[1]Jaimin M Shroff
[2]Sanjay M Shah

Entropy-Based Feature Selection for DDoS Detection: Enhancing Importance with Mutual Information Scores in SDN

Journal of Electrical Systems

Abstract: - DDoS attacks severely threaten computer networks by flooding systems with traffic from various sources, necessitating advanced real-time detection methods in cybersecurity. Current detection techniques, however, suffer from high false positive rates and struggle to identify complex attack patterns. There's an urgent need for improved detection systems that can accurately detect and mitigate these threats, requiring a deep understanding of network behavior, continuous traffic monitoring, and the use of sophisticated analytical tools to interpret the nuances of DDoS attack patterns effectively in Software Defined Network (SDN). This research introduces a novel Distributed Denial of Service (DDoS) detection strategy utilizing a multilayer feature selection technique, where features are initially selected based on their mutual information score. Subsequently, these features undergo further classification via a joint entropy-based method, pinpointing those crucial for identifying diverse DDoS attack types. This innovative approach is rigorously compared with established probability-based methods, including the Shannon, Ranyi, Tsallis, Bhattacharya, Bhatia Wolf, and Ubriaco coefficients, to assess its efficacy. Extensive incorporation of the CICDDoS 2019 dataset provides an in-depth analysis; the experimental results also demonstrate the superior importance score of top k features as compared to contemporary techniques. Impressively, the newly proposed technique has exceptional capability, acquiring an importance score of 0.99 (on the scale of 0 to 1) in the extraction of mutually correlated features, offering a high chance to improve the detection of DDoS attacks remarkably.

Keywords: *DDoS, Entropy, Feature Selection, Machine Learning, Mutual Information Score, SDN, Statistical*.

I. INTRODUCTION

In today's digital era, DDoS attacks stand as formidable threats, challenging the robustness and resilience of online infrastructures. These attacks not only disrupt service availability but also compromise the integrity and security of vast digital ecosystems, affecting entities ranging from individual enterprises to critical national infrastructure. With the advent of sophisticated attack vectors, leveraging the interconnectedness of IoT devices and cloud services, the traditional paradigms of network defense are increasingly being outstripped. This escalation underscores the need for innovative and adaptable mitigation strategies [1-3].

The evolution of the threat landscape, characterized by the sophistication of attacks and the democratization of cyber-offensive tools via the dark web, necessitates a paradigm shift in how network security is conceptualized and implemented. DDoS attacks, with their capacity to inflict significant economic and social damage, represent a critical vector of disruption, necessitating robust countermeasures to safeguard digital assets.

One notable example that illustrates the impact of DDoS attacks is the 2016 Dyn attack [4]. In this case, a massive botnet comprising compromised Internet of Things (IoT) devices was employed to launch a series of DDoS attacks on the infrastructure of Dyn, a major Domain Name System (DNS) provider. The attack resulted in widespread service disruptions for popular websites and services, including Twitter, Netflix, and Spotify. This incident highlighted the potential vulnerabilities within the interconnected ecosystem of internet infrastructure and the need for effective DDoS mitigation measures. Against this backdrop, Software-defined Networking (SDN) emerges as a beacon of hope, offering a transformative approach to network management and security. The architectural separation of the control and data planes in SDN not only introduces operational efficiencies but also paves the way for advanced security mechanisms that are dynamic, scalable, and intelligent. This paper delves into how SDN, augmented with entropy-based detection and mutual information scores, can revolutionize DDoS defense strategies, enhancing detection accuracy and facilitating a proactive security posture [5-7].

By contextualizing the severity and complexity of modern DDoS attacks and aligning them with the strategic benefits of SDN, this study underscores the critical need for advancing research in network security mechanisms.

[1] Gujarat Technological University, Ahmedabad-382424, India
[2] Government Engineering College, Rajkot-360005, India
* Corresponding author: jaimin_shroff22@yahoo.co.in

Our work seeks to bridge the gap between traditional detection methods and the exigencies of contemporary network threat landscapes, proposing a novel detection framework that epitomizes the synergy between statistical rigor and network engineering.

A. DDoS Attacks and Types:

A Distributed Denial of Service (DDoS) attack is a malicious attempt to disrupt the availability of a network, system, or service by overwhelming it with a flood of traffic from multiple sources. The goal of a DDoS attack is to exhaust the target's resources, such as bandwidth, processing power, or memory, rendering it inaccessible to legitimate users. DDoS attacks can have severe consequences, including financial loss, reputation damage, and disruption of critical services. Here are the main types of DDoS attacks:

- Volumetric Attacks: These attacks generate an enormous amount of traffic to saturate the bandwidth of the target system. They are straightforward in their approach but can be powerful due to the sheer volume of traffic generated [8].
- TCP State-Exhaustion Attacks: By exploiting the way TCP connections are established, these attacks fill up the connection tables in network devices, leading to a denial of service as new legitimate connections cannot be established [9].
- Application Layer Attacks: These are more sophisticated as they target specific aspects of an application or service. They require less bandwidth to execute but can be very effective in disrupting the targeted service [10].
- Reflective/Amplified Attacks: These involve a third-party component to increase the magnitude of the attack, making the mitigation more challenging as it involves filtering out malicious traffic from legitimate responses [11].

Understanding these types of DDoS attacks is crucial for developing effective mitigation strategies. Each type of attack requires a different approach to detect and prevent, highlighting the importance of having a comprehensive security posture that includes advanced detection methods, especially in dynamic environments like SDN.

B. Importance of advanced detection methods in SDN environments

The advanced DDoS attack mitigation methods facilitated by Software-defined networking (SDN) offer a comprehensive approach to safeguarding network infrastructure. tables show how advance detection method maps with capabilities of SDN [12].

