Nanotechnology Perceptions
ISSN 1660-6795
www.nano-ntp.com

Enhancing Cybersecurity in Software-Defined Networking: A Hybrid Approach for Advanced DDoS Detection and Mitigation

Karam Hammadeh[1], M. Kavitha[2], Nadim Ibrahim[3]

[1]Department of Computer Science and Engineering,Vel Tech RangarajanDr.Sagunthala R&D Institute of Science and Technology, Chennai, India, karam.m.hammadeh@gmail.com
[2]Department of Computer Science and Engineering, Vel Tech RangarajanDr.Sagunthala R&D Institute of Science and Technology,Chennai, India, kavitha@veltech.edu.in
[3]Department of Computer Science and Engineering, Vel Tech RangarajanDr.Sagunthala R&D Institute of Science and Technology, Chennai, India, nadimibrahimcs@gmail.com

Software-Defined Networking (SDN) offers a paradigm shift in network management, providing increased flexibility and centralized control. However, this centralized architecture introduces unique security challenges. The centralized controller becomes a prime target for attackers, exposing the network to various threats such as direct attacks, unauthorized access, data manipulation, Denial-of-Service (DoS) attacks, and switch vulnerabilities. Furthermore, existing DDoS detection methods in SDN face limitations due to reliance on network topology, incomplete attack type coverage, outdated datasets, and expensive hardware requirements. This dependence on outdated data hinders adaptability to new threats and slows down detection. This research addresses these challenges by proposing a sophisticated hybrid approach integrated within the ONOS controller. This approach combines entropy-based analysis and a machine learning algorithm to enhance the identification of both high-volume and low-volume DDoS attacks through a binary classification task. By leveraging the capabilities of the ONOS controller, the study advances intrusion detection, offering a deeper understanding of network patterns and strengthening resilience against evolving cyber threats. Notably, the results demonstrate outstanding accuracy of up to 97% in detecting and mitigating these threats, underscoring the effectiveness of the proposed methodology. This research contributes significantly to the ongoing discourse on securing SDN environments by proposing a highly effective and adaptable DDoS detection and mitigation approach. This approach addresses the inherent vulnerabilities of SDN while capitalizing on its inherent advantages in flexibility and centralized control.

Keywords: SDN, DDoS attack, Entropy, ONOS controller, SAE-LSTM.

1. Introduction

The rapid evolution of the Internet has exposed shortcomings within traditional network infrastructures, often necessitating piecemeal fixes that lead to increased complexity and reduced control. In response, SDN has emerged as a transformative solution by untethering control functions from hardware, effectively mitigating these issues [1, 2]. SDN architecture

(Fig. 1) boosts cybersecurity by enabling centralized control for swift and flexible security policy implementation. It segments networks, responds rapidly to threats, enhances monitoring, automates security measures, and adapts access controls based on context. This proactive approach strengthens network defences and bolsters overall cybersecurity [3].

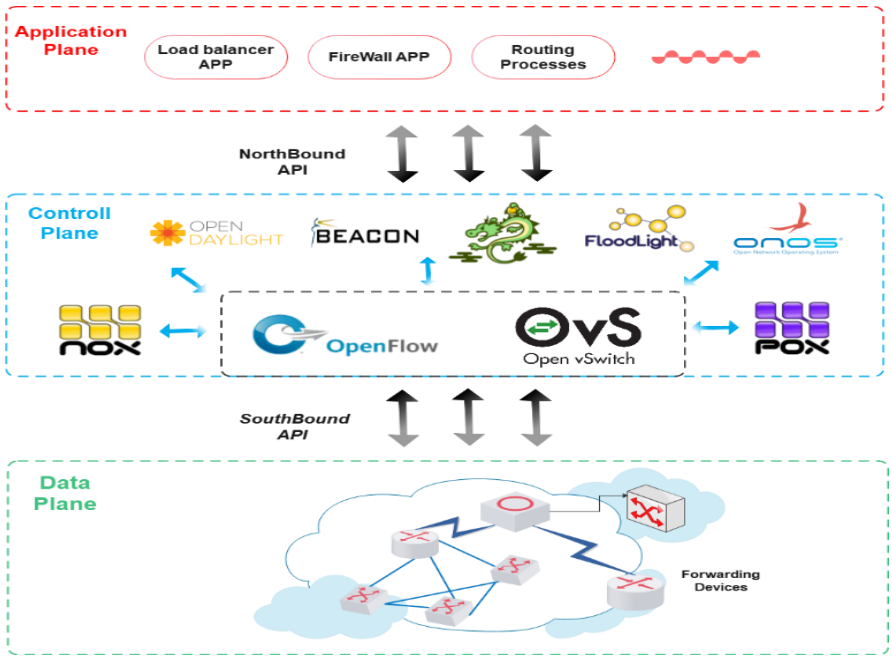

Fig.1.SDN Architecture

With a centralized control architecture, SDN enables controllers to comprehensively monitor switches within their domain and exert authority over the entire network using open interfaces like the South API. This paradigm shift empowers network administrators to overcome the limitations of conventional networks, fostering greater efficiency, flexibility, and control [4, 5].

Communication networks have confronted a spectrum of challenges over time, paramount among them the imperative to uphold confidentiality, integrity, and availability [6]. DoS and Distributed Denial-of-Service (DDoS) attacks have emerged as potent threats, escalating in frequency and sophistication, capable of disrupting organizations profoundly. DDoS attacks manifest in three primary forms: volumetric attacks overwhelm networks with traffic, protocol exploitation attacks capitalize on vulnerabilities in network protocols, and application layer attacks target specific applications [7]. To fortify against these threats, understanding these attack types and their mitigation techniques is essential for organizations, enabling the formulation of effective strategies that mitigate their impact and ensure network resilience [8, 9].

