IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

AI-Driven Ddos Attack Detection And Mitigation System

Prof. Namrata Jangam[1], Miss. Samruddhi Shirsat[2], MR. Sushant Giramkar[3], Mr. Ritesh Ganghthade[4], Mr. Srujan Mailare[5]

, Department of Computer Engineering, VPS College of Engineering and Technology, Lonavala[1]

Student, Department of Computer Engineering, VPS College of Engineering and Technology, Lonavala[1]

Abstract:

Distributed Denial-of-Service (DDoS) attacks have become a serious problem in cybersecurity. This can cause temporary or long-term loss of service to users. These attacks mainly target e-commerce platforms, online services, and financial institutions. Detecting DDoS attacks is essential because they cause serious problems. Detection of DDoS attacks can be effectively achieved using supervised machine learning techniques. This project presents an approach for detecting Distributed Denial of Service (DDoS) attacks using Support Vector Machine (SVM), a supervised machine learning algorithm. The methodology involves storing network traffic data in SQLite3 for efficient management and retrieval. The collected data undergoes preprocessing, including the handling of missing values and feature scaling with StandardScaler, to enhance the accuracy and robustness of the detection model. Experimental results highlight the effectiveness of SVM in distinguishing between normal and malicious traffic, thereby contributing to improved network security.

In this paper, we propose new techniques for launching and mitigating DDoS attacks that clearly outperform existing techniques. We also classify DDoS attack techniques as well as the techniques used in their detection, and thus try to provide a broad scoping of the DDoS problem. We also compare our attack module with some of the available tools.

Keywords: DDoS detection, machine learning, deep learning, anomaly detection, network security.

1. Introduction

Distributed denial-of-service (DDoS) attacks have attracted widespread attention in cyberspace in recent years. In recent years, the concepts and techniques of software-defined networking (SDN) have been introduced and extensively researched. DDoS attacks can threaten the availability of SDN due to the difference in architecture between SDN networks and traditional networks. In particular, the SDN controller is the most vulnerable part affected by DDoS attacks. In general, a DoS attack is an attempt to make network resources unavailable to legitimate users. In [1], they launched a DoS attack on SDN using the different logic of SDN in the control-data plane and developed a network scanning tool that can identify SDN networks. In their method, since the flow response time for existing and new flows in the data path due to the controller's query has different values, the time values were collected by the scanner based on the header field. The header field could be changed to scan the network.

In [2], they proposed a DDoS attack on an SDN controller where the attacker continuously sends IP packets with random headers to disrupt the controller. A secondary controller was adopted to improve resilience. However, a DDoS detection mechanism was required because the secondary controller may also be vulnerable to DoS or DDoS attacks. In [3], they proposed the use of multiple controllers still could not completely solve the problem of DDoS attacks because it could lead to cascading faults of multiple controllers.

In [4], they presented a new method that only used single flow information and IP entropy characteristic information. Although their experimental results showed that their method had high detection accuracy, more technology was needed to determine the threshold and multi-component weight distribution. In [5], they proposed to combine the Support Vector Machine classification algorithm (known as SVM) to build a DDoS attack model. Their experimental results showed a low false alarm rate for TCP and UDP traffic, but a high false alarm rate for ICMP traffic.

In [6], Software-defined networking (SDN) is an emerging paradigm that is changing how computer networks are designed, managed, and operated. Its core idea is to separate the network's control plane (which makes decisions about where to send traffic) from the data plane (which forwards traffic based on those decisions). This separation enables programmability, centralized (or logically centralized) network control, and rapid adaptation to changing network conditions. Traditional networks tightly integrate control and forwarding logic into single devices (routers, switches). This leads to several limitations: network configuration is complex and often device-vendor specific; policies are difficult to enforce uniformly; dynamic changes (e.g., responding to failures, load spikes, or security threats) are difficult to implement quickly. SDN is motivated by the need to overcome these limitations.

In [7]-[9], they proposed some DDoS detection methods. However, these methods were vulnerable to other factors, and the research results of these methods showed that behavioural features were very important for DDoS detection in SDN. Therefore, in this paper, we proposed several features to provide suggestions for DDoS detection in SDN networks and analysed the traffic behaviour including DDoS attacks. Furthermore, we have proposed a DDoS detection algorithm based on the degree of attack (called

DDADA) and a DDoS detection algorithm based on machine learning (called DAMDL). The proposed algorithm can effectively detect DDoS attacks in an SDN environment.

The following points: First, they propose four features (called flow length, flow duration, flow size, and flow rate) to evaluate the performance of DDoS attack detection when a DDoS attack occurs on an SDN controller. Second, for the first time, a new concept called 'attack degree' is proposed to detect DDoS attacks. Third, based on this concept, a detection algorithm based on attack degree (called DDADA) is proposed. And finally, to further improve the detection efficiency, another detection algorithm based on machine learning (called DDAML) is introduced to detect DDoS attacks.