Table 1. DDoS Attack Types and SDN Mitigation Methods

Attack Type	**Attack Description**	**Examples**	**SDN Mitigation Feature**	**Mitigation Technique**
Volumetric Attacks [8]	Aim to consume the target's bandwidth, or service unreachable.	UDP Flood, ICMP Flood, DNS Amplification	Enhanced Scalability	Dynamic resource scaling and traffic distribution
TCP State-Exhaustion Attacks [9]	Overwhelm the target's TCP connection state tables, preventing legitimate connections.	SYN Flood, ACK Flood, TCP Fragmentation Attacks	Automated and Programmable Responses	Automated traffic control and response
Application Layer Attacks [10]	Target specific applications/services to exhaust their resources.	HTTP/HTTPS Flood, Slowloris, Application Layer Protocol Attacks	Adaptability and Dynamic Configuration	Real-time policy and configuration updates
Reflective/Amplified Attacks [11]	Use legitimate servers to amplify the attack traffic directed at the target.	DNS, NTP Amplification, SNMP Amplification	Distributed Defence Mechanisms	Network-wide security function distribution

C. Entropy and Mutual information as tools for DDoS detection.

Entropy and mutual information are fundamental concepts in information theory that have been effectively adapted for use in DDoS detection within network security frameworks, particularly in Software-Defined Networking (SDN) environments. Entropy in network traffic analysis measures randomness, aiding in DDoS detection by signaling anomalous traffic changes, where high entropy suggests diverse sources (volumetric attacks) and low entropy indicates targeted attacks [13]. Mutual information in DDoS detection identifies key correlations among network traffic features, crucial for pinpointing attack indicators, particularly valuable in SDN's dynamic security environment [14].

II. RELATED WORK

The realm of Distributed Denial of Service (DDoS) attack detection has seen significant evolution, transitioning from traditional methods to more sophisticated contemporary approaches that leverage advancements in technology and computational methods. Wherever Times is specified, Times Roman or Times New Roman may be used. If neither is available on your word processor, please use the font closest in appearance to Times. Avoid using bit-mapped fonts if possible. True-Type 1 or Open Type fonts are preferred. Please embed symbol fonts, as well, for math, etc.

A. Traditional vs Contemporary DDoS Detection Methods

Traditional methods primarily relied on signature-based and anomaly-based detection. Signature-based detection involves matching known patterns of malicious activity within network traffic, effectively identifying well-documented attack vectors but faltering against new or modified threats. Anomaly-based detection, on the other hand, focuses on identifying deviations from established normal traffic patterns, offering a broader scope of detection that includes previously unknown attacks [15].

Table 2. DDoS Attack Detection Methods and Techniques

Detection Method	**Detection Category**	**Example Techniques**
Traffic-Anomaly Detection [16]	Traditional/ Contemporary	Statistical Analysis (standard deviation, moving average), Machine Learning (decision trees, SVM, k-means)
Signature-based Detection [17]	Traditional	Pattern matching with known attack signatures
Flow-based Detection [18]	Contemporary	Flow Size Analysis, Flow Duration Analysis, Flow Correlation
Heuristic-based Detection [19]	Contemporary	Threshold-based Heuristics (on packet rate, bandwidth), Behaviour-based Heuristics (traffic spikes, unusual patterns)

Recent advancements have introduced methods utilizing machine learning (ML) and artificial intelligence (AI) to enhance detection accuracy and response times. These methods analyze vast datasets to identify subtle patterns and anomalies indicative of DDoS activity, adapting to evolving attack behaviors dynamically. Additionally, the integration of these techniques into Software-Defined Networking (SDN) has provided a more centralized and flexible approach to network monitoring and management, allowing for real-time detection and mitigation of attacks [16-19].

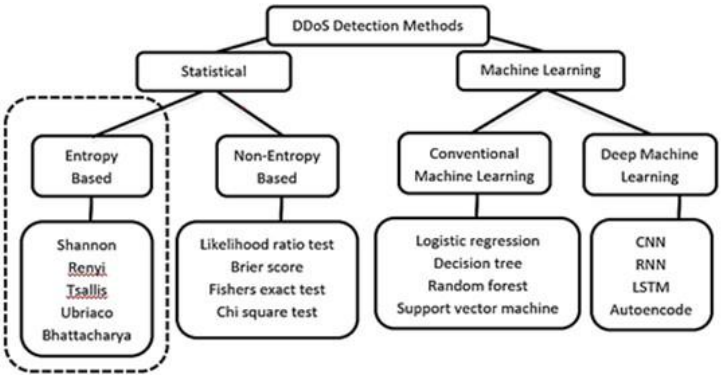

Figure 1. Classification of DDOS Detection Methods

Figure 1 represents the DDoS detection methods are divided into two main categories: statistical and machine learning. Under the statistical category, there are two subdivisions: entropy-based and non-entropy-based methods. Meanwhile, the machine learning category splits into conventional machine learning and deep learning techniques. Our proposed methodology falls under the entropy-based statistical approach.

In general concept, Entropy is the amount of information contained in the variable. The amount is not just determined by no. of different values the variable takes on but it is proportional to the amount of randomness. Shannon entropy is a classic and maximum used entropy formula to calculate entropy in information theory.

$$H(X) = -\sum_{i=1}^{N} p(x_i) \log p(x_i) \quad (1)$$

Where:

$P(x_i)$ is a probability that x takes value x_i.