Balancing the need for prompt attack detection with resource efficiency in SDN poses a challenge. Longer detection periods risk delayed responses during attacks, while shorter intervals lead to constant resource usage. Finding equilibrium requires dynamically adapting

detection parameters to optimize both speed and resource utilization based on network conditions [10].

This research introduces an innovative approach to DDoS attack detection and mitigation within SDN networks. The method relies on two pivotal elements: anomaly detection via entropy analysis and the deployment of hybrid machine learning, specifically utilizing Stacked Autoencoder (SAE) and Long Short-Term Memory (LSTM). Additionally, the primary goal is to improve the identification of both high and low-volume DDoS attacks using classification. By leveraging the ONOS controller, the study seeks to enhance intrusion detection capabilities, gain a deeper insight into network patterns, and fortify defenses against evolving cyber threats.

The subsequent sections of this paper are structured as follows: Section 2 delves into the related literature, while Section 3 elucidates the methodologies employed. Section 4 outlines the results and ensuing discussion, with Section 5 encapsulating the conclusion and delineating avenues for future research.

2. Related Work

The landscape of DDoS solutions in SDN networks is characterized by a multitude of studies primarily cantered on detection, mitigation, and integrated security measures. These endeavours commonly utilize a spectrum of methodologies, encompassing entropy-based techniques, various machine learning algorithms, and hybrid approaches that combine entropy with machine learning models to combat DDoS attacks effectively. Figure 2 provides a visual representation elucidating these methodologies and their interplay in the context of SDN DDoS solutions.

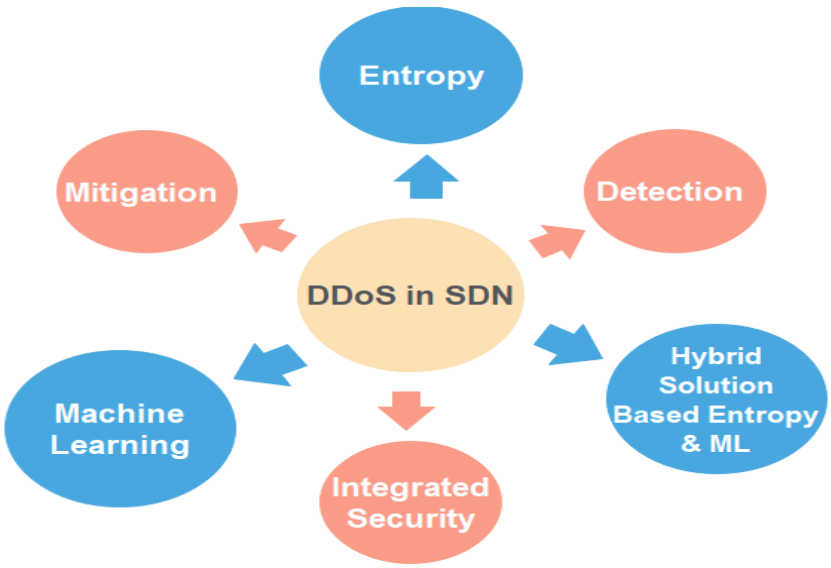

Fig. 2.DDoS solutions in SDN Networks

[11] Introduce an innovative approach to enhance DDoS detection and mitigation in SDN. They extend the packet number counter in the OpenFlow table's flow entry, leveraging SDN's

flow-centric design to collect flow statistics directly within the network switch. The authors then propose a streamlined DDoS flooding attack detection model based on entropy analysis, implemented at the edge switch of the OpenFlow network. This framework enables distributed anomaly detection within the SDN ecosystem, reducing the burden on the controller caused by excessive flow data collection. Wang's work represents a significant stride in improving the efficiency and scalability of DDoS detection and mitigation in SDN environments. [12] Present an innovative approach to combat DDoS attacks by leveraging entropy variations to distinguish attack traffic from normal network data. This method is designed for minimal computational overhead and includes a mitigation technique to reduce the disruptive impact of DDoS attacks. Compared to existing methodologies, Mishra's approach stands out for its high detection rate, low false positives, and effective mitigation capabilities. Comprehensive simulations validate its effectiveness, revealing an impressive 98.2% detection rate across various attack intensities, highlighting its robust performance in discerning and mitigating DDoS threats.

[13] Address the challenge of detecting low- rate DDoS attacks in SDNs, which can be difficult to identify since attackers mimic legitimate traffic patterns. To mitigate these attacks efficiently and protect network resources like bandwidth, memory, and CPU, they propose a DDoS detection technique called Renyi Entropy with Packet Drop (REPD). This technique utilizes packet dropping methods for mitigation. It evaluates network traffic fluctuations using an information distance metric based on Renyi Entropy and various probability distributions.

[14] Introduced a fusion entropy method for attack detection, measuring network event randomness for swift detection and notable entropy value reduction. Leveraging information entropy and log energy entropy complementarity, this approach efficiently identifies attacks. Experimental results display a 91.25% decrease in entropy values in attack scenarios compared to normal ones, showcasing significant advantages over other detection methods.

[15] Developed the SAFETY framework, based on entropy, for early detection, mitigation, and prevention of TCP-SYN flooding threats in SDN networks. Entropy, calculated from destination-IP and TCP-flags characteristics within a specified time frame, aids in detecting suspicious traffic below a predefined threshold. [16] proposed a method combining Renyi entropies and hidden Markov model (HMM-R) to identify low-rate DDoS attacks (L-DDoS) using IP addresses of data packets.

