https://doi.org/10.33472/AFJBS.6.6.2024.7590-7601

African Journal of Biological Sciences

Journal homepage: http://www.afjbs.com

Research Paper Open Access

A Novel Approach for Detection and Mitigation of Distributed Denial of Service Attacks in Sdn_Iot Environment

I.Varalakshmi[1*], Dr.M.Thenmozhi[2],

[*1]Research Scholar, Department of CSE, Pondicherry University, Puducherry
[2]Associate Professor, Department of CSE, Puducherry Technological University, Puducherry
Email: [2]thenmozhi@ptuniv.edu.in
Corresponding Email: [*1]varalakshmi.mka@gmail.com,

Article Info

Volume 6, Issue 6, July 2024

Received: 03 June 2024

Accepted: 31 June 2024

Published: 25 July 2024

doi: 10.33472/AFJBS.6.6.2024.7590-7601

ABSTRACT:

This research proposes a comprehensive approach for the early detection and mitigation of Distributed Denial of Service (DDoS) attacks in Software-Defined Networking (SDN) environments integrated with Internet of Things (IoT) devices. The objectives encompass the development of an entropy-based detection mechanism, enhancement of detection rates for various DDoS attack types, creation of a mitigation algorithm using stochastic techniques, implementation of adaptive control for dynamic network response, and integration of energy optimization to enhance overall network security and performance. Our proposed model introduces an Entropy-based DDoS Detection Algorithm (EDDA) leveraging entropy metrics to analyze traffic patterns and identify anomalies indicative of DDoS attacks, with strategies tailored for detecting UDP, TCP, and ICMP SYN flood DDoS attacks. To augment traditional methods, we incorporate a novel approach as Integrated DDoS Detection, Mitigation, and Energy Optimization Algorithm (IDMEOA). This method enhances the resilience of the detection system against evolving attack strategies, maintaining high accuracy while minimizing false positives. Through the integration of dynamic thresholding, our model aims to provide a robust defense mechanism against DDoS attacks in SDN_IoT environments, offering a comprehensive framework for enhancing network security and resilience without relying on machine learning or deep learning techniques.

Keywords: Distributed Denial of Service attacks, Software-Defined Networking, Internet of Things, Entropy-based detection, Stochastic mitigation, Adaptive control, Energy optimization

1. Introduction

The incorporation of SDN with the IoT has ushered in a new era of connectivity and innovation. This convergence promises unparalleled flexibility and efficiency in managing network resources, enabling seamless communication and orchestration of complex operations. However, this integration also amplifies the vulnerability of IoT devices to DDoS attacks, posing significant challenges to network availability and performance.

The escalating threat posed by DDoS attacks in SDN_IoT environments underscores the urgency of developing resilient defense mechanisms. These attacks not only disrupt critical network services but also jeopardize the economic viability and reputation of organizations and service providers. Addressing this challenge requires innovative approaches that can effectively detect and mitigate DDoS attacks, while ensuring minimal disruption to network operations.

Against this backdrop, this research endeavors to develop a IDMEOA for the early detection and mitigation of DDoS attacks in SDN_IoT environments. By leveraging entropy-based detection mechanisms, stochastic mitigation algorithms, adaptive control mechanisms, and energy optimization techniques, the proposed model aims to enhance network security, resilience, and performance. Through these efforts, this research seeks to contribute to the development of robust defense mechanisms capable of safeguarding SDN_IoT environments against the evolving threat landscape.

2. Related Works

Liatifis et al. [1] proposed a method for mitigating Syn Flood attacks and other DDoS attacks in SDN environments using an entropy-based algorithm. Their approach achieved an accuracy of 85% in detecting attacks, albeit within a small window of limited traffic. However, scalability remains a concern, as the method's efficacy may diminish under high traffic loads. Ali et al. [2] addressed DDoS attacks in SDN by employing an Intrusion Detection System (IDS) enhanced with machine learning techniques. Their system demonstrated high accuracy in identifying TCP and UDP attacks by considering network traffic patterns. Although effective, the reliance on machine learning may pose challenges in deployment and maintenance, particularly regarding model updates and scalability.

Misra et al. [3] proposed a tailored analytics algorithm for detecting DDoS attacks in SDN environments. Their approach exhibited promising results in detecting limited attack packets while reducing CPU utilization. However, the algorithm's performance under sustained or multi-vector attacks warrants further investigation. Rahman et al. [4] explored the use of Blockchain techniques in SDN_IoT environments for mitigating DDoS attacks, leveraging Network Function Virtualization (NFV) and mitigation protocols. While their approach showed potential in providing good throughput, concerns arose regarding network controller overhead and an increase in false positives, particularly with high traffic volumes.

Cherian et al. [5] developed a counter-based approach for detecting SYN Flood attacks in SDN IoT environments. Their method relied on real-time packet analysis and demonstrated effective detection based on packet counts entering the network. However, scalability and adaptability to varying attack scenarios may pose challenges in practical deployment. Aladaileh et al. [6] addressed volumetric DDoS attacks in SDN environments using NFV and process-based virtualization. While their approach showed promise in achieving good throughput, concerns were raised regarding its high energy consumption. Balancing performance with energy efficiency remains a crucial consideration for sustainable network operation.