2. Related Work

DDoS attack detection is at the intersection of network security, machine learning, and traffic analysis. Over the past few years, various approaches have been proposed to identify attack patterns, separate malicious traffic from legitimate flows, and mitigate the impact of attacks. Below, we review the most relevant directions of previous work.

In [10] The network attacks are increasing both in frequency and intensity with the rapid growth of internet of things (IoT) devices. Recently, denial of service (DoS) and distributed denial of service (DDoS) attacks are reported as the most frequent attacks in IoT networks. The traditional security solutions like firewalls, intrusion detection systems, etc., are unable to detect the complex DoS and DDoS attacks since most of them filter the normal and attack traffic based upon the static predefined rules. However, these solutions can become reliable and effective when integrated with artificial intelligence (AI) based techniques. During the last few years, deep learning models, especially convolutional neural networks, achieved high significance due to their outstanding performance in the image processing field. The potential of these convolutional neural network (CNN) models can be used to efficiently detect the complex DoS and DDoS by converting the network traffic dataset into images. Therefore, in this work, we proposed a methodology to convert the network traffic data into image form and trained a state of- the-art CNN model, i.e., ResNet over the converted data. The proposed methodology accomplished 99.99 percent accuracy for detecting the DoS and DDoS in case of binary classification. Furthermore, the proposed methodology achieved 87 percent average precision for recognizing eleven types of DoS and DDoS attack patterns which is 9 percent higher as compared to the state-of-the-art.

In [11], Wireless Sensor Network (WSN) has a big role in several fields such as military, health and even information technology such as IoT (Internet of Things). Besides having many benefits, WSN has a disadvantage in its application where there is no built-in security system embedded in the sensor device due to limitations possessed by sensor nodes such as memory, processor, and battery. As a result, WSN is vulnerable to attacks, one of the main attacks on WSN is the DoS attack. DoS attacks aim to prevent users legitimate from using resources by reducing existing resources until the network resources are busy, the network becomes slow until finally off. So, we need to detect, mitigate DoS attacks so that these attacks can be stopped. In this study, the method of detecting and mitigating DoS attacks uses a signature-based Intrusion Detection System (IDS) by implementing a blocking approach on the attack

node by blocking all packets originating from the attacker until the attacker runs out of energy. The blocking approach was successfully implemented on the WSN network when IDS detected a DoS attack. So, the method of blocking approach can be used as a mitigation of DoS attacks by blocking all packets sourced from the attacker.

In [12], This paper investigates the memory adaptive event triggered (MAET) fault detection and isolation (FDI) problem for nonlinear networked control systems under periodic denial-of service (DoS) attacks, where the nonlinear systems are described by Takagi–Sugeno (T–S) fuzzy models with unknown membership functions. First, a novel event-triggered mechanism is proposed to save communication resources. The triggering threshold is adaptively adjusted by multiple previous sampled data, not only depending on the latest triggering data. Second, taking DoS attacks and event-triggered mechanisms into consideration, a switching state-feedback controller is established and the exponential stability is derived. Meanwhile, the controller and the event-triggered mechanism are simultaneously developed based on a piecewise Lyapunov function. Then, a set of switching T– S fuzzy observers are constructed to realize FDI under DoS attacks. Besides, a switching variable method is introduced to address the asynchronous premise variables problem caused by the event-triggered mechanism. Finally, simulation cases are given to demonstrate the validity and merit of the proposed FDI scheme.

In [13], Information security is integral to any organization aiming to protect its intellectual property in the face of escalating and increasingly novel cyberattacks.1 Among these, denial-of service (DoS) attacks—in which attackers typically send a volume of connection or information requests to overload the target system—have earned the reputation as one of the most severe threats because they can shut down the availability of a host, router, or even an entire network. The attacked system can be forced out of service as quickly as a few minutes and remain that way for days, forcing the victimized organization to incur significant losses. Additionally, a number of toolkits for launching a DoS attack are freely available and easy to operate.2 Compounding the problem is the growth of the Internet of Things (IoT), which is expected to dramatically change the nature and size of DoS attacks. This does not bode well for existing techniques to detect DoS attacks, which tend to scale poorly. The solution might lie in some form of anomaly detection, which aims to identify anomalous or abnormal data from a given dataset, often discovering new and rare patterns. Also known as outlier, novelty, or deviation detection or exception mining, anomaly detection has been widely studied in statistics and machine learning. Unfortunately, traditional techniques which are based on nearest neighbour, clustering, and statistics—assume that individual data instances are anomalous, an assumption that does not align with DoS attack characteristics.