[17] Proposed an entropy-based DDoS detection and deep learning, combining Shannon and Renyi entropy for identifying distributed attack features in SDN traffic. Their research showcased the Stacked Auto Encoder (SAE) achieving 94% accuracy with 6% false positives, while the CNN averaged 93% accuracy in detecting DDoS attacks.[18] Introduced a system tailored for countering low-rate DDoS attacks on SDN. Notably, the framework segregates detection and prevention tasks from network applications, thus alleviating the controller's processing. [19] Present a hybrid model, CNN-ELM, enhancing DDoS attack detection in SDN by combining Convolutional Neural Network (CNN) for feature extraction with Extreme Learning Machine (ELM) for classification, thereby improving accuracy and efficiency.[20] Devised a cooperative DDoS detection using edge switch entropy monitoring and controller-based ensemble learning. This approach efficiently detects ICMP and SYN attacks, reducing communication overhead and detection delays by offloading tasks to edge switches. [21] Introduced a two-tier DDoS detection strategy within SDN, integrating

information entropy and deep learning. The initial level enhances the controller with traffic statistics, enabling quick attack source identification via information entropy detection without extra components. The subsequent level converts streaming data into grayscale images, leveraging spatial features to heighten accuracy and decrease false positives in fine-grained detection. [22] Proposed an efficient DDoS detection method involving two modules: an initial detection based on information entropy for rapid identification of anomalous traffic and a subsequent machine learning module using Stacked Sparse Autoencoder (SSAE) and SVM architecture to confirm suspicions. The approach, proven effective in experiments with real-time and benchmark datasets, surpasses existing methods by achieving over 98% accuracy in detecting DDoS traffic while significantly reducing training time and computational load. [23] Proposed a machine learning-driven DDoS attack detection method within an SDN-WISE IoT controller. They integrated a detection module, capturing attack traffic and processing it into datasets. Using NB, SVM, and DT algorithms, the module achieved 97.4%, 96.1%, and 98.1% accuracy rates, respectively. The framework utilized up to 30% memory and CPU, reducing memory usage by 70% and keeping CPU free up to 70%. With an average throughput of 48 packets per second, it reached 97.2% accuracy, demonstrating superior DDoS attack detection in an SDN-WISE IoT environment, potentially enhancing IoT network security.

3. Methods

The methodology outlined in Fig. 3 involves a systematic process: firstly, the creation of both normal and abnormal traffic using the tool 'hping3.' Over defined time intervals, traffic data is gathered and subjected to entropy calculations based on source and destination IP addresses. Subsequently, a SAE-LSTM model is employed to classify this traffic. Upon identification of potentially harmful traffic patterns, the system generates a role and updates the flow table within the network to implement measures aimed at mitigating DDoS attacks. This approach signifies a proactive method, leveraging both traffic analysis and machine learning for detection, classification, and swift response to potential threats within the network.

