Detecting DDoS Attacks in SDN: A Survey

Arafat Alawi Al-Hawshabi [1,*]
Belal Al-Fuhaidi [1,*]

[1] Computer Science Department, University of Science and Technology, Sana'a, Yemen
* Corresponding authors: arafatalawi8@gmail.com, belalarh@gmail.com, belalarh@ust.edu.ye

https://doi.org/10.59222/ustjet.4.1.3

Detecting DDoS Attacks in SDN: A Survey

Abstract:

Software-Defined Networking (SDN), despite enabling centralized control and dynamic programmability, exposes critical security vulnerabilities particularly to Distributed Denial-of-Service (DDoS) threats targeting centralized controllers. This review synthesizes recent detection methods, including entropy-driven statistical models, machine learning-based classifiers, and hybrid techniques integrating both approaches. Entropy-based methods are computationally lightweight but often yield high incorrect detections during peak traffic bursts. Pure ML approaches, while highly accurate, struggle with hardware demands incompatible with legacy SDN infrastructure. Hybrid models significantly improve detection robustness; however, they face practical implementation hurdles related to complexity and scalability. While pure ML approaches excel in deep feature extraction, their substantial hardware demands often surpass what most real-world SDN environments can accommodate.

Keywords: network cybersecurity, SDN, DDoS, information entropy, attack detection.

https://doi.org/10.59222/ustjet.4.1.3

اكتشاف هجمات رفض الخدمة في الشبكات المعرفة برمجيا

الملخص:

على الرغم من أنّ الشبكات المُعرَّفة بالبرمجيات (SDN) تمكّن من التحكم المركزي والبرمجة الديناميكية، فإنها تكشف عن ثغرات أمنية حرجة، ولا سيّما أمام هجمات حجب الخدمة الموزّعة (DDoS) التي تستهدف المتحكمات المركزية. تجمع هذه المراجعة أحدث أساليب الكشف، بما في ذلك النماذج الإحصائية المعتمدة على الإنتروبي، والمصنّفات المبنية على التعلّم الآلي، والأساليب الهجينة التي تدمج المنهجين معا. تعدّ الطرق المعتمدة على الإنتروبي خفيفة حسابيا، لكنها غالبا ما تنتج معدلات مرتفعة من الاكتشافات الخاطئة أثناء طفرات حركة المرور عند الذروة. أمّا الأساليب الخالصة للتعلّم الآلي على الرغم من دقتها العالية فتواجه صعوبات بسبب متطلبات العتاد التي لا تتوافق مع بُنى SDN القديمة. وتُحسّن النماذج الهجينة متانة الكشف بشكل ملحوظ؛ غير أنها تواجه تحديات عملية في التنفيذ تتعلق بالتعقيد وقابلية التوسّع. وعلى الرغم من تفوّق الأساليب الخالصة للتعلّم الآلي في استخلاص السمات العميقة، فإن متطلباتها الكبيرة من العتاد تتجاوز في كثير من الأحيان ما يمكن لبيئات SDN الواقعية استيعابه.

الكلمات المفتاحية : أمن الشبكات، الشبكات المعرفة برمجيا، الإنتروبي، هجمات رفض الخدمة.

1. Introduction

The architecture of Software-Defined Networking (SDN) separates control logic from data forwarding, granting network administrators unprecedented flexibility in managing and reconfiguring traffic flows. At its core, SDN centralizes decision-making through a controller that communicates with distributed switches enabling dynamic updates to routing policies in response to network conditions. Yet, this very centralization creates a critical vulnerability: the controller becomes a strategic bottleneck, susceptible to Distributed Denial-of-Service (DDoS) attacks that can flood it with malicious traffic or spurious control requests.

Over the past decade, researchers have proposed a wide array of DDoS detection mechanisms tailored for SDN. Early solutions favoured statistical or entropy-based metrics for their low computational cost, but these models often suffer from elevated incorrect detections during periods of traffic volatility. More recent work has turned to machine learning (ML) to exploit deeper patterns in traffic behaviour. However, ML models typically require significant computational resources and often fail to generalize across varying SDN topologies and deployment environments. A third class of solutions hybrid models combine entropy features with ML classifiers, aiming to harness the strengths of both paradigms. Hybrid detection models offer measurable gains in accuracy, yet they frequently overlook critical infrastructure disparities within real-world SDN environments. This disconnect between theoretical performance and practical feasibility continues to hinder their widespread deployment.

This paper conducts a critical survey of these detection strategies, evaluating their effectiveness, limitations, and suitability for deployment in realistic SDN environments. The analysis draws on metrics such as detection accuracy, false positive rate, latency tolerance, and hardware dependencies, offering insight into which techniques are most viable for contemporary SDN networks.