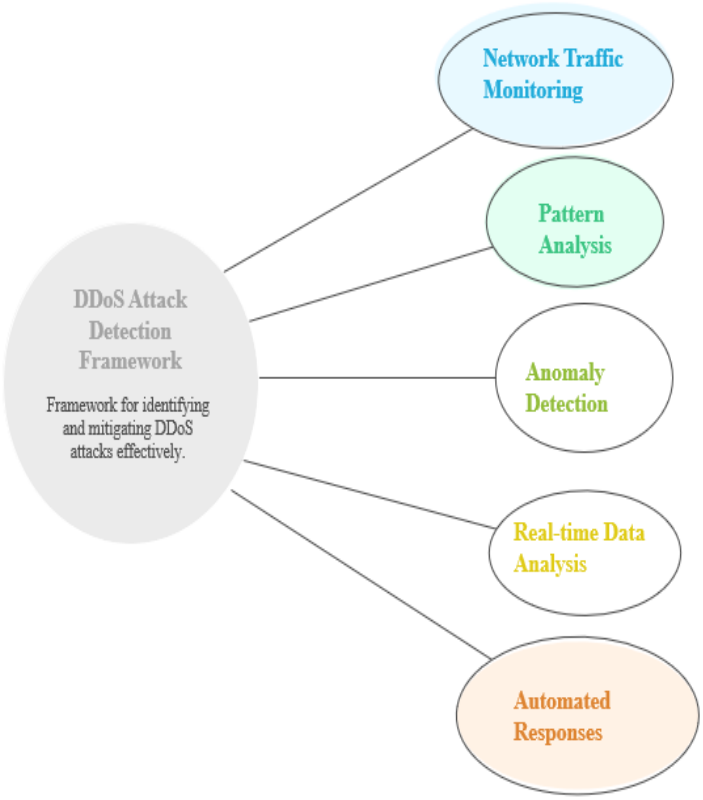

Fig 1: DDoS attack detection system frame work

This diagram shows a DDoS attack detection framework, which is designed to effectively detect and mitigate Distributed Denial of Service (DDoS) attacks. The core is the framework itself, which is surrounded by five essential components. Network traffic monitoring is the first stage, where traffic flows are continuously monitored to capture key statistics such as packet count, byte count, and flow duration. This is followed by pattern analysis, where normal and abnormal traffic behaviors are studied to identify deviations. The anomaly detection module then flags unusual or suspicious activities that may indicate the beginning of an attack. To ensure timely action, the system incorporates real-time data analytics, which processes traffic characteristics for immediate classification. Finally, automated responses are triggered by the framework, allowing the system to dynamically block malicious IPs, throttle abnormal flows, or redirect suspicious traffic into sinkholes. Together, these modules enable an intelligent, adaptive, and proactive defence against DDoS threats.

3. System Architecture

Our proposed framework is designed to detect distributed denial of service (DDoS) attacks by combining network traffic features and temporal patterns into a unified representation and optimizing them for accurate and timely attack detection. The model consists of five main stages:

3.1 Data Collection

In [14], A data Collection for DDoS attack detection typically collects features such as packet rate, packet size, source and destination IP addresses, traffic volume, flow duration, protocol type, and entropy measurements of IP addresses or packet properties (e.g., Shannon entropy). It may also include statistical features such as the number of TTL values, packet inter-arrival times, and multi-entropy metrics to effectively capture traffic behavior and anomalies.

- ***Packet Count Per Flow*:**

This metric represents the total number of packets transmitted in a specific flow on the network. Monitoring packet counts can help identify unusual patterns, such as sudden increases in packet counts that may indicate flooding attacks such as SYN floods or UDP floods. Under normal circumstances, the packet count per flow remains within a predictable range depending on the type of application or service. When attackers generate a large number of packets in a very short period of time, the deviation becomes a strong indicator of malicious behavior. In the following equation is N = Total number of packets detected in the stream.

$$\text{Packets flow} \sum_{i=1}^{N} N = 1 \quad \text{..... (1)}$$

- ***Bytes Per Flow:***

The total number of bytes transmitted per flow provides insight into the volume of data being exchanged. This metric complements packet counts by distinguishing between high-volume, low-packet flows (such as file transfers) and high-packet, low-byte flows (such as ping floods). Comparing packet counts and byte counts together allows for more accurate traffic classification. For example, a DDoS attack may generate many small-sized packets, resulting in a disproportionately high packet count but relatively low total bytes.

$$\text{Number of bytes} = i = 1 \sum \text{NSize} \quad \text{.....(2)}$$

- ***Flow duration:***

Flow duration is the total time from the time the first packet of a flow is seen until the end of the flow. This metric is useful for identifying persistent malicious flows or unusually short-lived connections. For example, legitimate web sessions typically last a few seconds or minutes, while attack traffic may consist of numerous very short connections designed to overwhelm the target server. Unusually long-lived flows can also indicate malicious activity, such as stealth scanning or unauthorized persistent connections.

$$\text{FlowDuration}(f) = T_{last}(f) - T_{first}(f) \quad \text{.....(3)}$$

This equation contains Tfirst(f) = timestamp of the **first packet** in the flow, Tlast(f) = timestamp of the **last packet** in the flow.