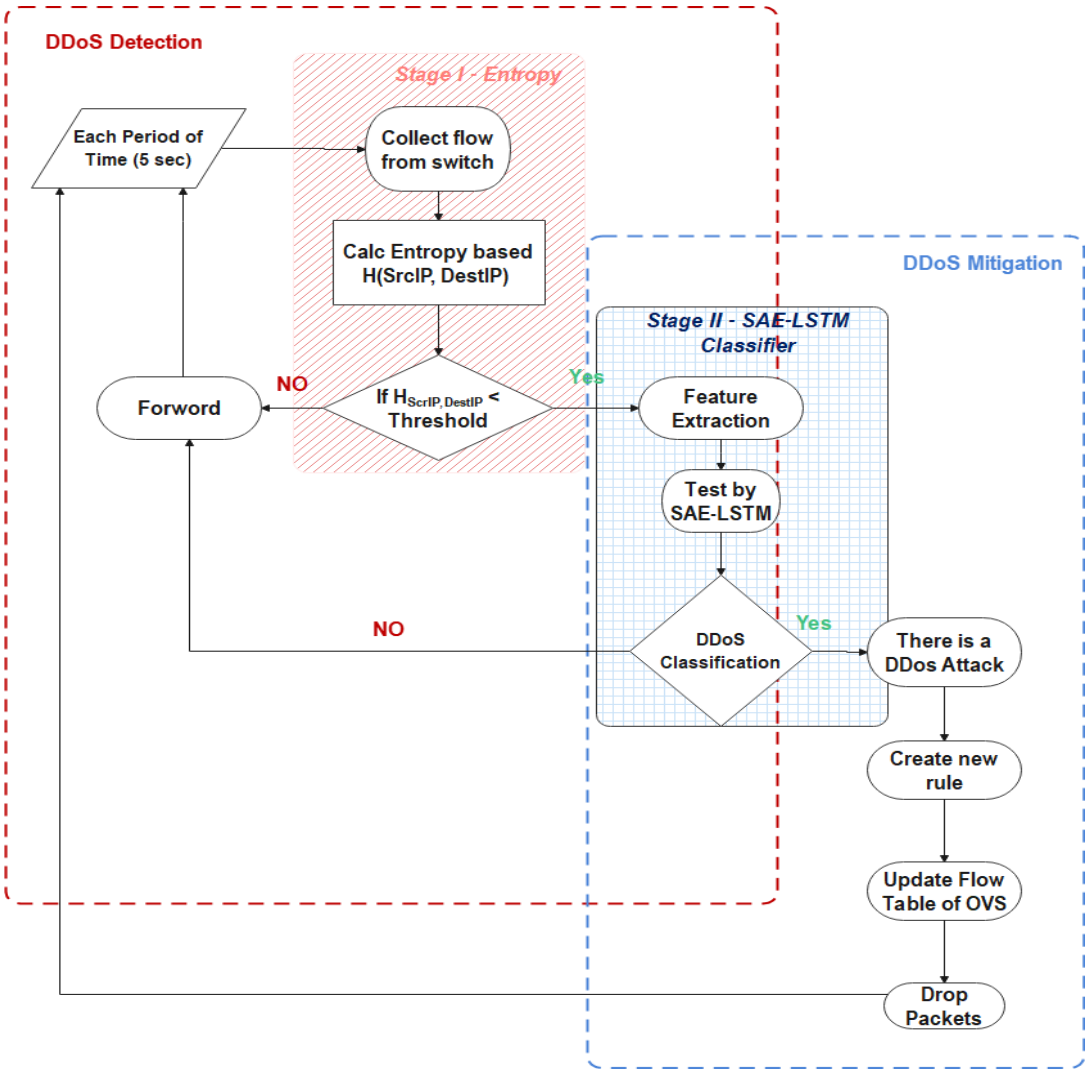

Fig. 3.Detect and Mitigate DDoS Methodology

Pseudocode: Methodology for detect and mitigate DDoS Attack
Design topology of SDN Network Using HPing3 to generate normal & attack traffic Calc entropy $H_{SrcIP,DestIP}$ IF $H_{SrcIP,DestIP}$<Thr Apply machine learning (SAE-LSTM) IF classify as DDoS attack Create new rules Update flow table for drop the sequence Else forward traffic Else forward traffic

3.1 Entropy

The utilization of entropy as a means to detect various attacks offers a significant advantage in swiftly filtering suspicious flows. Its application proves advantageous due to its efficiency, enabling quick identification of potentially malicious traffic patterns. This method is particularly suitable for SDN environments, where it can be easily developed and implemented by the controller, exhibiting low CPU load and straightforward integration. DDoS attacks, known for their capacity to impose additional overhead and disrupt web activities, prompt the measurement of the target system by computing the entropy of individual IPs within SDN networks [24,25]. The entropy calculation operates within a defined time window, denoted as W, encompassing n distinct elements, with representing the observation i within the set at time t. The size of W, as described in Equation (1), is referred to as the size of the time window, a crucial parameter in this entropy-based analysis. Equation (2) is utilized to compute the probability of occurrence for X(i, t) within the defined time window(W). Equation (3) follows Shannon's entropy formula. This equation computes the entropy, H(i, t), by multiplying the probability of each element within the dataset by its logarithm and summing these products. This entropy formula proves invaluable in assessing the complexity and irregularity of traffic patterns, pivotal for identifying potential anomalies in network behavior.

$$W = \{X(1,t), X(2,t), \dots, X(n,t)\} \quad (1)$$

$$P\big(X(i,t)\big) = X(i,t)/n \quad (2)$$

$$H(X(i,t)) = -\sum_{i=1}^{n} P\big(X(i,t)\big).\, logP(X(i,t)) \quad (3)$$

Setting entropy thresholds enables analysts and network administrators to categorize traffic patterns as either normal or anomalous. This approach facilitates the identification of substantial deviations from expected behavior, facilitating the detection of abnormal network activity and potential security threats such as DDoS attacks. The static threshold, as Equation (4), is determined based on the comparison between Hnormal which signifies the average entropy observed within normal flows, and Hack denoting the average entropy detected within the flow of an attack. Providing a fixed reference point for identifying deviations in entropy associated with abnormal network activity. An attack is flagged if the calculated entropy falls below the threshold as Equation (5)

$$Threshold = avg(Hattack) + avg(Hnormal)/2 \quad (4)$$

$$Threshold > H(X_{(i,t)}) \quad (5)$$

Pseudo code for Entropy based on SrcIP, DestIP
Calc the threshold (Thr) Each period of time Calc the entropy HSrcIP,DestIP IF HSrcIP,DestIP<Thr There a higher probability for DDoS attacks and continue with machine learning stage Else forward the packets

3.2 Machine learning model

The utilization of a SAE [26] coupled with a LSTM [27,28] model presents a robust approach for detecting DDoS attacks within SDN environments. The SAE initially extracts and compresses intricate features from network flow data, focusing on the most salient aspects. These encoded features are then fed into the LSTM architecture, allowing for the learning of sequential patterns and temporal dependencies inherent in network traffic. By combining the SAE's ability to capture essential features with the LSTM's proficiency in analyzing temporal behaviors, this hybrid model can discern deviations from normal network traffic, identifying potential DDoS attack patterns. Integrated into SDN, this model enables real-time monitoring and swift responses to fortify network security against threats [29].

In ONOS and OpenFlow, learning models enable dynamic network management by analyzing data to make informed decisions, while OpenFlow's flow table updates, guided by these models, facilitate adaptive responses for optimized performance and enhanced security in SDN environments. After classifying flows as DDoS attacks using proposed model, the approach involves generating specific rules for OpenFlow within ONOS to update the flow table, as Fig. 4. These rules dictate actions to prevent and discard packets originating from identified attackers [30].