Entropy in network security quantifies the variability or randomness of packet attributes within network traffic. For DDoS (Distributed Denial of Service) detection, monitoring involves analyzing these packet attributes to compute their entropy. Typically, higher entropy suggests increased randomness, but during a DDoS attack, where a specific host or network is the target, certain packet attributes like the destination IP or port may repeatedly occur, leading to a decrease in entropy for these attributes. Therefore, by conducting a statistical analysis of entropy values across different packet attributes, it's possible to detect anomalies indicative of DDoS attacks. This decrease in entropy, contrary to normal conditions where traffic attributes are more distributed, acts as a critical signal in identifying the focused nature of DDoS threats [20].

The mutual information (MI) score is a measure of the mutual dependence between two variables. It quantifies the amount of information obtained about one variable through the other. Mathematically, the mutual information I (X; Y) between two random variables X and Y is defined as:

$$I(X:Y) = \sum_{x \in X} \sum_{y \in Y} p(x,y) \log \frac{p(x,y)}{p(x)P(y)} \quad (2)$$

Where:

p (x, y) is the joint probability distribution function of X and Y,

p(x) and p(y) are the marginal probability distribution functions of X and Y, respectively, the logarithm is typically base 2, which means the information is measured in bits.

Mutual information in network security is employed for feature selection and correlation analysis. It helps in identifying key features in network traffic that signify threat presence and understanding relationships between traffic behaviors to enhance the accuracy of threat detection systems, particularly in identifying malicious activities [21].

Khan et al. [22] introduced an entropy-based feature selection combined with granular computing to effectively discern DoS attacks from normal traffic, utilizing the NSL KDD dataset. Their methodology, focused on optimizing the detection process, successfully identified 41 critical features, with Shannon entropy employed for the analytical assessment of each feature to enhance detection accuracy and system efficiency. Shukla et al. [23] developed an entropy-based anomaly detection technique that measures the entropy of network packet lengths to spot irregularities, achieving a 90% detection rate of attacks. However, their research lacks extensive validation with real-world data, relying solely on packet length entropy for anomaly detection. This singular focus might miss other critical network traffic features indicative of anomalies, suggesting that integrating more diverse features could enhance the detection's robustness and accuracy. Swami et al. [24] showcased an entropy-based method for DDoS attack detection, focusing on destination IP entropy across a network with 7 open flow switches and 48 hosts. Using a 25-packet window for entropy calculation, they achieved rapid DDoS detection with low computational overhead. However, their study lacks a mechanism for detecting slow DoS attacks, indicating a potential area for further research and method enhancement. Ramprasath et al. [25] proposed a method for dynamically updating Access Control List (ACL) rules based on network traffic pattern analysis to block malicious flood traffic effectively while allowing legitimate traffic. This real-time ACL adjustment, responsive to flood attack patterns, showed better accuracy in distinguishing malicious traffic compared to SVM. Basicevic et al. [26] explored the application of Tsallis entropy for detecting SYN flood DoS attacks, comparing it with Shannon entropy in terms of detection delay and accuracy. The study found Tsallis entropy-based detection to outperform Shannon's in reducing false positives,

though it necessitates precise adjustment of the Tsallis Q parameter to suit network traffic behavior. Ahalawat et al. [27] developed a Rényi Entropy-based method for detecting and mitigating low-rate DDoS attacks in SDN, focusing on traffic pattern analysis and threshold settings for effective discrimination between malicious and legitimate traffic, with challenges noted in accurately tuning false-negative rates and detection timings. This comparative analysis highlights the nuanced approach required to optimize entropy-based detection mechanisms in network security.

B. Existing gaps and challenges in current DDoS detection techniques

Traditional entropy-based detection methods may not effectively adapt to evolving DDoS attack strategies, summary of the research gaps and challenges identified in each of the discussed papers.

Table 3. Research Gaps and Challenges in DDoS Detection

Paper	**Research Gaps and Challenges**
Khan et al. [22]	Limited to the NSL KDD dataset; the methodology may need adaptation for real-time network traffic and diverse attack scenarios.
Shukla et al. [23]	Sole reliance on packet length entropy; lacks extensive real-world validation and overlooks other potentially indicative traffic features.
Swami et al. [24]	Focuses primarily on rapid detection with low computational overhead but does not address slow DoS attack detection.
Ramprasath et al. [25]	While effective in dynamic ACL rule updating, the method's adaptability to varying network conditions and attack types needs further exploration.
Basicevic et al. [26]	Requires careful tuning of the Tsallis Q parameter, and its performance comparison with Shannon entropy indicates a need for broader validation across different network settings.
Ahalawat et al. [27]	Challenges in tuning false-negative rates and detection timings, particularly in SDN environments with low-rate DDoS attacks.

III. PROPOSED METHOD

To develop a novel approach for DDoS detection in Software-Defined Networking (SDN) using entropy and mutual information, the proposed model pipeline describes in this figure 2.

The proposed DDoS detection strategy in SDN employs mutual information (MI) scores to discern vital network traffic attributes, significantly enhancing the importance score and velocity of detection. Initially, the MI score of each network feature is computed, isolating the top k features with the highest MI scores. Subsequently, joint entropy is utilized to evaluate the collective uncertainty of these selected features, furnishing a detailed insight into network traffic dynamics. This approach aids in swiftly pinpointing DDoS incidents. By integrating these methods, the detection mechanism becomes more streamlined, expediting the analysis process and fostering prompt and effective network security management. This holistic view enables a more nuanced detection of DDoS activities, leveraging the strengths of both mutual information and joint entropy to improve the detection framework.

Joint Entropy Calculation Equation is:

$$H\ (X,Y)\ =\ -\ \sum_{x\in X}\sum_{y\in Y} p(x,y)\log p(x,y) \qquad (3)$$

Where:

p (x, y) is the joint probability distribution function of X and Y.

After determining the relevance and mutual connections of the top K features for DDoS detection through joint entropy calculation, the next step involves partitioning the dataset into training and testing phases. Typically, an 80/20 split is used, where 80% of the data is allocated for training the detection model, and the remaining 20% is reserved for testing its performance.