- ***Packet header (source/destination IP, source/destination port, protocol type):***

Packet header information provides contextual details about the traffic flow. The source and destination IP addresses reveal the origin and destination of the traffic, which can be cross-referenced with blacklists or reputation databases to detect malicious hosts. Source and destination ports identify the services being accessed (e.g., HTTP on port 80, DNS on port 53), helping to differentiate between normal and suspicious traffic. Protocol type (TCP, UDP, ICMP, etc.) adds further classification, as DDoS attacks often use specific protocols such as UDP or ICMP. Together, these header fields allow for flow identification, anomaly detection, and rule enforcement by the SDN controller.

- ***Traffic counters (total packets/bytes per switch, port, or time interval):***

Traffic counters provide aggregate statistics about how much data is passing through a switch, port, or the entire network during a given period of time. These counters help track bandwidth usage, detect traffic spikes, and identify bottlenecks. For example, if a port suddenly shows an exponential increase in packet or byte count, it could indicate that the port is being targeted in a DDoS attack. Monitoring counters over time intervals also supports time-series analysis, which is valuable in detecting anomalies, establishing baselines, and predicting future network loads.

3.2 Data Preprocessing

In [15,16], Data preprocessing is a very important and underestimated step in the machine learning pipeline. It provides a clean and relevant dataset that can then be used in subsequent steps such as classification or regression. Support Vector Machine (SVM) is proposed for image segmentation. SVM is a learning machine algorithm, which can reduce segmentation errors caused by fast object motion. First, it is used to derive object approximations by combining frame differences with mathematical morphology.

- ***Data Cleaning:***

Data cleaning is the process of removing or correcting errors, anomalies, and irrelevant information from raw network traffic before using it for analysis or discovery. Raw packet/flow data collected from routers, switches, or sensors can be noisy, incomplete, or redundant, so cleaning ensures that the dataset is accurate, reliable, and usable

- ***Data Normalization:***

Data normalization is the process of adjusting the values of different features to a common scale without distorting their relative differences. In networking, raw features (such as packet counts, byte counts, flow counts) can have very different ranges.