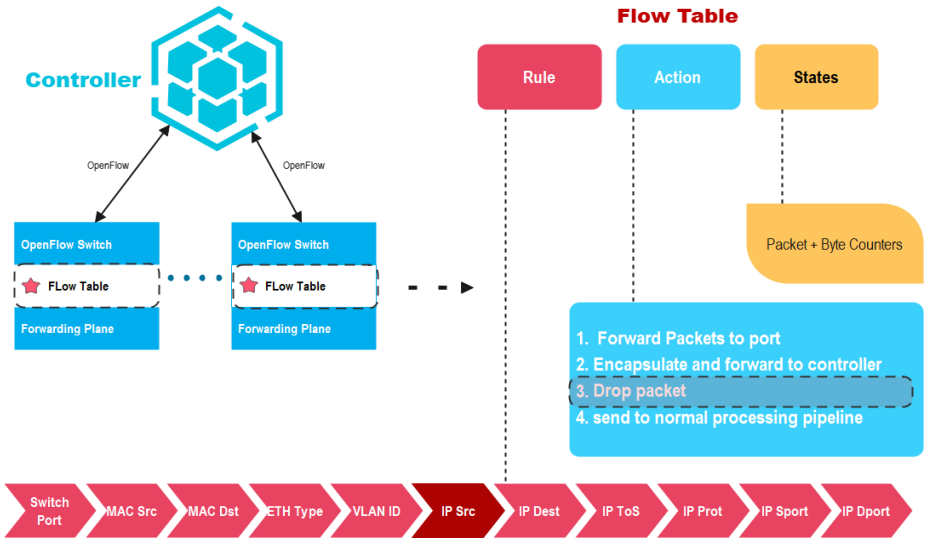

Fig. 4.Flow Table Management by the Controller

4. Results and Discussion

Environment setups: Simulation on a Dell PC with an Intel Core i7-9700H, 16GB RAM, running Ubuntu 20.04 in a virtual environment, utilized ONOS as the controller for its scalability and real-time capabilities. By orchestrating a DDoS attack on a virtual server, the study methodically evaluated the DDoS detection model's performance. Fig. 5 illustrates the topology of an SDN network employing an ONOS controller along with 16 hosts. This visual representation outlines the structure and connections within the network, showcasing the relationships between the ONOS controller and the various hosts integrated into the network infrastructure.

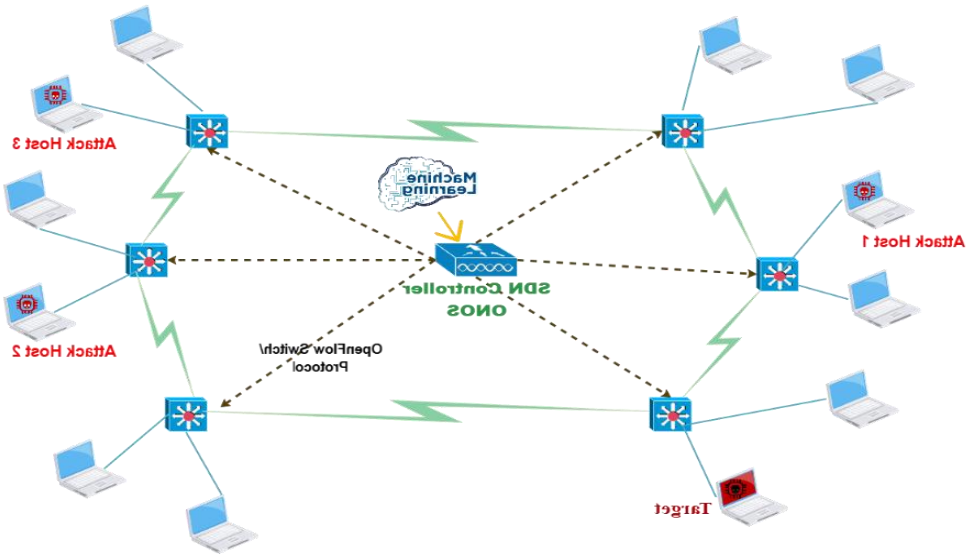

Fig. 5.Network Topology

Two instances of hping3 are employed to generate network traffic: one for normal traffic and the other simulating an DDoS attack by sending packets at an accelerated rate. Fig. 6 illustrates the distinction between the normal and attack traffic patterns. Fig. 7 displays the contrast in entropies between normal traffic and the attacking hosts.

