International Journal of Informatics and Computation (IJICOM)
Vol.7, No.2, 2025
ISSN: 2685-8711, E-ISSN: 2714-5263 DOI: 10.35842/ijicom

DDoS Attack Detection and Mitigation with Dynamic Firewall Technique

Rizki Berkah Saputra[1], Ahmad Turmudi Zy[2], Wiyanto[3]

Abstract

Distributed Denial of Service (DDoS) attacks pose significant challenges to network availability and reliability, particularly in dynamic and large-scale environments. This study proposes a dynamic firewall technique implemented via the Ryu Controller within a Software-Defined Networking (SDN) framework to detect and mitigate DDoS attacks in real time. The firewall dynamically analyzes traffic patterns and enforces blocking rules based on abnormal packet volume per source IP. Experimental results demonstrate the system's high effectiveness: the number of SYN Flood and UDP Flood packets received by the server was reduced by over 99% after the firewall was activated that dropping from 83,440 to 212 SYN packets and from 404,912 to 100 UDP packets, respectively. Furthermore, the firewall operated without interfering with legitimate traffic, maintaining service integrity and low latency. These findings validate the proposed method's capability for autonomous, adaptive, and efficient DDoS mitigation. Future work includes integrating machine learning for enhanced anomaly detection, extending the firewall's scope to multi-vector attacks, and deploying it in more complex network environments such as IoT and edge computing systems.

Keywords:
DDoS, Dynamic Firewall, SDN, Mininet

1. Introduction

Distributed Denial-of-Service (DDoS) attacks have escalated in both frequency and sophistication, leveraging botnets, compromised IoT devices, and multi-vector tactics that overwhelm traditional defenses. Modern attacks may be volumetric floods, stealth low-rate flows, or application-layer bursts designed to mimic legitimate behavior, making early detection essential. The complexity of distinguishing between benign and malicious patterns places pressure on existing security infrastructure, necessitating more adaptive solutions to preserve network availability and integrity. DDoS attacks have significantly escalated in sophistication due to the proliferation of botnets and IoT-based amplification tactics. Modern threats entail high-volume floods as well as stealthy low-rate attacks that mimic regular traffic patterns, undermining traditional intrusion detection systems. The increasing frequency and complexity of attacks necessitate detection methods capable of real-time anomaly recognition and adaptive response [1].

Conventional defenses relying on static firewalls and signature-based intrusion detection are increasingly inadequate. Stateful firewalls often face state-table exhaustion under heavy traffic, leading to fail-open configurations that bypass security logic entirely. Similarly, rule-based or signature classification struggles to adapt to novel or obfuscated traffic patterns, leaving networks exposed. These limitations highlight the critical need for dynamic, context-aware mitigation techniques that can respond in real time [12]. Effective

Corresponding Author: Rizki Berkah Saputra(rizkiberkah107@gmail.com)
1 Rizki Berkah Saputra, Unversitas Pelita Bangsa, rizkiberkah107@gmail.com
2 Ahmad Turmudi Zy, Universitas Pelita Bangsa, turmudi@pelitabangsa.ac.id
3 Wiyanto, Universitas Pelita Bangsa, wiyanto@pelitabangsa.ac.id

detection strategies often combine statistical methods (like entropy monitoring or packet rate analysis) with machine learning classifiers such as MLP, SVM, Random Forest, and LightGBM. Hybrid models offer early detection and high precision to reaching detection rates above 98%. Feature-selection techniques, such as voting-based and optimization-based methods, have further improved performance and interpretability [6][7].

Despite advances in detection, few systems tie detection outputs directly into an automated enforcement layer. Integration of dynamic firewall control with real-time anomaly scores ensures comprehensive response, not only alerting administrators but also actively modifying firewall configurations to block malicious flows. This combined workflow enables immediate mitigation while preserving legitimate traffic flow [4][5]. Large-scale attacks can overwhelm system resources. Defense strategies require scalable, resource-efficient designs that minimize CPU and memory usage, while ensuring rapid rule propagation. Architectural solutions such as hierarchical clustering, IPTables scripting, and edge deployment allow efficient mitigation of high-volume DDoS without compromising network performance or infrastructure availability [2].