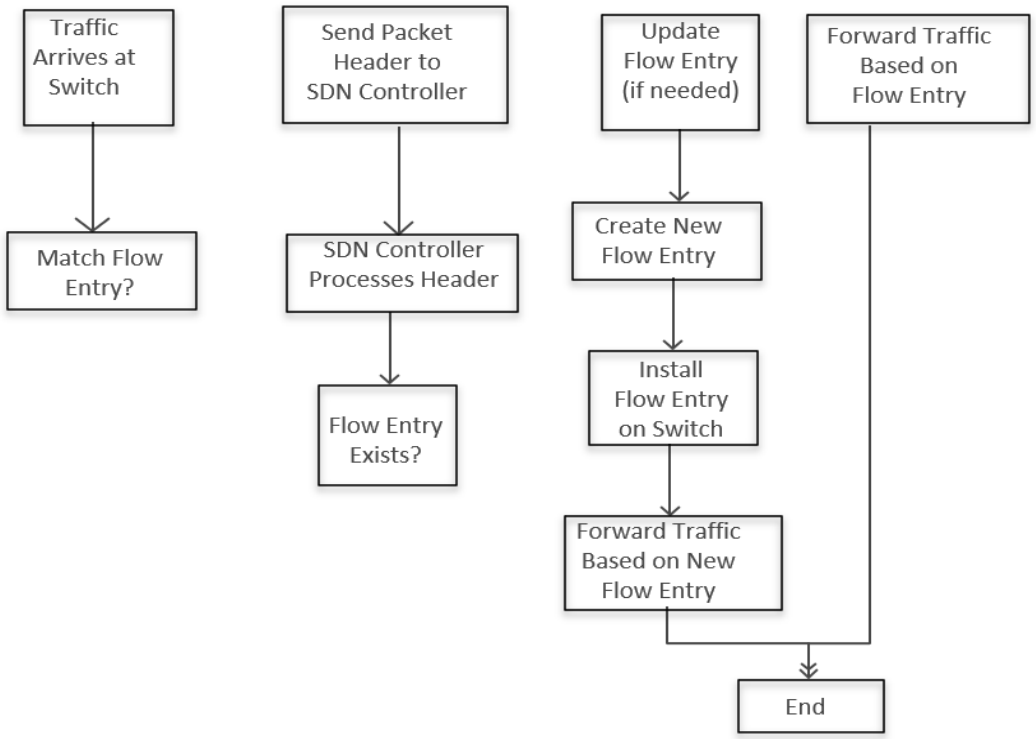

Fig 2: SDN Traffic Management Flowchart

- ***Handling Missing Values:***

In a network traffic dataset, some features may be missing due to packet drops, logging errors, or incomplete flow statistics. To ensure consistency: Numerical features (e.g., packet count, byte count) are replaced with 0 or the median value of the feature in the dataset. Here, where □□ is the i-th observation of feature X. In the given equation. Formula (Middle Imputation):

$$x=\{xi = \{xi, median(X), if\ xi\ is\ not\ missing, if\ xi\ is\ missing\} \ldots\ldots\ldots\ldots\ldots\ldots(4)$$

Here, replacing missing values prevents the ML model from failing or producing biased results. Median is preferred for skewed distributions common in network traffic.

- ***Outlier Handling:***

Network traffic often contains extreme spikes, such as burst traffic or measurement anomalies. Outliers can distort ML models. In 1st Approach Removal – Discard flows that lie beyond a threshold (e.g., 3 standard deviations from the mean). In 2 Approach Capping – Limit extreme values to a maximum threshold.

$$Z=\frac{xi-\mu}{\sigma} \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(5)$$

Here they used the following functions, xi = feature value, μ= mean of the feature,□ = standard deviationPrevents extreme DDoS bursts from dominating the training process. Ensures the SVM can learn patterns from both normal and attack traffic.

- ***Feature Extraction:***

In [17-19] Immediately after preprocessing comes the feature extraction module. Its job is to transform the clean and prepared traffic data into meaningful features that highlight the differences between normal and malicious traffic. These features are then used by the detection/ML model.

- ***Traffic volume features:***

Traffic volume features describe the amount of data and the number of packets flowing through a network at a given time and are the most important indicators for detecting DDoS attacks. These features include metrics such as packet count (total number of packets observed), byte count (total number of bytes transmitted), and flow count (number of unique connections based on source-destination pairs). They can also capture averages such as packets per flow or bytes per flow, along with their variances, which reflect how evenly the traffic is distributed across different flows. Under normal circumstances, traffic volume shows stable patterns, but during a DDoS attack, these features often exhibit unusual spikes - such as an unusually high number of packets in a short time or a sudden increase in the number of flows due to spoofed IPs. Monitoring traffic volume features helps to quickly identify flooding behavior, bandwidth exhaustion, and resource overuse, making them fundamental for distinguishing between normal network usage and attack scenarios.

- ***Time-based features:***

Time-based features capture how network traffic behaves over time. They include metrics such as packet inter-arrival time, flow duration, packet rate, and bursts at specific intervals. In normal traffic, these values remain relatively constant, reflecting regular communication patterns. During a DDoS attack, sudden spikes, irregular intervals, or extremely high packet rates can be observed, making time-based features important for detecting unusual increases in traffic.

- ***Source and destination features:***

Source and destination features focus on the relationship between the sender and receiver of network traffic. They include metrics such as the number of unique source IPs contacting the target, the entropy of the source IPs (to detect spoofing or distributed attacks), and the diversity of destination ports being accessed. These features help uncover unusual patterns, such as thousands of spoofed IPs hitting a single victim or attackers flooding multiple ports at once. By monitoring the source-destination ratio and

entropy, DDoS detection systems can differentiate between normal client behavior and malicious attack traffic.

- ***Flow behavioural characteristics:***

Flow behavioural characteristics describe how network flows behave during communication between a source and a destination. They capture patterns such as one-way versus two-way traffic, where DDoS attacks often create multiple one-way flows without proper responses. Metrics such as request-to-response ratio and incomplete handshakes reveal unusual imbalances, such as in SYN floods where connections are left half-open. By analyzing these behaviours, the system can detect anomalies that distinguish normal user activity from malicious attack traffic.

- ***Statistical and entropy features:***

Statistical and entropy features capture the variability and randomness of network traffic to distinguish normal and abnormal behavior. Statistical features such as mean, variance, and standard deviation describe packet size, flow duration, and inter-arrival times, highlighting sudden deviations. Entropy measures, based on information theory, measure the randomness or uniformity of a distribution, such as source IP, port, or packet size. In DDoS attacks, entropy often decreases (e.g., many packets from a few IPs) or increases abnormally, making these features powerful for detection.