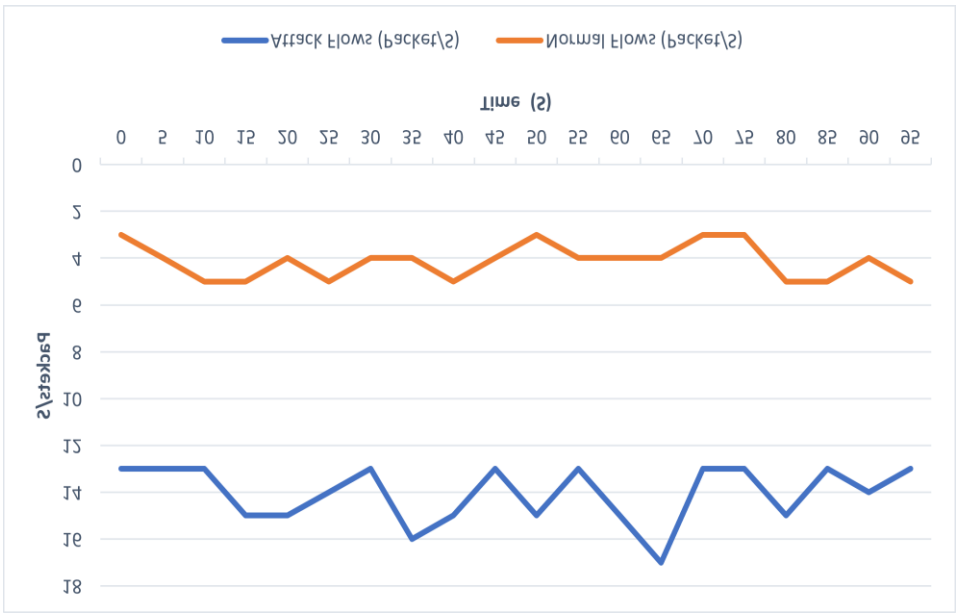

Fig. 6. Network Traffic for Normal and Attack Flow

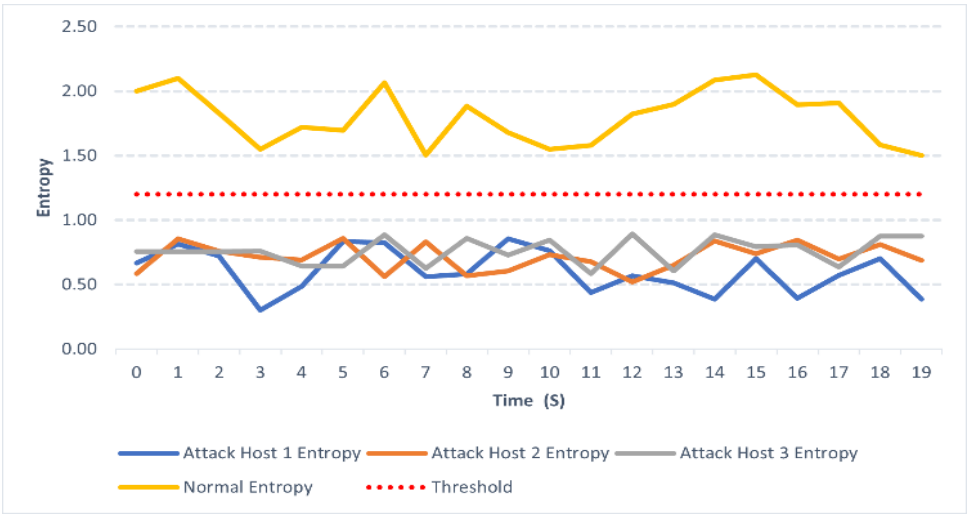

Fig. 7.Entropy for Normal and Attacker Host

An effective DDoS classifier requires a diverse set of traffic features, encompassing various distributions, including addresses, ports, data lengths, etc. These traffic anomalies exhibit random changes within the distribution of the most probable characteristics in the observed traffic area. The overview of selected traffic features, detailed in Table 1, is obtained by distributing specific features from test-bed datasets using Shannon entropy. This approach ensures a comprehensive representation of the dynamic and evolving nature of DDoS attack patterns in real-world traffic scenarios.

Table 1. Important Various Network Features

Selected Traffic Features	
Source IP	Timestamp
Source Port	Flow Duration
Destination IP	Flow Bytes/s
Destination Port	Flow Packets/s
Protocol	Time To Live duration

Balancing timely attack detection with minimal resource impact in SDN architecture is challenging. Choosing the right time-period for detection involves a trade-off longer periods may increase response time during attacks, while shorter ones continuously consume resources. Adaptive solutions, such as thresholds, machine learning for pattern recognition, event correlation, resource-aware monitoring, and selective packet sampling, can optimize detection efficiency. These approaches aim to intelligently allocate resources during suspected attack periods, enhancing the accuracy of detection without overwhelming the system during normal network traffic.

The proposed framework for detecting and mitigating DDoS attacks, leveraging the SAE-LSTM model, showcased outstanding performance with a high accuracy rate of 97%. The evaluation was conducted across different time windows, including 5, 10, 15, 20, and 30 seconds, demonstrating the model's adaptability to varying attack durations. The results, presented in Fig. 7 and summarized in Table 2, provide a detailed account of the experimental outcomes over these time intervals.

Table 2. Experimental Results Based on Data Generation

Period of Time	**Accuracy**	**Precision**	**Recall**	**F1 Score**
5	96.2	98.6	95.1	97.2
10	96.8	99.2	94.2	96.8
15	97.3	99.8	93.9	97.0
20	97.0	99.5	94.5	96.6
30	97.1	99.6	94.2	97.7

The approach has been thoroughly tested and validated using the CIC-DDoS2019 dataset. This dataset serves as the cornerstone for evaluating the effectiveness of the approach, offering a diverse range of network traffic data meticulously designed for studying distributed denial-of-service (DDoS) attacks. Through the utilization of this dataset, the methodology has undergone rigorous testing across different scenarios, effectively emulating real-world cyber

threats. This comprehensive evaluation process enables a detailed assessment of the approach's performance, resilience, and dependability in mitigating DDoS attacks.

Table 3. Results Based on CIC-DDoS2019 Dataset

Period of Time	Accuracy	Precision	Recall	F1 Score
5	93.9	97.9	94.6	97.3
10	94.3	98.4	95.2	97.6
15	94.8	98.7	95.1	96.9
20	95.1	98.8	94.7	96.5
30	94.7	98.6	95.3	97.1

The model exhibits high accuracy across both datasets, indicating its overall correctness in predictions. Nonetheless, a slight decline in accuracy when using the CIC-DDoS2019 dataset compared to the generated dataset implies disparities in data characteristics and complexities. Despite this, the model maintains consistent high accuracy, particularly in shorter time windows, showcasing its efficacy in real-time threat detection. The detailed experimental results offer insights into its performance across various time intervals, enhancing understanding of its robustness and reliability in DDoS threat mitigation.

The effectiveness and efficiency of the model depend on numerous critical factors and challenges associated with accuracy, processing duration (detection time), and resource usage (CPU and memory consumption). These factors collectively play a pivotal role in determining the model's ability to accurately detect and mitigate DDoS attacks while ensuring optimal utilization of computational resources. In this study, the focus is on balancing accuracy, processing duration, and resource usage in the model's operation. By incorporating entropy, the time taken for processing tasks is reduced, leading to more efficient operations. Additionally, breaking down the classification process into smaller time intervals improves the speed of detection while ensuring optimal utilization of memory and CPU resources. Table 4 presents a comparative analysis between the proposed model and previous research studies.

Table 4. Comparison of Various DDoS Detection Approaches with the Proposed Model

Ref.	Controller	Technology used	DataSet	Accuracy	Performance	Processing Time	Resource Utilization
[15]	Floodlight	Entropy destination IP, TCP flags	Generated dataset	100% TPR, works better in high traffic scenario	-	✓	✓
[16]	POX	Renyi entropy	-	98.4%	✓	✓	-

		with the hidden Markov model					
[18]	ONOS	SVM, MLP	CIC DoS	95%	✓	✓	-
[19]	RYU	CNN-ELM	CICIDS-2017	98.9%	✓	✓	×
[22]	Floodlight	Entropy and SSAE-SVM	real-time and benchmark datasets	98%	✓	✓	×
[23]	SDN-WISE	NB, DT, SVM	IoT-generated datasets	97.2%	✓	-	✓
Proposed Model	ONOS	Entropy and SAE-LSTM	Generated dataset and CICIDS-2019	97.3%	✓	✓	✓

The table 4 summarizes various DDoS detection approaches utilizing different controllers and technologies, with notable variations in accuracy, performance, and resource utilization. While some models achieve perfect accuracy or high detection rates, they may exhibit higher resource consumption. The proposed model, leveraging ONOS controller with entropy and SAE-LSTM, achieves a commendable accuracy of 97.3% across diverse datasets, maintaining a balance between performance and resource utilization.