Changati et al. [7] revisited Syn Flood attacks and other DDoS attack vectors in SDN environments, focusing on scalability and the limitations of their entropy-based algorithm.

While effective in detecting attacks, scalability and the algorithm's reliance on limited traffic present challenges in real-world deployment scenarios. Addressing these limitations is essential for ensuring the robustness and scalability of DDoS defense mechanisms in SDN environments. Aldaej et al. [8] proposed a multi-faceted approach for detecting and mitigating IP, TCP, and HTTP-based attacks, incorporating techniques such as monitoring resource utilization, anomaly detection, and traffic filtering. While effective initially, the detection accuracy of the system degrades over time, particularly when faced with new threats and attack patterns. Addressing this limitation is crucial for maintaining the system's efficacy in dynamically evolving threat landscapes.

Bhushan et al. [9] addressed a range of attacks including SSH brute-force, ICMP, DNS flooding, reflection, and TCP SYN attacks, employing both supervised and unsupervised detection techniques. However, performance degradation occurs due to the detection of threats at the destination device, highlighting the need for distributed detection mechanisms to alleviate the burden on individual network nodes. Lima Filho et al. [10] focused on securing communications by analyzing IP, TCP, UDP, and ICMP traffic using clustering, machine learning, and online detection approaches. While their method achieved high accuracy in detecting normal network behavior, it fell short in identifying abnormal attacks. Enhancing the system's ability to detect and respond to anomalous activities is imperative for comprehensive threat mitigation.

Jaafar et al. [11] explored detection techniques for flooding attacks targeting OSI layers 3, 4, and 7, employing signature-based, anomaly-based, and machine learning approaches. Notably, their anomaly-based detection method exhibited high computational efficiency but may require further refinement to effectively detect sophisticated attacks with nuanced patterns. Zekri and El Kafhali [12] focused on HTTP-based attacks, utilizing supervised classification techniques for detection. However, their method faced challenges in identifying new and unknown attack patterns, underscoring the importance of continuous model updates and adaptability to emerging threats.

Velliangiri et al. [13] employed deep learning, cloud computing, and artificial neural networks for detecting TCP and UDP attacks in SDN environments. Despite leveraging advanced technologies, the classifier's efficiency was compromised, particularly in scenarios involving multicasted log file requests, highlighting the need for robust and scalable detection mechanisms. Mikail Mohammed Salim et al. [14] utilized deep learning techniques implemented using the TensorFlow framework to detect TCP, UDP, and ICMP attacks. However, the accuracy of the system diminished when feature selection was based on random search methods, suggesting the importance of optimizing feature selection processes for improved detection performance.

Cvitić et al. [15] addressed TCP, UDP, and HTTP GET-based attacks through classification techniques. However, their method overlooked the time stability of send and receive data features, potentially leading to inaccuracies in detecting congestion occurrences. Ensuring the robustness of feature selection processes is essential for mitigating the risk of false positives and improving detection accuracy. Aamir et al. [16] focused on classifying DDoS attacks using the UCLA dataset, employing classification techniques. Their method encountered reduced accuracy when feature selection was based on random search methods. Optimizing feature selection processes to identify relevant attack indicators is crucial for enhancing the effectiveness of DDoS detection mechanisms.

Galeano-Brajones et al. [17] investigated TCP-based attacks, including GET/POST methods, utilizing classification techniques. However, their method faced challenges such as switches becoming unresponsive when the window size was increased, limiting scalability. Overcoming such limitations is essential for deploying detection mechanisms in diverse network environments effectively. Meejoung Kim et al. [18] employed Multilayer Perception and

Support Vector Machine with an RBF kernel classifier for detecting attacks. However, their method primarily detected low-rate attacks, potentially overlooking high-intensity attacks. Enhancing the sensitivity of detection algorithms to different attack magnitudes is critical for comprehensive threat mitigation.

N. Ravi et al. [19] utilized Support Vector Machine with RBF kernel classifiers for detecting UDP, TCP, and ICMP-based attacks. While their algorithm achieved detection by comparing with pre-existing datasets, its effectiveness may be limited in identifying novel or previously unseen attack patterns. Continuously updating datasets and refining detection algorithms can enhance adaptability to emerging threats. Y. Liu et al. [20] proposed the Server-Initiated Router Throttle (Sirt) Algorithm for mitigating DDoS attacks, achieving good accuracy in mitigation. However, reliance on pre-trained datasets in routers may restrict the algorithm's effectiveness in responding to dynamic attack scenarios. Developing mechanisms for real-time adaptation and learning can improve the agility and responsiveness of mitigation strategies in combating evolving DDoS threats.

