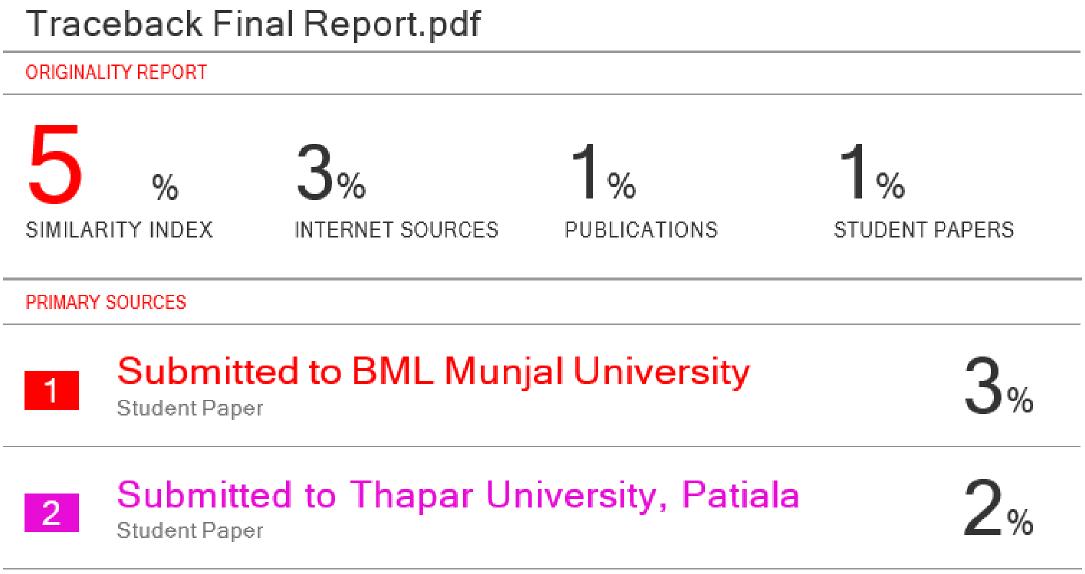
[21] Quyoom, A., Ali, R., Gouttam, D. N., & Sharma, H. (n.d.). A novel mechanism of detection of denial of service attack (DoS) in VANET using Malicious and Irrelevant Packet Detection Algorithm (MIPDA). doi:10.1109/CCAA.2015.7148411

[22] Song, A. Y. (n.d.). A Path Identification Mechanism to Defend against DDoS Attacks. From https://netsec.ethz.ch/publications/papers/pi.pdf

[23] Sumantra, I., & Gandhi, S. I. (n.d.). DDoS attack Detection and Mitigation in Software Defined Networks. doi:10.1109/ICSCAN49426.2020.9262408

[24] Wang, Q., Vu, L., Nahrstedt, K., & Khurana, H. (n.d.). MIS: Malicious Nodes Identification Scheme in Network-Coding-Based Peer-to-Peer Streaming. doi:10.1109/INFCOM.2010.5462226

[25] Zhijun Wu, W. F. (n.d.). Mitigation measures of collusive interest flooding attacks in named data networking. doi:https://doi.org/10.1016/j.cose.2020.101971



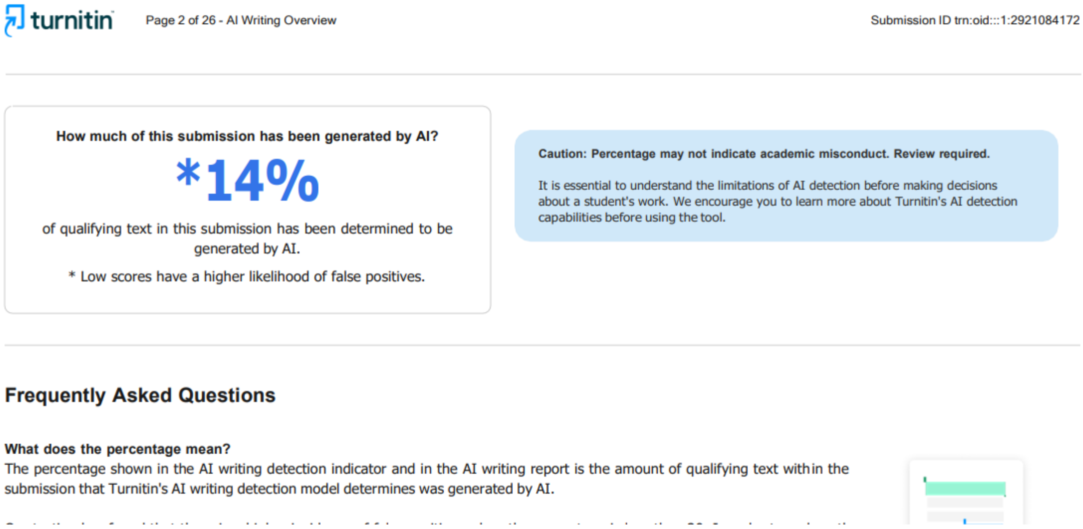
Traceback Final Report.pdf

ORIGINALITY REPORT

5 %	3%	1 %	1 %
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to BML Munjal University Student Paper	3%
2	Submitted to Thapar University, Patiala Student Paper	2%



turnitin Page 2 of 26 - AI Writing Overview Submission ID trn:oid:::1:2921084172

How much of this submission has been generated by AI?

*14%

of qualifying text in this submission has been determined to be generated by AI.

* Low scores have a higher likelihood of false positives.

Caution: Percentage may not indicate academic misconduct. Review required.

It is essential to understand the limitations of AI detection before making decisions about a student's work. We encourage you to learn more about Turnitin's AI detection capabilities before using the tool.

Frequently Asked Questions

What does the percentage mean?

The percentage shown in the AI writing detection indicator and in the AI writing report is the amount of qualifying text within the submission that Turnitin's AI writing detection model determines was generated by AI.