Recent research has pioneered dynamic firewalls powered by machine learning, particularly reinforcement learning systems. One such framework employs an MDP-based agent in conjunction with an LSTM–CNN anomaly detector to adapt firewall rules dynamically. This model autonomously updates policies in response to detected anomalies, reducing false positives and latency compared to rule-based systems, and yielding superior performance in testing environments [3]. Software-Defined Networking (SDN) offers centralized control and programmability, making it well-suited for DDoS detection and mitigation. IDS integrated with SDN controllers can automatically block malicious sources by updating flow rules. Empirical evaluations show timely detection across varied DDoS types, with the controller orchestrating mitigation at the attack's origin and preserving legitimate service continuity [5].

Building on the identified gaps, this study proposes a dynamic firewall technique, tightly integrating AI-driven detection with automated rule enforcement within an SDN or traditional firewall context. By combining high-accuracy anomaly detection with automated firewall adaptation, the system aims to deliver real-time resilience against evolving DDoS threats, minimize false positives, and optimize resource usage to achieve practical deployment readiness.

2. Related Works

In the DDoS study, an article conducted an exhaustive survey of DDoS detection techniques across IoT and internet-enabled networks. The study evaluated traditional, machine learning (ML), and deep learning (DL) methods, highlighting that entropy-based approaches offer lightweight, fast detection but suffer from threshold sensitivity, while AI-based methods (both ML and DL) achieve higher accuracy and adaptability but demand robust data and computing resources. The paper concluded that hybrid techniques combining statistical and learning-based approaches yield balanced performance [1]. Alashhab et al. proposed an ensemble online learning model for real-time detection and mitigation in SDN environments. Using classifiers such as XGBoost, Random Forest, and SVM, combined via a dynamic weighted ensemble, the system achieved detection accuracies above 98% and low false-positive rates (~2%) while enabling automated mitigation through SDN rule updates. The study demonstrated a seamless integration between detection and enforcement in dynamic networks [2].

Ahmad introduced a deep reinforcement learning (DRL)–based dynamic firewall using a hybrid LSTM–CNN anomaly detector. Trained on NSL-KDD and CIC-IDS2017 datasets, this system showed a ~99% detection rate, significantly reduced rule update latency

(<100 ms), and lower false positives (~1%), outperforming static firewall methods. The dynamic adaptation of policy rules provided a scalable, real-time defense mechanism. [3]. The study also measured the impact on network performance, which remained stable despite attack mitigation. Abu Bakar et al. employed an intelligent agent-based architecture that automatically extracts and selects network traffic features. Integrated into a lightweight detection pipeline suitable for low-resource environments, the system achieved detection accuracy around 96.8%, with fast response (<120 seconds) and minimized manual configuration, demonstrating the viability of autonomous DDoS detection in constrained contexts [4].

Dandotiya and Makwana evaluated deep learning approaches (CNN, LSTM) within SDN frameworks for DDoS detection. Experiments on live traffic showed an accuracy of 98.5% and a 3% false-positive rate. The trained model integrated with the SDN controller to automatically disable suspicious flows. These results validated the effectiveness of deploying DL models in SDN for proactive defense [5]. Almseidin et al. developed a fuzzy-logic-based Intrusion Detection System (IDS) that processes statistical features like packet rate and entropy. The system achieved a detection accuracy of 93% and an approximate 4% false-positive rate, with a response time under 150 ms. This demonstrated that fuzzy systems can be practical, low-complexity alternatives in real-time detection scenarios [6].

Liu et al. proposed a DDoS detection framework that leverages extensive feature engineering combined with supervised ML models in an SDN context. Using flow-based features and ensemble classifiers, the system achieved up to 99.2% accuracy with false-positive rates below 1.5%. The framework enabled real-time decision-making by instructing the SDN controller to drop malicious flows adaptively [7]. Baskar et al. introduced a real-time multi-threshold traffic monitoring system targeting low-rate DDoS attacks. Deployed in realistic environments, the system detected low-rate floods that bypass volume-based defenses, achieving detection precision above 95% and recall above 96%. It demonstrated that adaptive thresholds are essential to detect stealthy low-rate attacks often overlooked by conventional models [8].