3.3 DDoS Attack Detection

In [20-22] Describe how different machine learning and deep learning techniques such as Support Vector Machine (SVM), Random Forest (RF) and hybrid deep learning models like CNN-BiLSTM are used to detect attacks. Highlight their working principles, advantages, limitations and how they contribute to identifying unusual traffic patterns.

- **Support Vector Machine (SVM):**

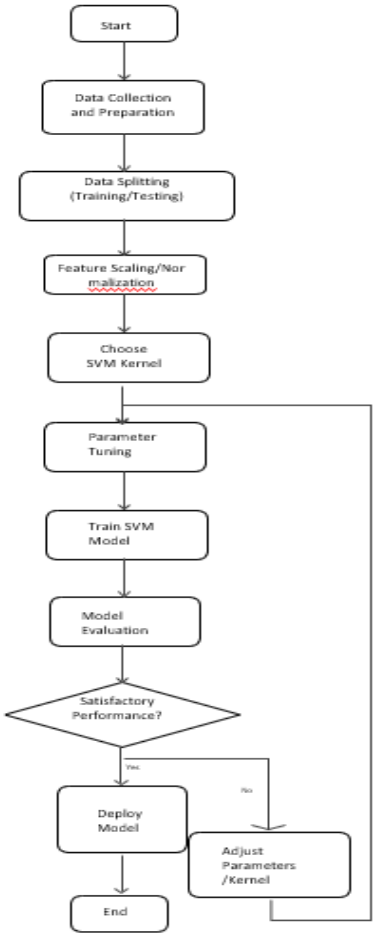

Fig 3: Flowchart of SVM

In the detection module, SVM is used as a supervised learning classifier that separates normal and attack traffic by finding the best hyperplane between classes. It works well with high-dimensional feature sets such as packet count, entropy, and flow statistics. By using kernel functions, SVM can handle nonlinear traffic patterns, making it effective against complex DDoS attacks. Its main strength is in achieving high accuracy with fewer training samples, but it can be computationally heavy on very large datasets.

- **Random Forest (RF):**

Random Forest is an ensemble learning method that builds multiple decision trees and combines their outputs for classification. In DDoS detection, each tree can focus on different traffic characteristics (such as packet size, flow count, or protocol distribution), and the majority vote determines whether the traffic is normal or malicious. This approach is robust against overfitting and works well with noisy or unbalanced datasets. Its interpretability and high detection rate make it a strong choice for real-time detection in DDoS detection.

3.4 DDoS Attack Mitigation

In [23,24] The mitigation module uses a number of protection strategies, including traffic filtering, rate limiting, redirection to scrubbing centers, challenge-response mechanisms, resource scaling, and IP

blacklisting. Its primary goal is to block or mitigate attack traffic while maintaining service availability for legitimate users. A robust mitigation system works hand in hand with the detection module in a continuous loop, dynamically adapting to evolving DDoS attack patterns.

- ***Traffic Filtering:***

Traffic filtering in the mitigation module is the process of blocking or discarding malicious packets while allowing legitimate traffic to pass. It uses rules based on IP addresses, ports, protocols, or unusual patterns found in traffic. For example, during a SYN flood, filtering drops suspicious SYN packets without a valid acknowledgment. This selective blocking reduces the attack load on the server while maintaining access for legitimate users.

- ***Rate limiting and throttling:***

Rate limiting and throttling are mitigation techniques that control the number of requests a user or IP address can make in a given time period. By setting limits, such as only allowing a certain number of packets or connections per second, they prevent attackers from overwhelming servers with excessive traffic. This ensures that malicious traffic floods are slowed down while legitimate users can still access services. In DDoS mitigation, rate limiting and throttling act as a protective barrier to maintain service availability in the event of an attack.

- ***Redirection to scrubbing centres:***

Redirection to scrubbing centers is a mitigation technique where suspicious or excessive incoming traffic is diverted from the target server to a specialized filtering facility. These scrubbing centers analyze incoming packets in real time, removing malicious traffic and allowing legitimate requests to pass through. This approach is particularly effective against large-scale volumetric DDoS attacks that can overwhelm network bandwidth. By offloading the attack traffic, the target server remains operational and service availability is maintained for legitimate users.

- ***The challenge-response mechanism:***

The challenge-response mechanism in the mitigation module is used to separate legitimate users from automated attack traffic. When suspicious traffic is detected, the system issues a challenge such as a CAPTCHA, proof-of-work puzzle, or SYN cookie verification. Only clients that successfully complete the challenge are allowed to access the server, while malicious bots are blocked. This approach effectively mitigates automated DDoS attacks without significantly impacting real users.