The comparison phase includes evaluating different types of entropy metrics to assess their effectiveness in detecting DDoS attacks. This involves comparing the importance score of various entropy-based methods, such as Shannon entropy, Rényi entropy, and Tsallis entropy, Ubriaco Entropy, Bhattacharya Entropy to determine which provides the best performance in identifying DDoS activities accurately.

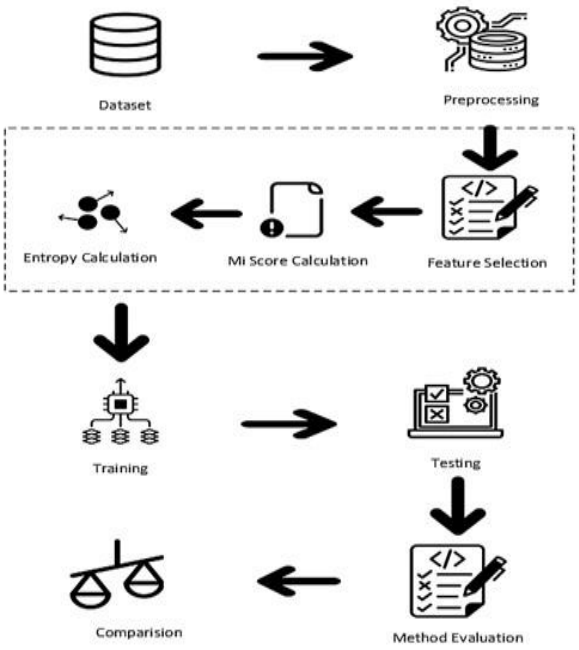

Figure 2. Proposed Model Pipeline

This structured approach allows for a comprehensive evaluation of the detection method ensuring that the chosen method not only identifies the significant features effectively but also performs well in practical scenarios, distinguishing between normal and malicious traffic with high importance score. In the first stage of the proposed flowchart's pre-processing phase, a novel two-tiered feature selection method is employed. This method is divided into two distinct steps:

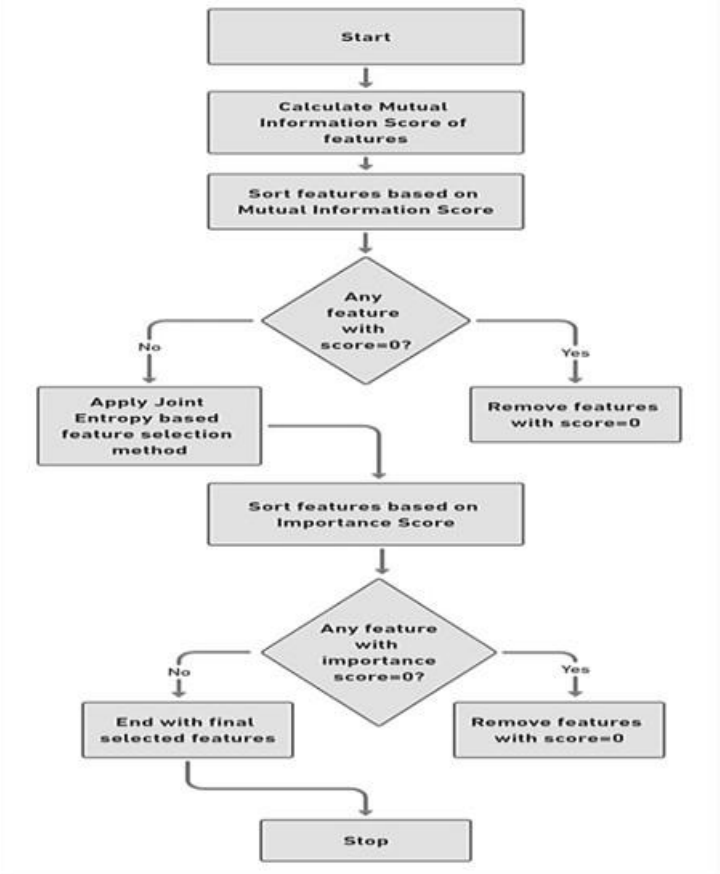

Figure 3. Flow chart of proposed method

Relevance Assessment: Initially, the features in the dataset are scrutinized to evaluate their relevance. This is achieved by calculating the mutual information score for each feature. The mutual information score is a statistical measure that quantifies the amount of information obtained about one variable through another. In this context, it helps in identifying the extent to which each feature in the dataset contributes to the understanding of the outcome variable.

Importance Determination: Following the initial relevance assessment, the second phase engages a secondary level of feature selection. Here, the importance of each feature is gauged using a computation known as joint entropy. Joint entropy is a concept from information theory that measures the amount of uncertainty present in a set of variables. In this scenario, it is used to calculate the feature importance score, which signifies the collective contribution of each feature to the predictive power of the model. This innovative two-level feature selection approach in the pre-processing phase not only helps in identifying the most relevant and important features in the dataset but also streamlines the data, making it more manageable and effective for the predictive modeling process.

IV. EXPERIMENTAL RESULT AND ANALYSIS

A. The Dataset

The CICDDoS2019 dataset is a comprehensive collection that includes both benign and various common DDoS attack traffic, simulating real-world network conditions. This dataset was crafted using the CICFlowMeter-V3 for network traffic analysis, providing labelled flows with detailed information such as timestamps, source and destination IPs, ports, protocols, and attack types. The dataset's structured and detailed nature makes it an excellent resource for developing and evaluating DDoS detection methods, providing a robust platform to test the effectiveness of proposed methods in a controlled yet realistic network environment [28].