Proposed Model

The proposed IDMEOA offers a comprehensive approach for the early detection and mitigation of DDoS attacks in SDN environments integrated with IoT devices. It encompasses the development of an entropy-based detection mechanism to analyze traffic patterns and identify anomalies indicative of DDoS attacks, with tailored strategies for detecting UDP, TCP, and ICMP SYN flood attacks. Additionally, the model incorporates dynamic thresholding techniques for real-time analysis of network traffic behavior, adaptively adjusting threshold values to distinguish between normal and abnormal activities. To mitigate detected attacks, a stochastic mitigation algorithm is developed to minimize false positives and efficiently mitigate DDoS attacks. Adaptive control mechanisms enable dynamic network response and decision-making, while integration of energy optimization techniques enhances overall network security and performance. An overall workflow of proposed model is shown in fig 1.

Idmeoa

The Integrated DDoS Detection, Mitigation, and Energy Optimization Algorithm (IDMEOA) offer a comprehensive solution for managing network security and efficiency in SDN environments with IoT devices. IDMEOA employs an entropy-based detection mechanism to identify anomalies indicative of DDoS attacks by monitoring and calculating the entropy of network traffic. Upon detecting an anomaly, the algorithm uses stochastic techniques to mitigate the attack, leveraging rules of stochastic process representation, stationarity, and entropy rate calculation to determine mitigation probability and implement rate-limiting measures. Simultaneously, IDMEOA optimizes network energy consumption by adjusting device states based on current load and routing traffic through energy-efficient paths, ensuring robust defense against attacks while maintaining optimal network performance and energy efficiency.

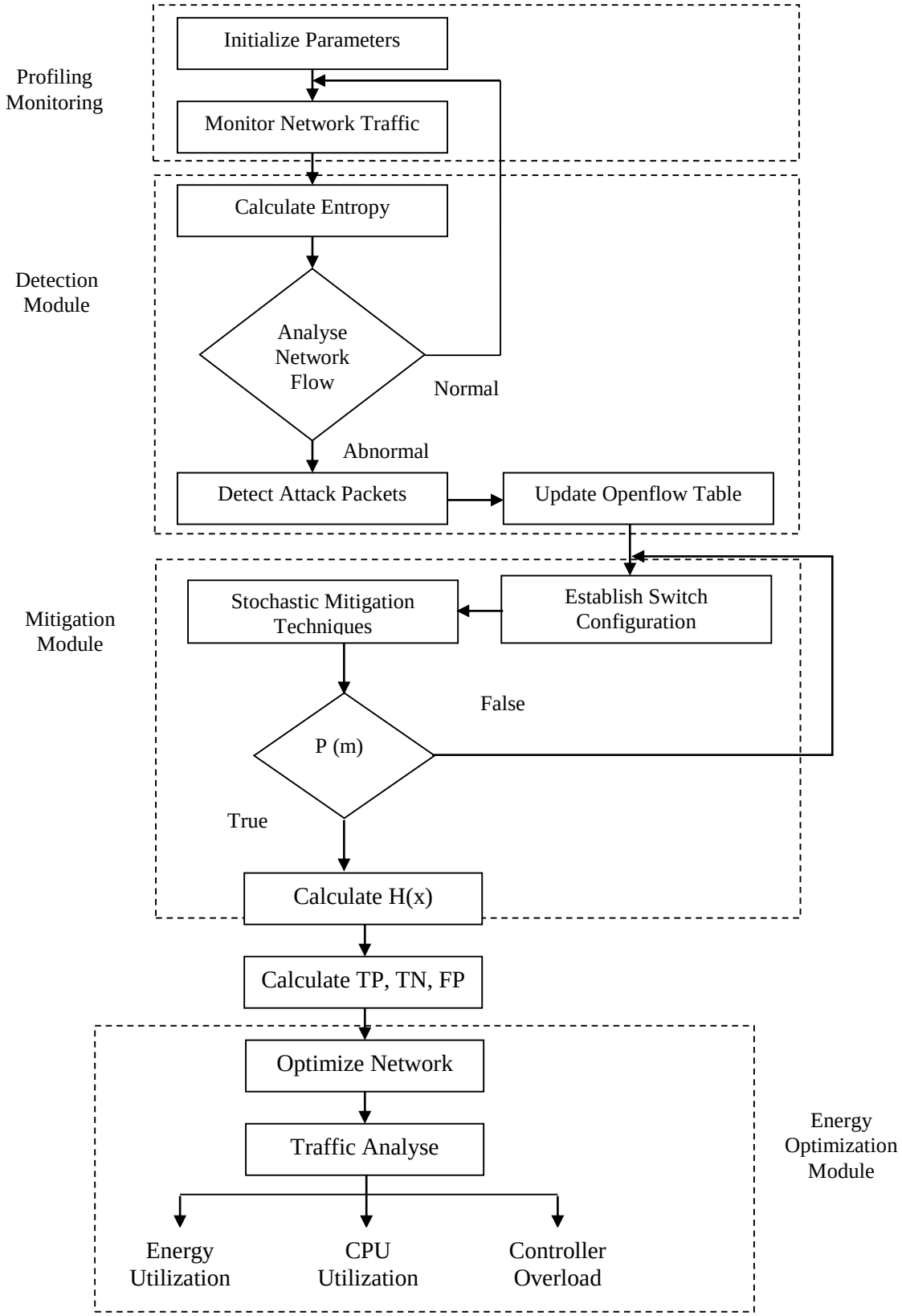

Figure 1: Overall Workflow of Proposed model

Entropy is a measure of uncertainty or randomness in a random variable. In the context of network traffic analysis, entropy is used to quantify the unpredictability of packet distributions. The equation for entropy calculation is:

$$H(X) = -\sum P(xi) log2 P(xi) \quad (1)$$

H(X): Entropy of the random variable X, P(xi): Probability of occurrence of the ith event xi, log2: Logarithm base 2.

A stochastic process is a collection of random variables indexed by time or space. In IDMEOA, network traffic data is represented as a stochastic process to capture the temporal dynamics of traffic patterns. The stochastic process representation equation is:

$X(t) = \{X(t1), X(t2), \ldots, X(tn)\}$ (2)

X(t): Stochastic process at time t, X(ti): Random variable at time ti.

Entropy rate measures the average rate of information production per unit time in a stochastic process. It provides insights into the complexity and predictability of the process over time. The entropy rate calculation equation is:

$$H(X) = limn \to \infty \frac{1}{n} H(X1, X2, \ldots, Xn) \quad (3)$$

H(X): Entropy rate of the stochastic process X, n: Number of observations in the stochastic process.

Mitigation probability determines the likelihood of successfully mitigating an attack based on the observed characteristics of the traffic data. It helps IDMEOA make informed decisions about whether to implement rate-limiting measures. The mitigation probability equation is:

$P = 1 - e - \lambda \Delta t$ (4)

P: Mitigation probability, λ: Mitigation rate parameter, Δt: Time interval.

IDMEOA optimizes network energy consumption by dynamically adjusting the states of network devices based on their current load. This adjustment ensures that devices operate efficiently while maintaining network performance. The equation for adjusting device state is:

$new\_state = current\_state - adjustment\_factor \times current\_load$ (5)

new_state: Updated state of the device, current_state: Current state of the device, adjustment_factor: Predefined adjustment factor, current_load: Current load on the device.

IDMEOA selects energy-efficient routing paths to optimize energy consumption in the network. It utilizes algorithms improved energy optimize algorithm to find the shortest and most energy-efficient paths between network devices. The equation for energy-efficient routing is:

$Routing\_Paths = improved\_energy\_optimize\_algorithm\ (G, s, t)$ (6)

Where, Routing_Paths: Selected routing paths. G: Network topology, s: Source node, t: Destination node.

Algorithm IDMEOA

Input: Source_IP, Destn_IP, Sport, Dport, Δt, S_config(S), δ, Traffic(T), Θ, Energy(E)
Output: Detect illegitimate packets, mitigate attacks, optimize network energy consumption
Procedure IDMEOA
Initialize Parameters:
Pc ← 0
baseline_entropy ← initial_baseline_entropy
adjustment_factor ← predefined_adjustment_factor
historical_data ← load_historical_data()
network_topology ← define_network_topology()
traffic_demand ← define_traffic_demand()
threshold_load ← predefined_threshold_load

While network is operational do
Traffic Monitoring and Entropy Calculation
Pc ← Pc + 1
Delay(Δt)
packet_distribution ← get_packet_distribution(network_traffic)
current_entropy ← calculate_entropy(packet_distribution)
If dynamic_threshold_adjustment(current_entropy, baseline_entropy, adjustment_factor) then
Anomaly detected
Report "Anomaly detected"
update_flow_rules(sdn_controller, malicious_sources)
Mitigation Phase Using Stochastic Techniques
T ← collectTrafficStatistics()
If detectAttack(T, Θ) then
F ← getAffectedFlows(T)
S ← getAffectedSwitches(F)
For each switch in S do
Rule 1: Stochastic Process Representation
stochastic_process ← stochastic_process_representation(T, range(len(T)))
Rule 2: Stationarity of Stochastic Process
If assume_stationarity(stochastic_process) then
Rule 3: Entropy Rate of Stochastic Process
entropy_rate ← calculate_entropy_rate(stochastic_process)
P ← mitigation_probability(stochastic_process, adjustment_factor, entropy_rate)
R ← generate_random_number()
If R ≤ P then
Drop the attack packets
Configuration ← RateLimitingConfiguration(S, F, Θ)
Else
Continue normal operations
Energy Optimization Phase
F ← getAffectedFlows(T, Θ)
S ← getAffectedSwitches(F, Θ)
For each device in network_devices do
current_load ← device.get_current_load()
adjust_device_state(device, current_load, threshold_load)
routing_paths ← energy_efficient_routing(network_topology, traffic_demand)
Configuration ← routing_paths
Monitoring and Evaluation
Calculate(Dacc, Mt, FPR, Util, E)
End Procedure

From the above algorithm, IDMEOA enhances network security and performance in SDN-IoT environments by integrating three key phases: detection, mitigation, and energy optimization. Initially, the algorithm monitors network traffic and calculates entropy to detect anomalies indicative of DDoS attacks, adjusting thresholds dynamically. Upon detecting an anomaly, it employs stochastic techniques to mitigate the attack by representing traffic data as a stochastic

process, assuming its stationarity, and calculating entropy rates to determine the mitigation probability, subsequently applying rate-limiting measures if necessary. Concurrently, IDMEOA optimizes energy consumption by adjusting device states based on current load and routing traffic through energy-efficient paths, ensuring robust defense against attacks while maintaining optimal network performance and energy efficiency.