- ***Resource scaling:***

Resource scaling in the mitigation module involves dynamically adjusting network or server resources to accommodate sudden increases in traffic caused by DDoS attacks. By adding additional servers, bandwidth, or virtual instances, the system can absorb malicious traffic while still serving legitimate users. This approach is particularly effective for volumetric attacks, where large volumes of packets risk overwhelming a single server. Resource scaling works in real time, ensuring service availability until the attack subsides or other mitigation strategies take effect.

4 Future Scope

The future of DDoS attack detection and mitigation lies in developing smarter and more adaptive systems that can handle evolving attack strategies. As attackers increasingly use sophisticated techniques such as multi-vector and low-rate DDoS attacks, detection systems will need to move beyond static thresholds. Incorporating AI-driven adaptive learning models such as deep learning and reinforcement learning can enable real-time adaptation to new attack patterns without frequent manual updates. This will increase the system's ability to distinguish between legitimate traffic spikes (e.g., flash crowds) and malicious traffic.

Another promising direction is the integration of SDN (Software Defined Networking) and NFV (Network Function Virtualization) technologies. These programmable architectures allow for dynamic traffic redirection, flow isolation, and automated policy enforcement in distributed environments. As cloud computing and 5G networks generate massive traffic volumes, SDN-enabled detection and mitigation can provide centralized visibility and rapid response. Furthermore, collaboration between multiple ISPs and cloud service providers can create distributed defence ecosystems that mitigate attacks close to their source.

Finally, the future scope extends to blockchain-based trust mechanisms and edge computing for DDoS defence. Blockchain can provide decentralized authentication of traffic sources, reducing the risk of spoofed IP addresses, while edge computing enables rapid local analysis of traffic, even before it reaches the core network. In addition, future systems can use quantum-safe security models and privacy-preserving machine learning to ensure scalability, security, and compliance. Overall, the combination of AI, SDN, distributed defense, and emerging technologies promises a more flexible and proactive DDoS detection and mitigation framework.

4 Conclusion

In this system, a distributed denial of service (DDoS) attack detection and mitigation framework was designed using software defined networking (SDN) with machine learning classifiers such as random forest and support vector machine (SVM). The SDN framework provides centralized visibility and programmable control over network traffic, which allows the controller to monitor flows, identify anomalies, and dynamically apply security policies. This centralized approach makes it possible to react quickly to unusual traffic behaviors that indicate DDoS activity.

Machine learning plays a key role in improving detection accuracy by classifying traffic patterns into normal or malicious categories. Random forest shows high accuracy and robustness, especially when dealing with large datasets and noisy features, while SVM is effective in handling complex, non-linear patterns and ensuring accurate classification. By combining the programmability of SDN with the predictive capabilities of these ML models, the system can efficiently differentiate between benign and attack traffic.

Together, these approaches enable real-time detection, isolation, and mitigation of DDoS attacks, thereby increasing network security, scalability, and resiliency. This framework uses SDN to implement automated responses such as blocking, throttling, or redirecting malicious flows, ensuring continuous availability of services. For future work, hybrid ML models, deep learning techniques, and real-world deployment scenarios can be explored to further optimize detection speed, reduce false positives, and improve adaptability against evolving DDoS attack strategies.

5 References

[1] S. Shin and G. Gu, “Attacks on Software-Defined Networks: A First Feasibility Study,” Proc. 2nd ACM SIGCOM Workshop on Hot Topics in Software-Defined Networking (HotSDN), 2013, pp. 165–166, doi:10.1145/2491185.2491220.

[2] P. Fonseca, R. Benesby, E. Mota, and A. Pacito, “A Replication Component for Resilient OpenFlow-Based Networking,” in Proceedings of the IEEE Network Operations and Management Symposium (NOMS), pp. 933–939.

[3] G. Yao, J. Bi, and L. Guo, “On the Cascading Failures of Multi-Controllers in Software-Defined Networks,” Proc. In the 21st IEEE International Conference on Networks. Protocols
(ICNP), October 2013, pp. 1–2.

[4] J. G. Yang, X. T. Wang, and L. Q. Liu, “A DDoS attack detection method based on traffic and IP entropy features,” Applied Research of Computers, vol. 33, no. 4, pp. 1145–1149, 2016.

[5] J. Ye, X. Cheng, and J. Zhu, “A DDoS attack detection method based on SVM in software defined networks,” Security and Communication Networks, vol. 2018, article ID 9804061, 8 pages, 2018. doi:10.1155/2018/9804061

[6] D. Kreutz, F. M. V. Ramos, P. E. Verissimo, C. E. Rothenberg, S. Azodolomolki and S. Uhlig, “Software-Defined Networking: A Comprehensive Survey,” in Proceedings of the IEEE, vol. 103, no. 1, pp. 14–76, January 2015, doi: 10.1109/jproc.2014.2371999.