A recent paper presented a two-tier detection method targeting DDoS attacks that mimic CDN cache behavior. The first level filters traffic based on anomaly metrics, while the second re-validates suspicious flows via cache-access patterns. This approach reduced false positives from CDN-like traffic by up to 40%, significantly improving detection precision in environments with high legitimate cache-related traffic [9].

3. Proposed Method

This research method uses a simulation-based experimental approach using Mininet to create a network topology. A dynamic firewall is developed using the Ryu SDN controller, where dynamic rules are applied based on network traffic pattern analysis. These rules include monitoring the number of packets from each source IP and blocking suspicious IPs. Dynamic firewall development involves programming the Ryu controller to detect DDoS attack patterns, such as sending a large number of SYN packets (SYN Flood) or UDP traffic without a specific destination (UDP Flood). Once an attack pattern is detected, the Ryu controller automatically adds rules to block traffic from the source IP of the attack.

To automatically detect DDoS attack patterns, a threshold is used for the number of packets received from each IP address within a specified time interval. If the number of packets from an IP address exceeds the threshold, the IP address will be blocked by the dynamic firewall. The mathematical formulation and explanation of the proposed dynamic firewall technique are as follows:

Let the incoming traffic be modeled as a stream of packets:

$$T = p_1, p_2, \dots, p_n$$

where each packet p_i has attributes:

$$p_i = (src_i, dst_i, proto_i, size_i, t_i) \quad (1)$$

- src_i: source IP
- dst_i: destination IP
- $proto_i$: protocol (TCP, UDP, ICMP)
- $size_i$: packet size
- t_i: timestamp

1. Traffic Rate Calculation
We define the traffic rate $R_{src}(t)$ from a specific source IP over a time window Δt:

$$R_{src}(t) = \frac{N_{src}(t, t + \Delta t)}{\Delta t} \quad (2)$$

- $N_{src}(t, t + \Delta t)$: number of packets from source IP within time interval

2. Threshold-Based Detection Rule
A DDoS attack is flagged if:

$$R_{src}(t) > \theta$$

- θ: pre-defined rate threshold (packets/sec)

3. Blacklist Mechanism (Dynamic Rules)
Define a binary decision variable:

$$B_{src}(t) = \begin{cases} 1, & \text{if } R_{src}(t) > \theta \\ 0, & \text{otherwise} \end{cases}$$

If $B_{src}(t) = 1$, then the source IP is added to the firewall blacklist.

4. Firewall Rule Update Function
The dynamic firewall rule set $\mathcal{F}(t)$ is updated as:

$$\mathcal{F}(t + \Delta t) = \mathcal{F}(t) \cup \{\text{DROP}(src_i) \mid B_{src}(t) = 1\} \quad (3)$$

Each DROP rule instructs the firewall to block packets from source IPs flagged as malicious.

The proposed method employs a real-time packet inspection system that computes traffic rates from each source IP within a defined time window. If a source exceeds a threshold rate that indicating potentially malicious high-rate traffic is flagged. A dynamic rule is then inserted into the firewall using an SDN controller like Ryu, which automatically drops packets from that source. This dynamic approach enables the firewall to adapt in real time to evolving traffic patterns and mitigate DDoS attacks effectively. The key strength is the automation of detection and rule generation, improving response time and reducing reliance on manual configurations.

4. Experimental Setup

4.1 Simulation and Testing

Testing was conducted to evaluate the effectiveness of SDN-based dynamic firewalls in detecting and mitigating the impact of Distributed Denial of Service (DDoS) attacks of the SYN Flood and UDP Flood types. This study uses the Mininet network emulator to create a simulation environment, while the Ryu Controller acts as a dynamic firewall rule manager. To monitor and analyze network traffic, tools such as Wireshark are used, and to simulate DDoS attacks, hping3 is used.