The rest of this paper is organized as follows: Section 2 provides essential background information on SDN architecture. Section 3 categorizes and reviews the main detection techniques, including statistical, entropy-based, and machine learning methods. Section 4 highlights critical challenges and identifies research areas that remain open. Finally, Section 5 concludes by summarizing the key findings and suggesting directions for future research in SDN security.

https://doi.org/10.59222/ustjet.4.1.3

2. Background of Software-Defined Networking

Software-Defined Networking (SDN) redefines traditional network architecture by decoupling the control plane from the data plane. Rather than embedding decision-making logic into individual devices, SDN centralizes control within a software-based controller. This design relegates routers and switches to forwarding roles, while the controller maintains a global view of the network, issuing flow rules to enforce policies and manage traffic dynamically.

The decoupled architecture enables a high degree of programmability. Administrators can orchestrate traffic flows in real time, automate service provisioning, and implement consistent policy enforcement across heterogeneous environments. These capabilities are particularly valuable in cloud data centres, software-defined WANs, and enterprise networks where agility and scalability are essential. SDN also supports fine-grained Quality of Service (QoS) mechanisms and allows for rapid reconfiguration in response to faults or load imbalances.

At the heart of SDN's programmability is the communication between the controller and the underlying hardware. This controller-switch interaction is facilitated by southbound interfaces, the most prominent of which is OpenFlow. OpenFlow provides a standardized protocol for manipulating flow tables on switches, using instructions such as FLOW_MOD to install rules and PACKET_IN messages to alert the controller about unmatched traffic. The abstraction offered by OpenFlow simplifies control logic development and enhances interoperability across hardware from different vendors.

By isolating decision-making from forwarding, SDN lays the foundation for network automation, adaptive traffic engineering, and robust security policy enforcement. These structural changes not only increase operational efficiency but also create new opportunities and challenges for detecting and mitigating threats like Distributed Denial-of-Service (DDoS) attacks.

3. Literature Review

In Software-Defined Networking (SDN), the controller plays a pivotal role in managing network behaviour. This centralization, while enabling programmability and global visibility, also creates a single point of failure making it an ideal target for Distributed Denial-of-Service (DDoS) attacks. Unlike traditional networks, SDN's architectural decoupling exposes novel vulnerabilities that legacy security models are ill-equipped to handle.

Recognizing these weaknesses, researchers have moved beyond conventional detection methods, introducing a spectrum of SDN-specific defence mechanisms. Some rely on entropy-based metrics to flag irregularities in traffic patterns, while others blend statistical indicators with machine learning (ML) to adaptively recognize attack signatures. More recent work explores deep learning, time-series decomposition, and elf-tuning thresholds to respond to emerging and low-rate attack variants.

This section critically evaluates the evolution of DDoS detection in SDN across three main lines of inquiry: standalone statistical and entropy-based models, hybrid frameworks combining entropy with ML classifiers, and pure ML-driven systems. Each approach is assessed not only by detection accuracy but also by practical deployment constraints such as resource consumption, adaptability to heterogeneous environments, and compatibility with real-world SDN topologies.

3.1. Statistical and Entropy-Based Detection Approaches

Entropy-based models have long been favored in SDN environments for their lightweight computation and rapid response capabilities. Yet their reliability often declines in real-world conditions, particularly under dynamic traffic patterns and evolving attack types.

To address the limitations of static thresholds, researchers have proposed adaptive statistical mechanisms. Authors [1] employed Interquartile Range (IQR) analysis to detect SYN flood attacks by analyzing packet-in anomalies. Their method achieved up to 100% accuracy in controlled settings but remains untested in heterogeneous or large-scale SDN infrastructures. Similarly, Authors in [2] implemented a real-time entropy-based system capable of adjusting detection thresholds based on live traffic dynamics. Although it reached 94% accuracy in production networks, its performance degraded under multi-vector or stealthy attack scenarios. Researchers in [3] took a probabilistic route, using Chebyshev's inequality to recalibrate detection thresholds during volatile traffic periods, completely eliminating incorrect detections during experimentation though broader validation across datasets is still pending.

Beyond threshold calibration, researchers have explored hybrid entropy mechanisms that combine multiple statistical features. Researchers in [4] integrated Shannon and Rényi entropy to detect low-rate attacks such as Slowloris (52 kbps) in under five milliseconds. Researchers in [5] introduced

https://doi.org/10.59222/ustjet.4.1.3

the MMSA framework, leveraging entropy metrics alongside moving averages to detect TCP SYN floods within three seconds. However, this approach has yet to demonstrate similar efficacy against other DDoS variants. Researchers in [6] addressed false alarm reduction by coupling Rényi joint entropy with an Exponentially Weighted Moving Average (EWMA), yielding a 63% improvement in accuracy over static-threshold models.