Table 4. Feature Usage in DDoS Attack Detection Methods

Type	**Actual Feature**	**Used Feature**	**Data Points**
NTP	84	77	225001
DNS	84	79	225001
LDAP	84	74	225001
MSSQL	84	78	225001
NetBIOS	84	80	225001
SNMP	84	79	225001
SSDP	84	75	225001
UDP	84	79	235236
UDP-Lag	84	79	225001
SYN	84	76	225001
TFTP	84	81	225001

B. Evaluation Matrix

In these experiments, the CICDDoS 2019 dataset served as the primary source of data, featuring 11 distinct attack types. Although the dataset comprises 84 network packet attributes, the selection for analysis was based on the mutual information score, ensuring only pertinent features were considered for each type of attack. The classification table for the CICDDoS 2019 dataset highlights that the number of critical features for identifying various attacks is fewer than the total features specified per attack. Approximately 225,000 data points for each attack type were utilized in our analysis.

Initially, preprocessing was undertaken to eliminate non-numerical columns and cleanse the data. Subsequently, we embarked on the feature selection phase, employing the mutual information (MI) score to evaluate each attribute's relevance. Based on these MI scores, we prioritized the top K features for in-depth analysis, setting K values at 5, 14, 35, and encompassing all pertinent features for various DDoS attack categories to determine the optimal feature count required for each attack type.

Following feature selection, we proceeded to compute entropy using six distinct methodologies: Shannon entropy, Renyi entropy, Tsallis entropy, Bhatia-Wolf entropy, Bhattacharya coefficient, and the Ubriaco method. Our innovative approach, however, hinges on joint entropy calculations to discern the most significant features, sequentially analysing sets of the first 5, 14, 35 features, and ultimately, all the employed features to ascertain their joint entropy.

The final stage entails a comparative analysis between our novel method and the six aforementioned techniques, culminating in the importance score assessment during the training and testing phases. This comprehensive evaluation is graphically represented to illustrate the efficacy of our proposed method in relation to the other established entropy calculation methods.

The graphs presented below compare various methods against our proposed approach, which is predicated on joint entropy calculations. For different categories of Distributed Denial of Service (DDoS) attacks, the outcomes vary significantly. These results demonstrate that joint entropy, rather than generalized entropy measures, yields more effective outcomes in distinguishing between the types of attacks.

Figure 4 displays an analysis of distributed denial-of-service (DDoS) attacks on UDP packets. The findings reveal that the importance scores for the top five features derived from Shannon, Renyi, Tsallis, and Bhatia Wolf entropy methods are all 0.80, while Ubriaco slightly decreases to 0.66. However, the Bhattacharya coefficient yields promising results at 0.90, but proposed method significantly improves the outcome to 0.97. As the number of top features increases, so does the result, increase marginally, when all top k features are considered, such as in the case of 79 features. In Figure 5, the analysis shifts to DDoS attacks on DNS packets. Here, both the Bhattacharya method and our proposed method prove highly effective compared to other entropy-based methods, boasting an importance score of 0.98. However, in DNS packets, increasing the number of features results in a slight decrease in the proposed method's performance. Figure 6 presents an analysis of DDoS attacks on LDAP packets, while Figures 7 through 14 depict DDoS attacks on various other packets such as MSSQL, NetBIOS, NTP, SNMP, SSDP, SYN, TFTP, and UDP Lag. Across all these analyses, the proposed method consistently outperforms the other six methods in terms of feature importance score.

Overall, the graphs demonstrate that for a DDoS attack's top five features, the importance score is approximately 0.99. Expanding the analysis to encompass 14 or 35 features enhances the importance score, but this score diminishes when evaluating the entire set of selected features. This decline in relevance score is attributed to the inclusion of features with notably low mutual information scores, which undermines the method's effectiveness.