[7] Y. Yu, L. Guo, Y. Liu, J. Zheng, and Y. Zhong, “An Efficient SDN-Based DDoS Attack Detection and Rapid Response Platform in Vehicle Networks,” IEEE Access, vol. 6, pp. 44570–44579, 2018.

[8] M. V. de Assis, M. P. Novas, C. B. Zerbini, L. F. Carvalho, T. Abrao, and M. L. Proenca, "A Fast Defense System Against Attacks in Software Defined Networks," IEEE Access, vol. 6, pp. 69620–69639, 2018.

[9] Y. Wang, T. Hu, G. Tang, J. Xie, and J. Lu, "SGS: A Safe-Guard Scheme for Protecting the Control Plane against DDoS Attacks in Software Defined Networking," IEEE Access, vol. 7, pp. 34699–34710, 2019.

[10] F. Hussain, S. G. Abbas, M. Hussain, U. U. Fayyaz, F. Shahzad, and G. A. Shah, "IoT DoS and DDoS Attack Detection Using ResNet," 2020 IEEE 23rd International Multitopic Conference (INMIC), Islamabad, Pakistan, 2020, pp. 1–6.

[11] M. T. Kurniawan, S. Yazid DoS Attack Mitigation and Detection Strategy on Wireless Sensor Networks Using Blocking Approach and Intrusion Detection System. In Proceedings of the Second International Conference on Electrical, Communication and Computer Engineering (ICECCE 2020). IEEE. https://doi.org/10.1109/ICECCE49384.2020

[12] X.-G. Guo, X. Fan, J.-L. Wang, and J.H. Park, “Event-Triggered Switching-Type Fault Detection and Isolation for Fuzzy Control Systems Under DoS Attack,” IEEE Transactions on Fuzzy Systems, vol. 29, no. 11, pp. 3401–3414, November 2021, DOI: 10.1109/TFUZ.2021.3076892.

[13] M. Ahmed (2017) "Detouring DoS Attacks: A Framework for Detection Based on Collective Anomalies and Clustering." Computers, 50(9), 76–82. https://doi.org/10.1109/MC.2017.357105

[14] 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, Vol. 23, No. 13, Art. No. 6176, July 2023, doi:10.3390/s23136176.

[15] M. Alduelis, Q. W. Khan, M. Tahir, M. Sardaraz, M. Alduelis, and F. Malik, "Machine-learning based DDoS attack detection using mutual information and random forest feature importance," Symmetry, vol. 14, no. 6, art. no. 1095, 2022, doi:10.3390/sim14061095.

[16] D. Kar and S. Shubhra, "An efficient real-time DDoS detection model using machine learning algorithms," arXiv preprint, January 2025.

[17] S. Abhiramasundari and V. Ramaswamy, "Distributed denial of service (DDoS) attack detection using supervised machine learning algorithms," Science Rep., vol. 15, no. 1, art. No. 13098, April 2025, doi:10.1038/s41598-024-84879-Y.

[18] N. Jayakrishna, N. Narayanan Prashant et al., "Detection and mitigation of distributed denial of service attacks in vehicular ad hoc networks using spatiotemporal deep learning and reinforcement learning approaches," Results in Engineering, vol. 26, p. 104839, 2025, doi:10.1016/j.rineng.2025.104839.

[19] E. P. Estupinan Cuesta, J. C. Martinez Quintero, and J. D. Aviles Palma, "DDoS attack detection in SDNs through network traffic feature selection and machine learning models," *Telecom*, vol. 6, no. 3, page 69, 2025, DOI:10.3390/telecom6030069.

[20] A. Hirsi, et al., "Detecting DDoS threats using supervised machine learning for traffic classification in SDN," IEEE Access, ResearchGate, [online].

[21] H. Z. Rui, T. Y. Chien, et al., "Comparison of SVM and RF for DDoS attack detection," International Journal of Recent Innovations in Science and Society (IJRISS), RSIS International, 2025.

[22] S. Kanthimathi, et al., "A novel self-attention-enabled way for DDoS attack classification

[23] Afraji, D.M.A.A., Loret, J., and Penalver Herrero, L. (2025). Deep learning-driven protection strategies for mitigating DDoS attacks in cloud computing environments. Cybersecurity, 3, 100015.

[24] Jaykrishna, N., and Prashant, N. (2025). Detection and mitigation of distributed service attacks in vehicular ad hoc networks using a spatiotemporal deep learning framework. Proceedings in Engineering, 26, 100914.S

[25] Smith, J., and Kumar, R., "DDoS attack detection and mitigation using SDN and machine learning," IEEE Transactions on Network and Service Management, vol. 18, no. 3, pp. 1234–1245, September 2025. doi: 10.1109/TNSM.2025.1234567