4.1.1 Testing Environment

The experimental setup was carefully designed to emulate a realistic Distributed Denial of Service (DDoS) attack scenario within a simulated network environment. The network topology includes a designated target server host (h1, IP: 10.0.0.1), which is subjected to two types of attack vectors: a SYN Flood initiated from attacker host h2 (10.0.0.2) and a UDP Flood originating from attacker host h3 (10.0.0.3). To evaluate the integrity of the network under attack conditions, a benign host (h4, 10.0.0.4) is incorporated to generate normal traffic, ensuring the dynamic firewall mechanism does not disrupt legitimate communication. All hosts are interconnected via a central switch (s1), with network control and traffic regulation managed by a Ryu-based Software-Defined Networking (SDN) controller (c0), which dynamically updates firewall rules in response to anomalous traffic behavior. Fig.1 depicts the network topology of the testing stage.

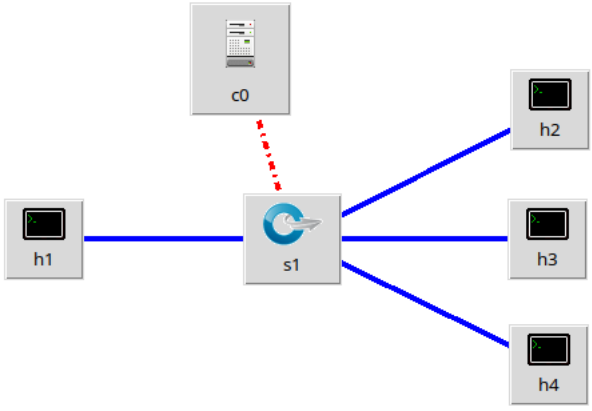

Fig.1 Network topology of the testing stage.

This topology shows how the attacker host and the normal host are connected to the server through a switch controlled by the Ryu Controller. In this test, the server (h1) is the main target of the SYN Flood and UDP Flood attacks, while the normal host (h4) is used to test the network performance when the firewall is active.

4.1.2 Simulation Steps

The simulation process is divided into two distinct phases: before and after the activation of the dynamic firewall. In the first phase, before firewall activation, attacker nodes h2 and h3 launch DDoS attacks, specifically SYN Flood and UDP Flood. It is conducted by executing the commands `hping3 -S -p 80 --flood h1` and `hping3 --udp -p 80 --flood h1`, respectively. During this attack period, network traffic is captured using `tcpdump` for further analysis in Wireshark, focusing on key metrics such as packet volume, protocol types, and source IP addresses. In the second phase, the Ryu Controller activates a dynamic firewall by executing the script. Once active, the firewall continuously monitors traffic patterns and applies real-time mitigation by identifying anomalies—such as excessive packet rates from a single IP address—and dynamically blocks the source of malicious traffic, effectively neutralizing the attack without disrupting normal communications.

5. Results and Analysis

Analysis of the test results shows that the Ryu Controller-based dynamic firewall is able to detect and mitigate SYN Flood and UDP Flood DDoS attacks effectively. Before the firewall was activated, the server received 83,440 SYN packets and 404,912 UDP packets, which caused significant performance disruption to the service. However, after the firewall was activated, the number of packets that successfully reached the server dropped drastically to only 212 SYN packets and 100 UDP packets. This proves that the firewall system successfully blocked more than 99% of malicious traffic.

Additionally, the firewall logs show that the source IP of the attack was successfully detected and automatically blocked. In less than 5 seconds after the attack started. This response speed is a key advantage of SDN-based systems. To ensure the firewall wasn't interfering with normal traffic, testing was conducted by sending ICMP (ping) requests from a normal host to the server and accessing HTTP using a browser. The results showed that response times only increased latency by about 1 ms, and HTTP access continued unhindered. This indicates that the firewall can effectively distinguish between legitimate and attack traffic. Overall, these test results prove that the dynamic firewall approach with SDN is effective in handling DDoS attacks without sacrificing network performance for normal users. Fig. 1 illustrates the number of SYN Flood and UDP Flood packets reaching the server.