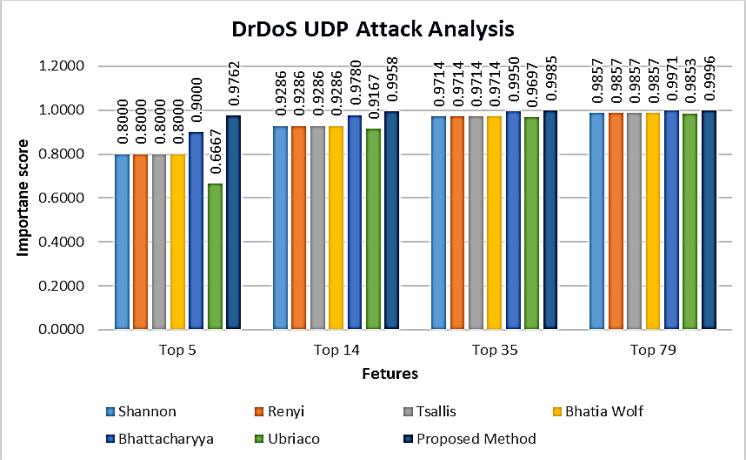

Figure 4. DrDoS UDP Attack Analysis

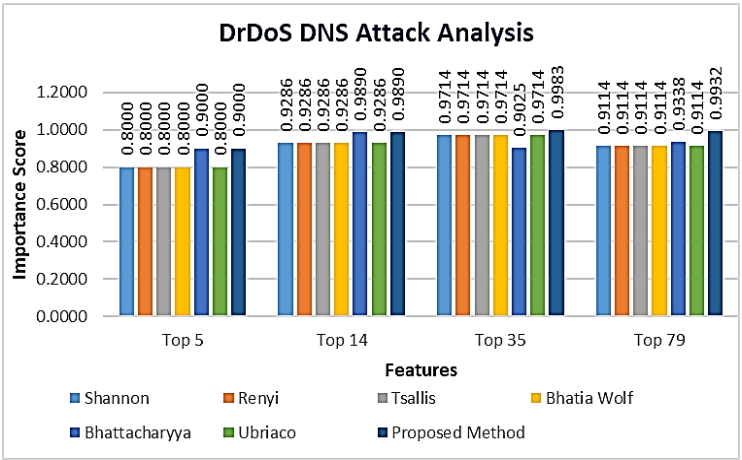

Figure 5. DrDoS DNS Attack Analysis

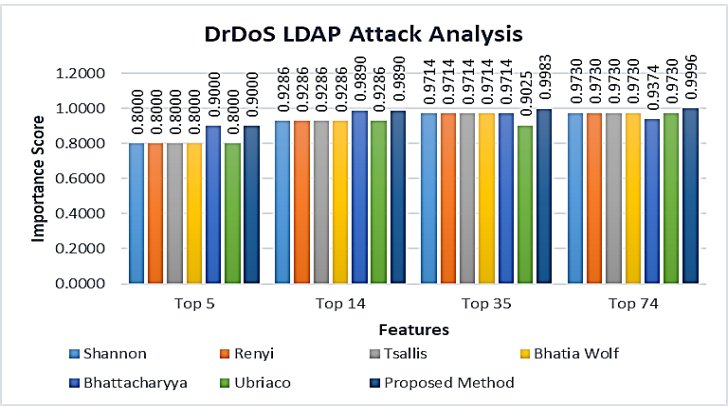

Figure 6. DrDoS LDAP Attack Analysis

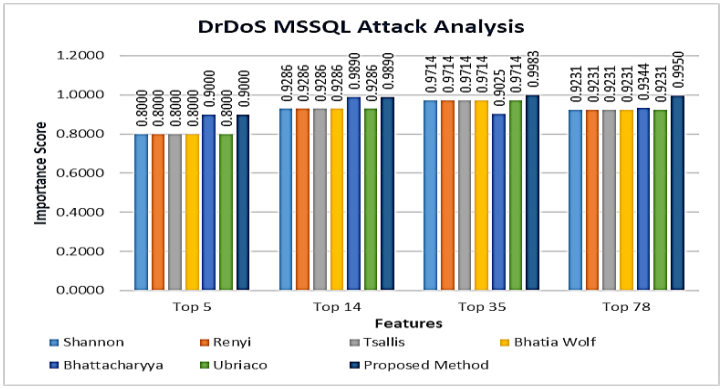

Figure 7. DrDoS MSSQL Attack Analysis

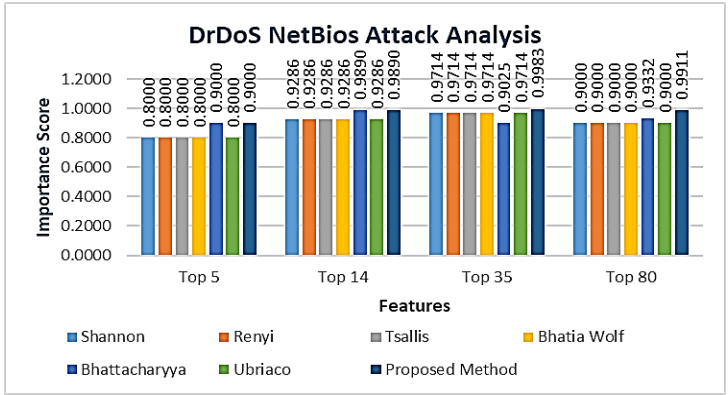

Figure 8. DrDoS NetBios Attack Analysis

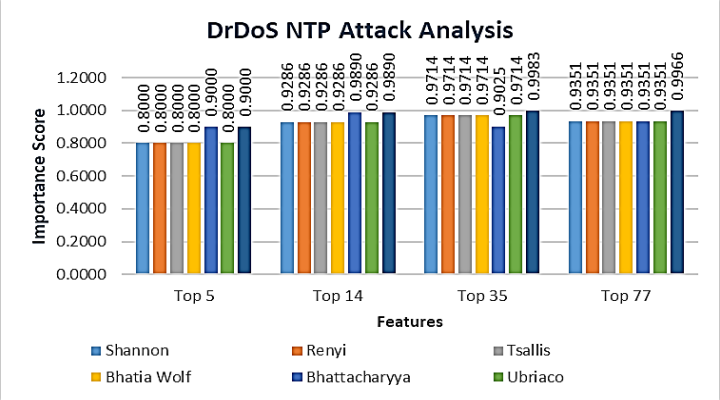

Figure 9. DrDoS NTP Attack Analysis

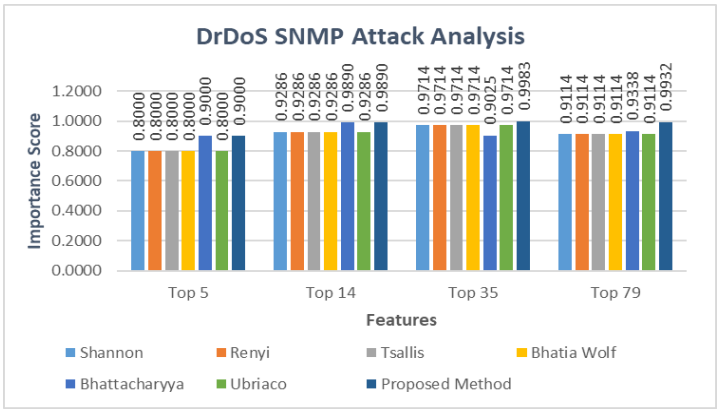

Figure 10. DrDoS SNMP Attack Analysis

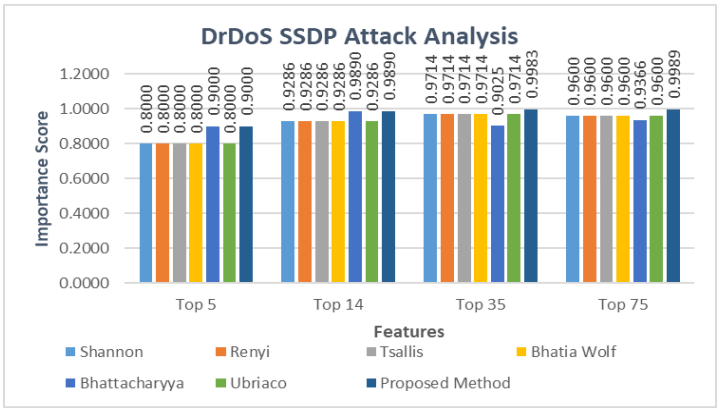

Figure 11. DrDoS SSDP Attack Analysis

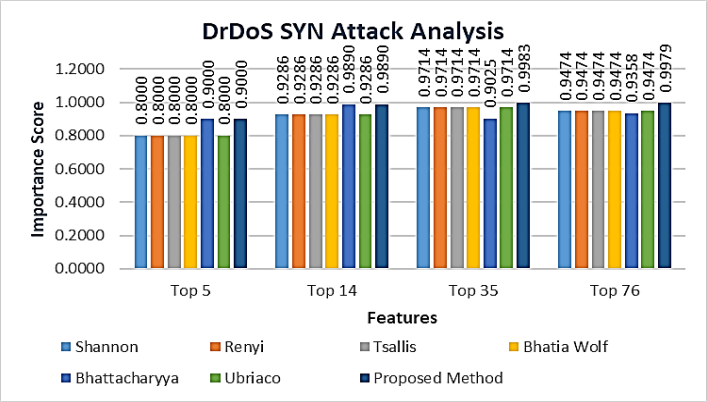

Figure 12. DrDoS SYN Attack Analysis

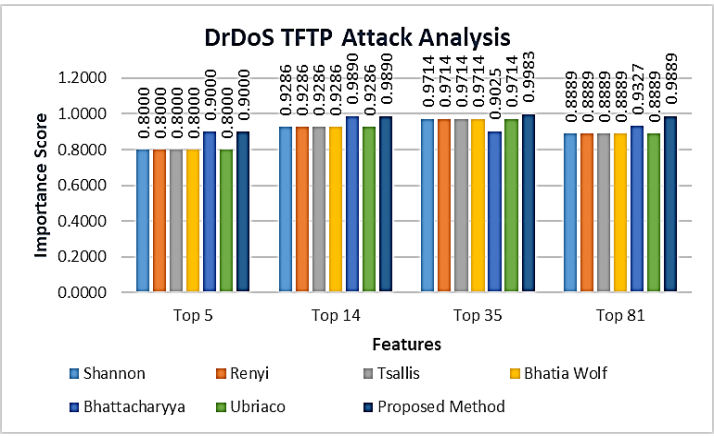

Figure 13. DrDoS TFTP Attack Analysis

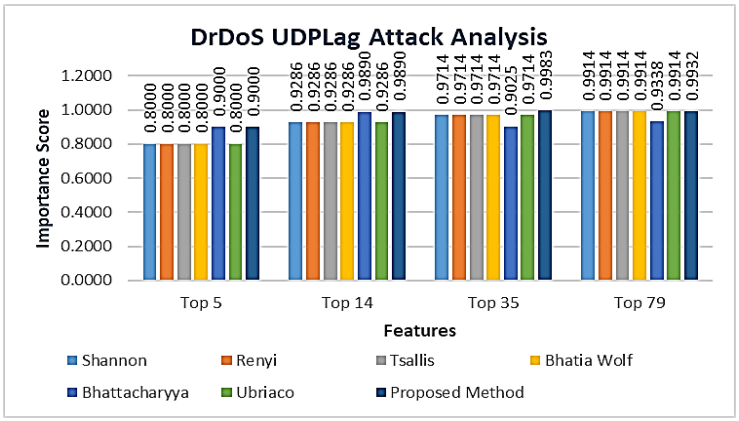

Figure 14. DrDoS UDPLag Attack Analysis

V. CONCLUSION AND FUTURE DIRECTION

The graph analysis for DDoS attack detection indicates that the initial five features score highly in terms of feature importance, approximately 0.99. When the feature set is expanded from 14 to 35, the importance score increases, yet it diminishes as it approaches the total possible features. This reduction is attributed to the inclusion of features with very low mutual information scores, negatively affecting the method's efficiency. Therefore, the selection of appropriate packet data is essential for the effective identification of DDoS attacks, ensuring a balance between comprehensive detection and computational efficiency. In future research, these optimally selected features could be integrated into machine learning models to assess their practical applicability and efficiency.

REFERENCES

[1] Peng, T., Leckie, C., & Ramamohanarao, K. (2007). “Survey of network-based defense mechanisms countering the DoS and DDoS problems”. ACM Computing Surveys, 39(1)

[2] Bhatia, S., Behal, S., & Ahmed, I. (2018). “Distributed Denial of Service Attacks and Defense Mechanisms: Current Landscape and Future Directions” In Advances in Information Security (Vol. 72, pp. 55–97). Springer New York LLC.

[3] D’Cruze, H., Wang, P., Sbeit, R. O., & Ray, A. (2018). “A software-defined networking (SDN) approach to mitigating DDoS attacks”. Advances in Intelligent Systems and Computing, 558, 141–145.

[4] Eustis, A.G. (2019). “The Mirai Botnet and the Importance of IoT Device Security”. In: Latifi, S. (eds) 16th International Conference on Information Technology-New Generations (ITNG 2019). Advances in Intelligent Systems and Computing, vol 800. Springer, Cham.

