

Introduction

- Software-Defined Networking separates control and data planes, offering dynamic network management. [1]
- However, centralised controllers become single points of failure, making SDNs vulnerable to Distributed Denial of Service attacks. [2]
- Many existing detection solutions rely on complex machine learning models that require high computational resources.
- This project investigates a lightweight entropy-based method to detect DDoS traffic in real-time using an SDN testbed.

Methodology

- An SDN was emulated using Mininet, with the Ryu controller managing traffic flows via OpenFlow.
- A custom Python-based entropy detection algorithm was integrated into the controller to monitor the randomness of source IPs in real-time.
- Benign and malicious traffic were generated using hping3 to simulate normal network usage and DDoS attack.
- The system responded to significant drops in entropy by logging alerts and blacklisting attacker IPs.
- Key metrics evaluated included detection accuracy, latency, CPU and memory usage during attack scenarios.

Future Work

- Implement a dynamic threshold to improve adaptability of varying traffic patterns.
- Evaluate performance using more complex and realistic SDN topologies.
- Integrate additional attack types and detection features for broader threat coverage.
- Explore combining entropy-based detection with machine learning for hybrid models. [3]

Aim

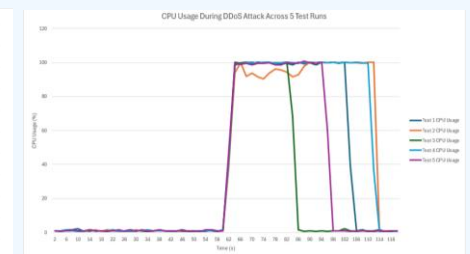
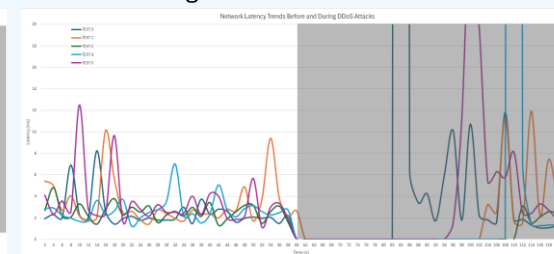
The aim of this project is to select an existing DDoS detection algorithm, implement a proof of concept within a simulated Software-Defined Network environment, and analyse and evaluate its effectiveness through experimental testing.

Objectives

- Conduct a systematic literature review on SDNs, DDoS attacks, and detection methods.
- Adapting to a suitable research methodology, including evaluation metrics and justification for the chosen detection method.
- Design and implement an SDN simulation using Mininet and the Ryu controller to test the selected DDoS detection method.
- Analyse and compare the detection method based on accuracy, latency, and resource usage, providing recommendations.

Results

- Entropy dropped significantly during DDoS traffic, enabling prompt detection.
- Detection accuracy: 100% (no false positives across 5 trials)
- CPU usage increased to 100% during attacks
- Latency spiked during attack, stable during detection and mitigation



Conclusion

- Successfully implemented a real-time entropy-based DDoS detection system in a simulated SDN environment.
- Achieved 100% detection accuracy across test runs with no false positives.
- The solution demonstrated low CPU and memory overhead, with minimal impact on network latency.
- Fully met the project's aim and objectives through functional design and practical evaluation.
- Demonstrated that entropy analysis is an effective lightweight approach for SDN security.

References

- [1] H. Yin and R. Duan, "Research on Table-Miss Attack Detection in SDN," 2022-08. doi: 10.1109/icfeict57213.2022.00088.
- [2] V. Prabhu and P. Balamurugan, "Survey on Security Based Approach to Prevent Attacks in SDN Using IoT Framework," 2023-07-19. doi: 10.1109/icecaa58104.2023.10212199.
- [3] J. Hussain and V. Hnamte, "A Novel Deep Learning Based Intrusion Detection System : Software Defined Network," 2021-09-29. doi: 10.1109/3ict53449.2021.9581404.