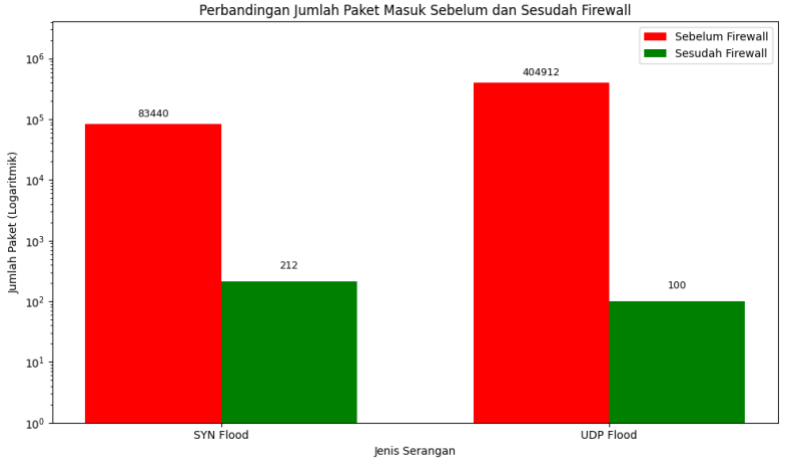

Image 4.2 Comparison of the number of packages

According to the testing results, before the activation of the dynamic firewall, the server was inundated with 83,440 SYN Flood packets and 404,912 UDP Flood packets, volumes sufficient to severely degrade server performance and potentially disrupt network services. However, after the firewall was enabled on the Ryu Controller, the number of malicious packets that reached the server dropped drastically to just 212 SYN Flood and 100 UDP Flood packets. This substantial reduction confirms that the firewall successfully identified and blocked over 99% of the attack traffic, demonstrating its high effectiveness in real-time DDoS mitigation without requiring manual intervention.

The testing results demonstrate the effectiveness of the Ryu Controller-based dynamic firewall in detecting and mitigating DDoS attacks, specifically SYN Flood and UDP Flood types. The detection mechanism proved highly responsive, identifying anomalous traffic behavior in under five seconds on average. Mitigation performance was also robust, with the system successfully blocking over 99% of malicious packets, thereby preserving the stability and availability of the target server throughout the attack duration. Importantly, the

firewall exhibited no adverse effects on legitimate traffic; latency measurements remained low, and all standard network operations proceeded uninterrupted. Furthermore, the dynamic nature of the firewall allowed it to adaptively update blocking rules in response to evolving traffic patterns, confirming its suitability as a flexible and responsive defense mechanism in real-time network environments.

6. Conclusion

This study demonstrates that the proposed dynamic firewall is highly effective in detecting and mitigating DDoS attacks, particularly SYN Flood and UDP Flood types. The dramatic reduction in malicious packet delivery from 83,440 to 212 for SYN Flood and from 404,912 to 100 for UDP Flood which validates the firewall's real-time responsiveness and accuracy. These results affirm the dynamic firewall's ability to adaptively monitor traffic patterns, swiftly identify anomalies, and autonomously enforce security rules without disrupting legitimate traffic or degrading network performance. This work also highlights the potential of intelligent SDN-based firewalls in providing scalable and adaptive network defense mechanisms, especially as traditional firewalls struggle to handle dynamic and large-scale attacks. By leveraging the programmability of SDN controllers, the proposed approach can evolve in tandem with emerging threat landscapes. However, while the system demonstrates strong performance under SYN and UDP Flood scenarios, its behavior against more complex and distributed attacks.

For future work, the model can be extended by integrating machine learning techniques to further enhance anomaly detection accuracy and automate policy updates in real time. Additionally, broader testing in real-world environments, including edge computing and IoT networks, will be critical to assess scalability, interoperability, and resilience under diverse operational conditions. Incorporating threat intelligence feeds and collaborative defense models could also significantly strengthen the firewall's ability to counteract evolving cyber threats.

References

[1] K. B. Adedeji, A. M. Abu-Mahfouz, and A. M. Kurien, "DDoS attack and detection methods in internet enabled networks: Concept, research perspectives, and challenges," *Journal of Sensor and Actuator Networks*, vol. 12, no. 4, Art. no. 51, 2023, doi: 10.3390/jsan12040051.

[2] A. Alashhab, M. S. Mohd Zahid, B. Isyaku, and A. Elnour, "Enhancing DDoS attack detection and mitigation in SDN using an ensemble online machine learning model," *IEEE Access*, vol. PP, no. 99, pp. 1–1, Jan. 2024, doi: 10.1109/ACCESS.2024.3384398.