[5] Mohammadi, R., Javidan, R., & Conti, M. (2017). “SLICOTS: An SDN-based lightweight countermeasure for TCP SYN flooding attacks”. IEEE Transactions on Network and Service Management, 14(2), 487–497.

[6] Alshamrani, A., Chowdhary, A., Pisharody, S., Lu, D., & Huang, D. “A defense system for defeating DDoS attacks in SDN based networks”. MobiWac 2017 - Proceedings of the 15th ACM International Symposium on Mobility Management and Wireless Access, Co-Located with MSWiM 2017, 83–92.

[7] Bawany, N. Z., Shamsi, J. A., & Salah, K. (2017). “DDoS Attack Detection and Mitigation Using SDN: Methods, Practices, and Solutions”. Arabian Journal for Science and Engineering, 42(2), 425–441.

[8] Swami, R., Dave, M., & Ranga, V. (2021). “Detection and Analysis of TCP-SYN DDoS Attack in Software-Defined Networking”. Wireless Personal Communications, 118(4), 2295–2317.

[9] Batool, S., Zeeshan Khan, F., Qaiser Ali Shah, S., Ahmed, M., Alroobaea, R., Baqasah, A. M., Ali, I., & Ahsan Raza, M. “Lightweight Statistical Approach towards TCP SYN Flood DDoS Attack Detection and Mitigation in SDN Environment”. Security and Communication Networks, 2022.

[10] Cil, A. E., Yildiz, K., & Buldu, A. (2021). “Detection of DDoS attacks with feed forward based deep neural network model”. Expert Systems with Applications, 169.

[11] Zheng, J., Li, Q., Gu, G., Cao, J., Yau, D. K. Y., & Wu, J. (2018). “Realtime DDoS Defense Using COTS SDN Switches via Adaptive Correlation Analysis”. IEEE Transactions on Information Forensics and Security, 13(7), 1838–1853.

[12] Swami, R., Dave, M., & Ranga, V. (2019). “Software-defined Networking-based DDoS Defense Mechanisms”. ACM Computing Surveys, 52(2).

[13] Wang, P., Yang, L. T., Nie, X., Ren, Z., Li, J., & Kuang, L. (2020). “Data-driven software defined network attack detection: State-of-the-art and perspectives”. Information Sciences, 513, 65–83.

[14] Basicevic and S. Ocovaj, "Application of entropy formulas in detection of denial-of-service attacks," International Journal of Communication Systems, vol. 32, no. 15, 2019

[15] Bhushan, K., & Gupta, B. B. (2019). “Distributed denial of service (DDoS) attack mitigation in software defined network (SDN)-based cloud computing environment”. Journal of Ambient Intelligence and Humanized Computing, 10(5), 1985–1997.

[16] Balarezo, J. F., Wang, S., Chavez, K. G., Al-Hourani, A., & Kandeepan, S. (2022). “A survey on DoS/DDoS attacks mathematical modelling for traditional, SDN and virtual networks”. Engineering Science and Technology, an International Journal, 31.

[17] Dimolianis, M., Pavlidis, A., & Maglaris, V. (2021). “Signature-based traffic classification and mitigation for ddos attacks using programmable network data planes”. IEEE Access, 9, 113061–113076.

[18] David, J., & Thomas, C. (2015). “DDoS attack detection using fast entropy approach on flow-based network traffic”. Procedia Computer Science, 50, 30–36.

[19] Arivudainambi, D., Varun, V. K., & Sibi Chakkaravarthy, S. (2019). “LION IDS: A meta-heuristics approach to detect DDoS attacks against Software-Defined Networks”. Neural Computing and Applications, 31(5), 1491–1501.

[20] Banitalebi Dehkordi, A., Soltanaghaei, M. R., & Boroujeni, F. Z. (2021). “The DDoS attacks detection through machine learning and statistical methods in SDN”. Journal of Supercomputing, 77(3), 2383–2415.

[21] Jiao, R., Nguyen, B. H., Xue, B., & Zhang, M. (2023). “A Survey on Evolutionary Multiobjective Feature Selection in Classification: Approaches, Applications, and Challenges”. IEEE Transactions on Evolutionary Computation.

[22] Khan, S., Gani, A., Wahab, A. W. A., & Singh, P. K. (2018). “Feature Selection of Denial-of-Service Attacks Using Entropy and Granular Computing”. Arabian Journal for Science and Engineering, 43(2), 499–508.

[23] Shukla, A. S., & Maurya, R. (2018). “Entropy-Based Anomaly Detection in a Network”. Wireless Personal Communications, 99(4), 1487–1501.

[24] Rochak Swami, Mayank Dave, & Virender Ranga. (2019). “Defending DDoS against Software Defined Networks using Entropy”. 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU).

[25] Ramprasath, J., & Seethalakshmi, V. (2021). “Mitigation of Malicious Flooding in Software Defined Networks Using Dynamic Access Control List”. Wireless Personal Communications, 121(1), 107–125.

[26] Basicevic, I., Ocovaj, S., & Popovic, M. (2015). “Use of Tsallis entropy in detection of SYN flood DoS attacks”. Security and Communication Networks, 8(18), 3634–3640.

[27] Ahalawat, A., Babu, K. S., Turuk, A. K., & Patel, S. “A low-rate DDoS detection and mitigation for SDN using Renyi Entropy with Packet Drop”, Journal of Information Security and Applications, 68,2022

[28] Iman Sharafaldin, A. H. L. (2019). “Developing Realistic Distributed Denial of Service (DDoS) Attack Dataset and Taxonomy”. International Carnahan Conference on Security Technology (ICCST).