5. Conclusion and Future Works

In conclusion, this research propels the frontier of cybersecurity within Software-Defined Networking (SDN) by introducing a pioneering hybrid approach. The seamless integration of entropy-based analysis and a machine learning algorithm within the ONOS (Open Network Operating System) controller not only enhances the identification and mitigation of Distributed Denial-of-Service (DDoS) attacks but also attains an impressive accuracy of up to 97%. These findings underscore the efficacy of the proposed methodology, affirming its potential to fortify SDN environments against the multifaceted landscape of evolving cyber threats. As the digital realm continues to evolve, this research contributes valuable insights and methodologies crucial for the ongoing enhancement of network security paradigms in SDN.

Future work in this field could involve refining the suggested hybrid approach by exploring a broader range of machine learning models and optimizing parameters to elevate detection accuracy. It's crucial to assess the adaptability of this methodology to emerging cyber threats and evolving network structures. Additionally, investigating mechanisms to dynamically adapt to shifting network conditions and scaling the approach for more extensive and intricate

SDN environments is a promising direction for research. This might include incorporating multi-point controllers, implementing dynamic entropy solutions, and integrating wide datasets to further enhance the system's capabilities.

References

1. V. -G. Nguyen, A. Brunstrom, K. -J. Grinnemo and J. Taheri, "SDN/NFV-Based Mobile Packet Core Network Architectures: A Survey," in IEEE Communications Surveys & Tutorials, vol. 19, no. 3, pp. 1567-1602, thirdquarter 2017, doi: 10.1109/COMST.2017.2690823.
2. Z. Yang and K. L. Yeung, "SDN Candidate Selection in Hybrid IP/SDN Networks for Single Link Failure Protection," in IEEE/ACM Transactions on Networking, vol. 28, no. 1, pp. 312-321, Feb. 2020, doi: 10.1109/TNET.2019.2959588.
3. Y. Maleh, Y. Qasmaoui, K. El Gholami, Y. Sadqi, and S. Mounir, "A comprehensive survey on SDN security: threats, mitigations, and future directions," Journal of Reliable Intelligent Environments, vol. 9, Feb. 2022, doi: https://doi.org/10.1007/s40860-022-00171-8.
4. R. Mohammadi, R. Javidan and M. Conti, "SLICOTS: An SDN-Based Lightweight Countermeasure for TCP SYN Flooding Attacks," in IEEE Transactions on Network and Service Management, vol. 14, no. 2, pp. 487-497, June 2017, doi: 10.1109/TNSM.2017.2701549.
5. P. Vizarreta, K. Trivedi, V. Mendiratta, W. Kellerer and C. Mas-Machuca, "DASON: Dependability Assessment Framework for Imperfect Distributed SDN Implementations," in IEEE Transactions on Network and Service Management, vol. 17, no. 2, pp. 652-667, June 2020, doi: 10.1109/TNSM.2020.2973925.
6. R. von Solms and J. van Niekerk, "From Information Security to Cyber Security," Computers & Security, vol. 38, no. 38, pp. 97–102, Oct. 2013, doi: https://doi.org/10.1016/j.cose.2013.04.004.
7. P. Kumari and A. K. Jain, "A Comprehensive Study of DDoS Attacks over IoT Network and Their Countermeasures," Computers & Security, p. 103096, Jan. 2023, doi: https://doi.org/10.1016/j.cose.2023.103096.
8. J. F. Balarezo, S. Wang, K. G. Chavez, A. Al-Hourani, and S. Kandeepan, "A survey on DoS/DDoS attacks mathematical modelling for traditional, SDN and virtual networks," Engineering Science and Technology, an International Journal, Oct. 2021, doi: https://doi.org/10.1016/j.jestch.2021.09.011.
9. M. A. Bouke, A. Abdullah, S. H. ALshatebi, M. T. Abdullah, and H. E. Atigh, "An intelligent DDoS attack detection tree-based model using Gini index feature selection method," Microprocessors and Microsystems, vol. 98, p. 104823, Apr. 2023, doi: https://doi.org/10.1016/j.micpro.2023.104823.
10. S. Ejaz, Z. Iqbal, P. Azmat Shah, B. H. Bukhari, A. Ali and F. Aadil, "Traffic Load Balancing Using Software Defined Networking (SDN) Controller as Virtualized Network Function," in *IEEE Access*, vol. 7, pp. 46646-46658, 2019, doi: 10.1109/ACCESS.2019.2909356.
11. R. Wang, Z. Jia and L. Ju, "An Entropy-Based Distributed DDoS Detection Mechanism in Software-Defined Networking," *2015 IEEE Trustcom/BigDataSE/ISPA*, Helsinki, Finland, 2015, pp. 310-317, doi: 10.1109/Trustcom.2015.389.
12. Mishra, N. Gupta, and B. B. Gupta, "Defense mechanisms against DDoS attack based on entropy in SDN-cloud using POX controller," Telecommunication Systems, Jan. 2021, doi: https://doi.org/10.1007/s11235-020-00747-w.
13. Ahalawat, K. S. Babu, A. K. Turuk, and S. Patel, "A low-rate DDoS detection and mitigation for SDN using Renyi Entropy with Packet Drop," Journal of Information Security and Applications, vol. 68, p. 103212, Aug. 2022, doi: https://doi.org/10.1016/j.jisa.2022.103212.