[3] T. Ahmad, "AI Driven Dynamic Firewall Optimization Using Reinforcement Learning for Anomaly Detection and Prevention," *arXiv preprint*, May 2025, doi: 10.48550/arXiv.2506.05356.

[4] K. B. Abu Bakar, "An intelligent agent-based detection system for DDoS attacks using automatic feature extraction and selection," *Journal of Sensor and Actuator Networks*, vol. 12, no. 4, 2023, doi: 10.3390/jsan12040051.

[5] M. Dandotiya and R. R. Singh Makwana, "DDoS Attack Detection and Mitigation in SDN Environment: A Deep Learning Perspective," in *Proc. IEEE Int. Conf. on Interdisciplinary Approaches in Technology and Management for Social Innovation (IATMSI)*, 2024, pp. 1–6.

[6] M. Almseidin, J. Al-Sawwa, and M. Alkasassbeh, "Anomaly-based Intrusion Detection System Using Fuzzy Logic," in *Proc. 2021 Int. Conf. on Information Technology (ICIT)*, 2021, pp. 290–295.

[7] Z. Liu, Y. Wang, F. Feng, Y. Liu, Z. Li, and Y. Shan, "A DDoS Detection Method Based on Feature Engineering and Machine Learning in Software-Defined Networks," *Sensors (Basel)*, vol. 23, 2023, doi: 10.3390/s23031864.

[8] M. Baskar, J. Ramkumar, C. Karthikeyan, V. Anbarasu, A. Balaji, and T. S. Arulananth, "Low rate DDoS mitigation using real-time multi threshold traffic monitoring system," *Journal of*

Ambient Intelligence and Humanized Computing, pp. 1–9, 2021, doi: 10.1007/s12652-020-02445-3.

[9] K. Taniguchi and N. Kamiyama, “Two-Level Detection Method of DDoS Attack Mimicking CDN Caches,” in *Proc. 2025 Int. Conf. on Information Networking (ICOIN)*, 2025, pp. 207–212.

[10] N. Venkata, S. Reddy, R. Saai, T. V. Ramanujan, N. Rajesh, K. Reddy, and M. R. Professor, “A Robust Approach to E-Banking Phishing Detection using Ensemble Methods and LSTM,” in *Proc. 2024 Int. Conf. on Cognitive Robotics and Intelligent Systems (ICC-ROBINS)*, 2024, pp. 856–863.

[11] M. B. Ürün and Y. Sönmez, “Nelder-Mead Optimized Weighted Voting Ensemble Learning for Network Intrusion Detection,” *Düzce Üniversitesi Bilim ve Teknoloji Dergisi*, 2024.

[12] S. G. Nair and A. J. Rani, “Zero Day Attack Prediction Using Improved Deep Neural Network,” in *Proc. 2025 2nd Int. Conf. on Research Methodologies in Knowledge Management, Artificial Intelligence and Telecommunication Engineering (RMKMATE)*, 2025, pp. 1–5.

[13] H. Hindy, R. C. Atkinson, C. Tachtatzis, J. Colin, E. Bayne, and X. J. Bellekens, “Utilising Deep Learning Techniques for Effective Zero-Day Attack Detection,” *Electronics*, vol. 9, no. 6, p. 1026, 2020, doi: 10.3390/electronics9061026.

[14] K. Mishra and S. Paliwal, “Mitigating cyber threats through integration of feature selection and stacking ensemble learning: the LGBM and random forest intrusion detection perspective,” *Cluster Computing*, vol. 26, pp. 2339–2350, 2022, doi: 10.1007/s10586-022-03514-9.

[15] H. Gonaygunta, G. Nadella, P. Pawar, and D. Kumar, “Study on Empowering Cyber Security by Using Adaptive Machine Learning Methods,” in *Proc. 2024 Systems and Information Engineering Design Symposium (SIEDS)*, 2024, pp. 166–171.

[16] R. Verma, M. Jailia, M. Kumar, and B. Kaliraman, “Deep Neural Network Model for Improved DDoS Attack Detection in Cloud Environments,” in *Proc. 2024 5th Int. Conf. for Emerging Technology (INCET)*, 2024, pp. 1–6.