3. Results and Discussions

The performance of the IDMEOA algorithm in detecting DDoS attacks is evaluated using metrics such as True Positives (TP), True Negatives (TN), and False Positives (FP). Entropy measures the randomness and unpredictability in network traffic, serving as a key indicator of potential anomalies. Energy efficiency is a critical aspect of IDMEOA, especially in IoT environments where resource constraints are prevalent. The algorithm's impact on CPU utilization is crucial for assessing its overhead on network resources. The controller's ability to handle additional processing tasks without significantly affecting overall network performance is vital.

The IDMEOA algorithm has demonstrated substantial benefits in enhancing network security and efficiency in SDN environments with IoT devices. The entropy-based detection mechanism effectively identifies anomalies indicative of DDoS attacks with high true positive rates and low false positives. This accuracy ensures that legitimate traffic is minimally disrupted while malicious activities are promptly mitigated.

Table 1: Comparison of Performance Evaluation

Metric	SIRT Algorithm [20]	Kernel method [19]	Entropy-Based Approach [6]	IDMEOA (Proposed)
True Positives (TP)	89%	90%	92%	97%
True Negatives (TN)	90%	92%	95%	98%
False Positives (FP)	10%	8%	5%	2%
Entropy Deviation	45%	30%	20%	5%
Energy Utilization	1500 kWh	1400 kWh	1300 kWh	1125 kWh
CPU Utilization	50%	48%	36%	15%
Controller Overhead	15%	14%	13%	10%

The table 1 compares four algorithms—SIRT Algorithm, Kernel method, Entropy-Based Approach, and IDMEOA (the proposed method)—across various performance metrics. IDMEOA shows the highest efficacy with a True Positive (TP) rate of 97%, outperforming the others (SIRT: 89%, Kernel: 90%, Entropy-Based: 92%). Similarly, IDMEOA excels in True Negatives (TN) at 98%, with the lowest False Positives (FP) at 2%, indicating superior accuracy in both detecting and rejecting cases compared to the other methods. The proposed algorithm also demonstrates the lowest entropy deviation at 5%, suggesting more stable and predictable performance. In terms of resource efficiency, IDMEOA is the most energy-efficient, utilizing only 1125 kWh, significantly lower than the others (SIRT: 1500 kWh, Kernel: 1400 kWh, Entropy-Based: 1300 kWh). It also has the lowest CPU Utilization at 15%,

indicating less computational demand, and the lowest Controller Overhead at 10%, reflecting reduced system strain and improved overall efficiency.