14. Fan, N. M. Kaliyamurthy, S. Chen, H. Jiang, Y. Zhou, and C. Campbell, “Detection of DDoS Attacks in Software Defined Networking Using Entropy,” Applied Sciences, vol. 12, no. 1, p. 370, Dec. 2021, doi: https://doi.org/10.3390/app12010370.
15. P. Kumar, M. Tripathi, A. Nehra, M. Conti and C. Lal, "SAFETY: Early Detection and Mitigation of TCP SYN Flood Utilizing Entropy in SDN," in *IEEE Transactions on Network and Service Management*, vol. 15, no. 4, pp. 1545-1559, Dec. 2018, doi: 10.1109/TNSM.2018.2861741.
16. W. Wang, X. Ke, and L. Wang, “A HMM-R Approach to Detect L-DDoS Attack Adaptively on SDN Controller,” Future Internet, vol. 10, no. 9, p. 83, Aug. 2018, doi: https://doi.org/10.3390/fi10090083.
17. R. M. A. Ujjan, Z. Pervez, K. Dahal, W. A. Khan, A. M. Khattak, and B. Hayat, “Entropy Based Features Distribution for Anti-DDoS Model in SDN,” Sustainability, vol. 13, no. 3, p. 1522, Feb. 2021, doi: https://doi.org/10.3390/su13031522.
18. J. A. Pérez-Díaz, I. A. Valdovinos, K. -K. R. Choo and D. Zhu, "A Flexible SDN-Based Architecture for Identifying and Mitigating Low-Rate DDoS Attacks Using Machine Learning," in *IEEE Access*, vol. 8, pp. 155859-155872, 2020, doi: 10.1109/ACCESS.2020.3019330.
19. J. Wang and L. Wang, “SDN-Defend: A Lightweight Online Attack Detection and Mitigation System for DDoS Attacks in SDN,” Sensors, vol. 22, no. 21, p. 8287, Oct. 2022, doi: https://doi.org/10.3390/s22218287.
20. S. Yu, J. Zhang, J. Liu, X. Zhang, Y. Li, and T. Xu, “A cooperative DDoS attack detection scheme based on entropy and ensemble learning in SDN,” EURASIP Journal on Wireless Communications and Networking, vol. 2021, no. 1, Apr. 2021, doi: https://doi.org/10.1186/s13638-021-01957-9.
21. Y. Liu, T. Zhi, M. Shen, L. Wang, Y. Li, and M. Wan, “Software-defined DDoS detection with information entropy analysis and optimized deep learning,” Future Generation Computer Systems, Nov. 2021, doi: https://doi.org/10.1016/j.future.2021.11.009.
22. Z. Long and W. Jinsong, “A hybrid method of entropy and SSAE-SVM based DDoS detection and mitigation mechanism in SDN,” Computers & Security, vol. 115, p. 102604, Apr. 2022, doi: https://doi.org/10.1016/j.cose.2022.102604.
23. J. Bhayo, S. A. Shah, S. Hameed, A. Ahmed, J. Nasir, and D. Draheim, “Towards a machine learning-based framework for DDOS attack detection in software-defined IoT (SD-IoT) networks,” vol. 123, pp. 106432–106432, Aug. 2023, doi: https://doi.org/10.1016/j.engappai.2023.106432.
24. Krishnan, Gokul, et al. "Artificial intelligence in clinical medicine: catalyzing a sustainable global healthcare paradigm." Frontiers in Artificial Intelligence 6 (2023)
25. S. Syed, V. Sangeetha, and C. Prabhadevi, “Entropy based Anomaly Detection System to Prevent DDoS Attacks in Cloud,” arXiv (Cornell University), Jan. 2013, doi: https://doi.org/10.48550/arxiv.1308.6745.
26. Z. Liu, Y. He, W. Wang and B. Zhang, "DDoS attack detection scheme based on entropy and PSO-BP neural network in SDN," in *China Communications*, vol. 16, no. 7, pp. 144-155, July 2019, doi: 10.23919/JCC.2019.07.012.
27. H. Polat, M. Turkoglu, and O. Polat, “Deep network approach with stacked sparse autoencoders in detection of DDoS attacks on SDN-based VANET,” IET Communications, vol. 14, no. 22, pp. 4089–4100, Dec. 2020, doi: https://doi.org/10.1049/iet-com.2020.0477.
28. J. D. Gadze, A. A. Bamfo-Asante, J. O. Agyemang, H. Nunoo-Mensah, and K. A.-B. Opare, “An Investigation into the Application of Deep Learning in the Detection and Mitigation of DDOS Attack on SDN Controllers,” Technologies, vol. 9, no. 1, p. 14, Feb. 2021, doi: https://doi.org/10.3390/technologies9010014.
29. K. Hammadeh and M. Kavitha, “Unraveling Ransomware: Detecting Threats with Advanced Machine Learning Algorithms,” International journal of advanced computer science and

applications/International journal of advanced computer science & applications, vol. 14, no. 9, Jan. 2023, doi: https://doi.org/10.14569/ijacsa.2023.0140952.

30. Meaad Alrehaili, Adel Alshamrani, and Ala Eshmawi, “A Hybrid Deep Learning Approach for Advanced Persistent Threat Attack Detection,” The 5th International Conference on Future Networks & Distributed Systems, Dec. 2021, doi: https://doi.org/10.1145/3508072.3508085.
31. M. Revathi, V. V. Ramalingam, and B. Amutha, “A Machine Learning Based Detection and Mitigation of the DDOS Attack by Using SDN Controller Framework,” Wireless Personal Communications, Sep. 2021, doi: https://doi.org/10.1007/s11277-021-09071-1.