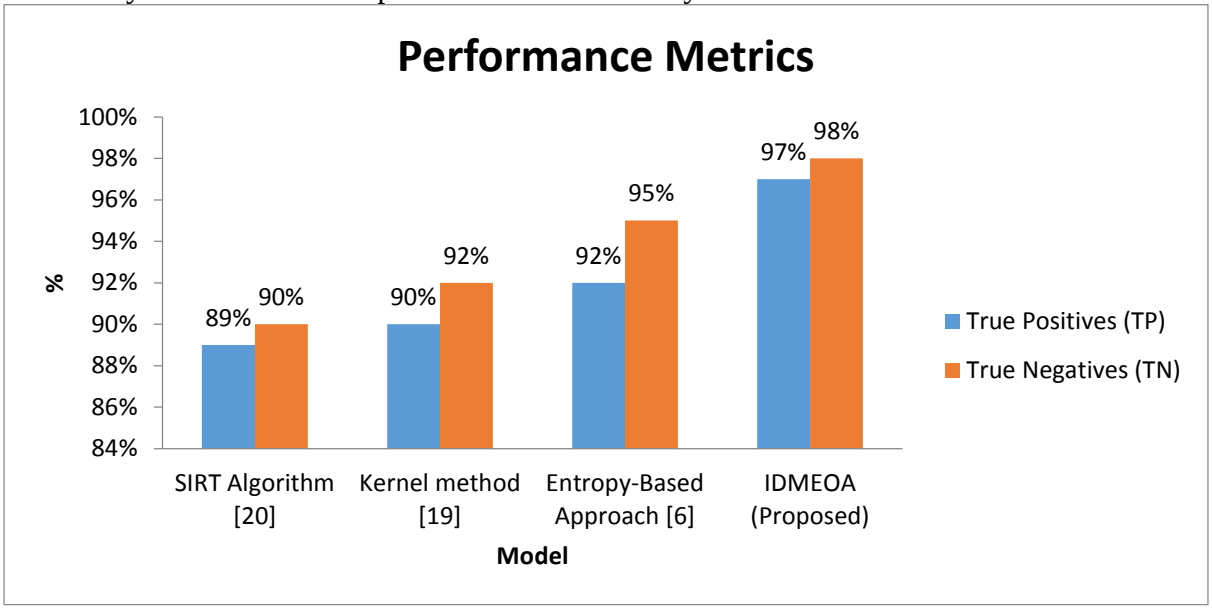

Figure 2: Performance Comparison of TP and TN

From the fig 2, the IDMEOA demonstrates the highest performance with a TP rate of 97%, indicating its superior ability to correctly identify positive cases. Similarly, IDMEOA also achieves the highest TN rate at 98%, reflecting its effectiveness in correctly identifying negative cases. It shows IDMEOA as the most effective algorithm in accurately classifying both positive and negative cases, surpassing the performance of the other three methods.

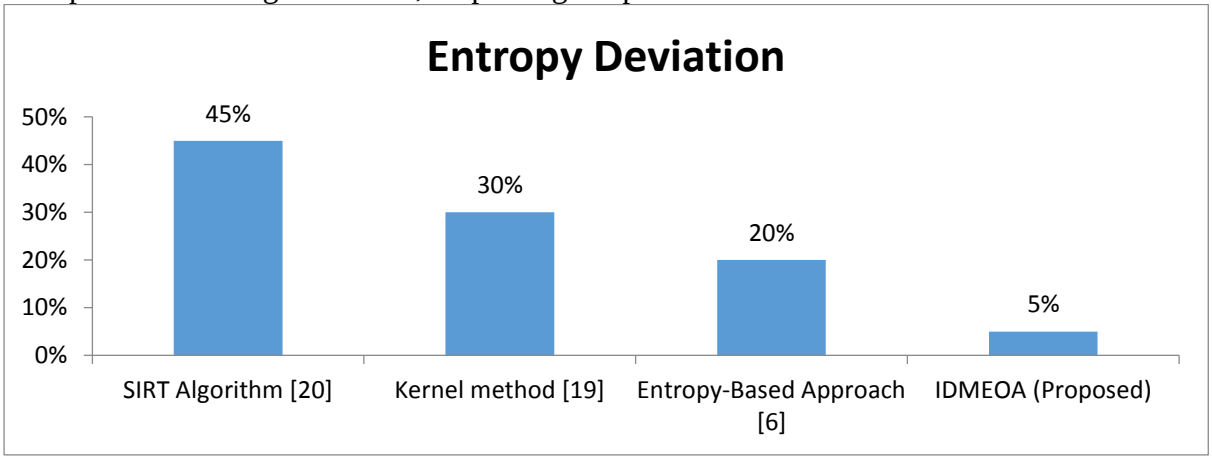

Figure 3: Comparison of Entropy Deviation

From the fig 3, IDMEOA shows the lowest entropy deviation at 5%, indicating that it produces the most stable and predictable results. This is significantly lower compared to the Entropy-Based Approach at 20%, the Kernel method at 30%, and the SIRT Algorithm at 45%. The data clearly highlights that IDMEOA is the most reliable and consistent algorithm, as it minimizes variability and maintains a higher degree of order in its operations compared to the other methods.

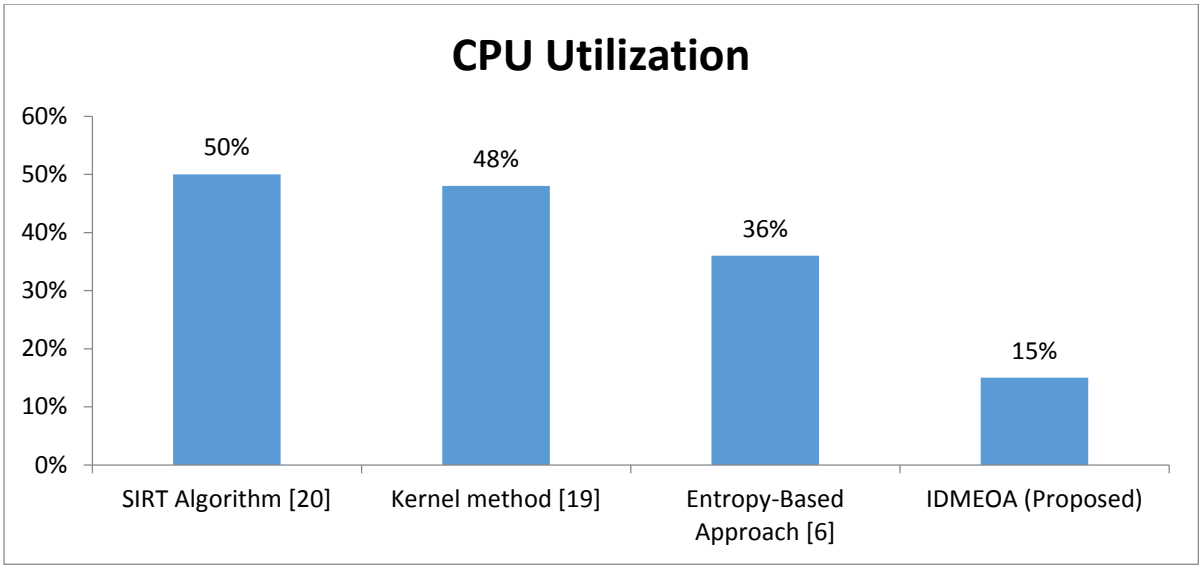

Figure 4: CPU Utilization

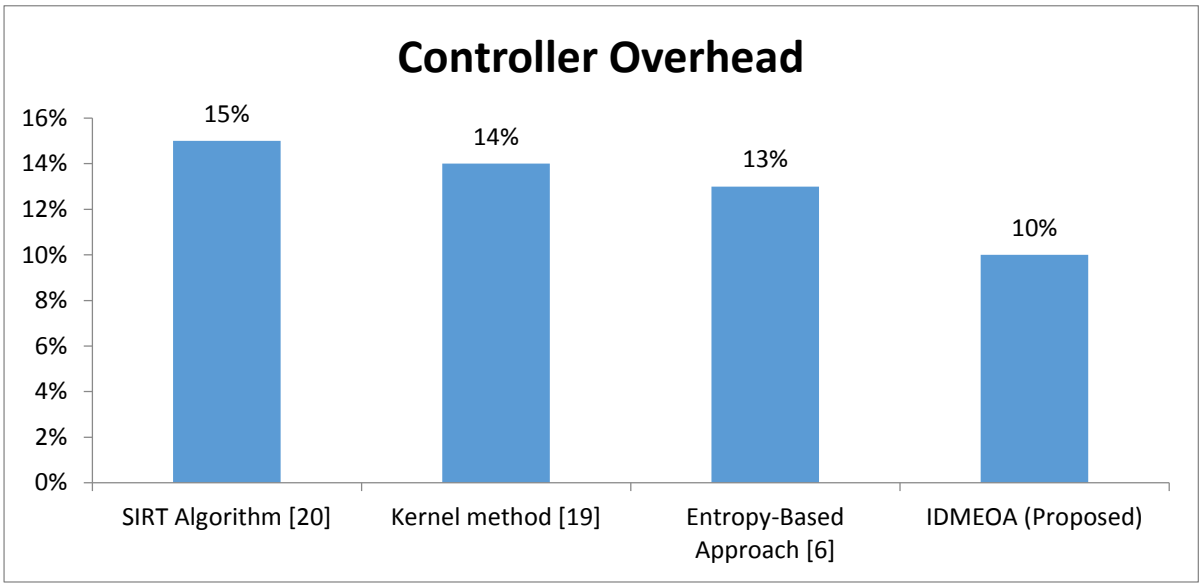

Figure 5: Controller Overhead Comparison

Fig 4 and 5 compares the CPU Utilization and Controller Overhead of four algorithms: the SIRT Algorithm, Kernel method, Entropy-Based Approach, and IDMEOA (the proposed method). In terms of CPU Utilization, which measures the percentage of CPU capacity used, the IDMEOA is the most efficient, utilizing only 15% of CPU resources. This is a substantial improvement over the Entropy-Based Approach at 36%, the Kernel method at 48%, and the SIRT Algorithm at 50%. Regarding Controller Overhead, which indicates the additional processing burden placed on the system controller, the IDMEOA again demonstrates superior performance with the lowest overhead at 10%. This compares favorably to the Entropy-Based Approach at 13%, the Kernel method at 14%, and the SIRT Algorithm at 15%. These metrics underscore IDMEOA's efficiency and minimal impact on system resources, making it the most resource-efficient among the algorithms evaluated.

4. Conclusion

DDoS attacks pose a significant threat to network security, necessitating the development of more advanced techniques for their detection and mitigation. Special attention is required to identify and neutralize attack nodes within the network effectively. The EDDA plays a crucial role in this endeavor, achieving high detection rates for attack nodes. Upon detection, these attack nodes are mitigated using stochastic techniques, leading to a notable enhancement in network performance. Furthermore, energy optimization techniques are employed to improve the overall efficiency of the network, synergizing with the enhanced detection and mitigation capabilities. Comparative analysis reveals that the proposed approaches outperform existing methods, with notable achievements in detection accuracy, mitigation time reduction, and optimization control. The IDMEOA outperforms the other algorithms in several key areas. It has the highest True Positive (TP) rate at 97% and the highest True Negative (TN) rate at 98%, indicating superior accuracy in correctly identifying both positive and negative cases. Additionally, it has the lowest False Positive (FP) rate at 2%, the lowest entropy deviation at 5%, and the most efficient energy utilization at 1125 kWh. IDMEOA also demonstrates remarkable efficiency in terms of resource usage, with the lowest CPU Utilization at 15% and the least Controller Overhead at 10%. These metrics collectively highlight IDMEOA as the most effective and efficient algorithm among those evaluated, excelling in both accuracy and resource management.

5. References

1. Liatifis, A., Sarigiannidis, P., Argyriou, V., & Lagkas, T. (2023). Advancing sdn from openflow to p4: A survey. ACM Computing Surveys, 55(9), 1-37.
2. Ali, M. N., Imran, M., din, M. S. U., & Kim, B. S. (2023). Low rate DDoS detection using weighted federated learning in SDN control plane in IoT network. Applied Sciences, 13(3), 1431.
3. Misra, S., Pal, S., Ahmed, N., & Mukherjee, A. (2023). Sdn-controlled resource- tailored analytics for healthcare iot system. IEEE Systems Journal.
4. Rahman, A., Islam, J., Kundu, D., Karim, R., Rahman, Z., Band, S. S.. & Kumar,N. (2023). Impacts of blockchain in software-defined Internet of Things ecosystem with Network Function Virtualization for smart applications: Present perspectives and future directions. International Journal of Communication Systems, e5429.
5. Cherian, M., & Varma, S. L. (2023). Secure SDN–IoT Framework for DDoS Attack Detection Using Deep Learning and Counter Based Approach. Journal of Network and Systems Management, 31(3).
6. Aladaileh, M. A., Anbar, M., Hintaw, A. J., Hasbullah, I. H., Bahashwan, A. A., Al-Amiedy, T. A., & Ibrahim, D. R. (2023). Effectiveness of an Entropy-Based Approach for Detecting Low-and High-Rate DDoS Attacks against the SDN Controller: Experimental Analysis. *Applied Sciences*, *13*(2), 775.
7. Chaganti, R., Suliman, W., Ravi, V., & Dua, A. (2023). Deep learning approach for SDN-enabled intrusion detection system in IoT networks. Information, 14(1), 41.
8. Aldaej, A. (2019). Enhancing cyber security in modern internet of things (iot) using intrusion prevention algorithm for iot (ipai). IEEE Access
9. Bhushan, K., & Gupta, B. B. (2018). Hypothesis test for low-rate DDoS attack detection in cloud computing environment. Procedia computer science, 132, 947-955.
10. Lima Filho, F. S. D., Silveira, F. A., de Medeiros Brito Junior, A., Vargas-Solar, G., & Silveira, L. F. (2019). Smart detection: an online approach for DoS/DDoS attack detection using machine learning. Security and Communication Networks, 2019.

11. Jaafar, G. A., Abdullah, S. M., & Ismail, S. (2019). Review of recent detection methods for HTTP DDoS attack. Journal of Computer Networks and Communications, 2019.
12. Zekri, M., El Kafhali, S., Aboutabit, N., & Saadi, Y. (2017, October). DDoS attack detection using machine learning techniques in cloud computing environments. In 2017 3rd International Conference of Cloud Computing Technologies and Applications (CloudTech) (pp. 1-7). IEEE.
13. Velliangiri, S., Karthikeyan, P., & Vinoth Kumar, V. (2020). Detection of distributed denial of service attack in cloud computing using the optimization-based deep networks. Journal of Experimental & Theoretical Artificial Intelligence, 1-20
14. Mikail Mohammed Salim1 · Shailendra Rathore1 · Jong Hyuk Park1(2019) Distributed denial of service attacks and its defenses in IoT:A survey Springer,The Journal of Supercomputing
15. Cvitić, I., Peraković, D., Periša, M., & Botica, M. (2019). Novel approach for detection of IoT generated DDoS traffic. Wireless Networks, 1-14.
16. Aamir, M., & Zaidi, S. M. A. (2019). DDoS attack detection with feature engineering and machine learning: the framework and performance evaluation. International Journal of Information Security, 18(6), 761-785.
17. Galeano-Brajones, J., Carmona-Murillo, J., Valenzuela-Valdés, J. F., & Luna-Valero, F. (2020). Detection and Mitigation of DoS and DDoS Attacks in IoT-Based Stateful SDN: An Experimental Approach. Sensors, 20(3).
18. Galeano-Brajones, J., Carmona-Murillo, J., Valenzuela-Valdés, J. F., & Luna-Valero, F. (2020). Detection and Mitigation of DoS and DDoS Attacks in IoT-Based Stateful SDN: An Experimental Approach. Sensors, 20(3
19. N. Ravi, S.M. Shalinie, Learning-driven detection and mitigation of DDoS attack in IoT via SDN-cloud architecture.IEEE Internet Things J. 7(4), 3559–3570 (2020)
20. X. Liu, S. Zhao, A. Liu, N. Xiong, and A. V. Vasilakos, ``Knowledge-aware proactive nodes selection approach for energy management in Internet of Things," Future Generat. Comput. Syst., Aug. 2017,doi: https://doi.org/10.1016/j.future.2017.07.022