At the algorithmic level, more specialized techniques have been explored. authors in applied a Cumulative Sum (CuSum) algorithm to track real-time anomalies, although it incurred a 22% false alarm rate on the CAIDA dataset. Li and Wu [8] developed φ-entropy to improve early detection of high-intensity attacks but faced difficulty detecting low-volume threats. authors in [9] analyzed expected packet size (EPS) deviations, successfully identifying slow-rate attacks; however, its reliance on fixed parameters made it less adaptable to varying traffic baselines.

Entropy-based detection is attractive for its lightweight implementation, but static thresholds are brittle under changing traffic conditions [2, 36]. Recent work shows that using dynamic thresholds can improve robustness compared with fixed cut-offs and reports results from practical SDN testbeds rather than pure simulation [2]. Low-rate and IoT-originated floods remain challenging for purely entropy-based schemes, motivating adaptive or hybrid designs [36, 38, 43].

3.2. Hybrid Entropy and Machine Learning Models

To address the limitations of standalone detection approaches, many researchers have adopted hybrid frameworks that fuse entropy-based analysis with machine learning (ML) classification. These models leverage the rapid anomaly-spotting capabilities of entropy with the pattern generalization strengths of ML algorithms, aiming to enhance detection performance without significantly increasing system overhead. Even though entropy-based detection models provide resource-conscious design benefits, several critical limitations still restrict their widespread practical deployment.

One early line of work explored layered architectures that sequentially combine entropy filters with ML classifiers. For example, authors in [12] designed a two-stage framework in which entropy flagged potential anomalies before forwarding them to a support vector machine (SVM) for validation. This design trimmed processing load by 15% and shortened detection latency by 40%, demonstrating a favorable balance between responsiveness and accuracy.

A similar approach by Zhang et al. [13] introduced a cascaded structure integrating entropy deviation analysis with autoencoder–SVM classification. Although their model reduced incorrect detections by 62%, it introduced an additional 300 ms processing delay at the controller raising concerns about scalability during real-time operation.

Other efforts have sought to broaden entropy's role by incorporating diverse traffic features. Zhou et al. [14], for instance, extracted five entropy-based indicators including IP flow variance and ICMP anomalies and used them to train a Random Forest classifier. While the model delivered an F1 score of 0.99, its memory footprint reached 1.8 GB per controller, limiting its feasibility for deployment in memory-constrained environments. In a different direction, authors in [15] combined Shannon and Rényi entropy measures with a convolutional neural network and stacked autoencoder (CNN–SAE) architecture. Their framework maintained 93% precision under typical loads but suffered a 67% performance drop during high-throughput conditions (>10 Gbps), indicating high sensitivity to bandwidth fluctuations.

Dynamic thresholding has also become a key theme in hybrid system design. Dehkordi et al. [16] proposed a three-tier model incorporating both static and adaptive entropy thresholds feeding into ML classifiers. This approach achieved 99.85% detection accuracy with minimal incorrect detections (0.1%). However, its compatibility was limited to newer OpenFlow versions, excluding the widely used 1.0–1.2 deployments still prevalent in many enterprise networks. Similarly, Researchers in [11] introduced a spatial-temporal detection framework combining cross-entropy analysis at the controller with flow feature learning using a CNN–LSTM pipeline. Despite reaching 99.9% accuracy on the InSDN and Mininet platforms, the model's performance depended on a fixed 5 ms controller-switch latency an assumption that fails in real-world networks, where latency variance often exceeds 20 ms.

Researchers in [17] approached hybridization from a different angle by coupling Principal Component Analysis (PCA) with Rényi entropy. PCA identified statistical deviations, while sustained entropy drops confirmed attack patterns. Their method surpassed alternatives like Shannon and Tsallis entropy in detection accuracy (86.45%) on the InSDN dataset. Yet the increased computational burden posed challenges for implementation on low-capacity SDN switches.

https://doi.org/10.59222/ustjet.4.1.3

Researchers in [18] developed a collaborative detection architecture combining entropy-based anomaly indicators with deep learning classifiers, specifically MLP, CNN, and LSTM for traffic verification. The model, trained on 81 extracted features, achieved a 99.83% detection rate. By leveraging entropy to filter suspicious flows before deep learning processing, the approach minimizes overhead and supports scalable detection in bandwidth-limited or unequal-access SDN setups.

Researchers in [19] implemented a distributed detection and mitigation solution where initial anomaly detection occurs at the edge switch, and final attack confirmation is handled at the controller using CNN-LSTM models informed by entropy and RMSE metrics. The framework achieves 98.5% accuracy while reducing incorrect detections by 87%, demonstrating the value of load-balanced, entropy-guided detection in handling asymmetric SDN topologies.

Hybrid detectors (e.g., entropy for fast screening plus ML for confirmation) show promise, but computational overhead and controller resource limits complicate real SDN deployments [22, 39]. Studies also note that detection logic placed exclusively at the controller can be sensitive to latency/bandwidth overheads, motivating work that shifts features or detection closer to the data plane to reduce reaction time [39, 40].

3.3. Machine Learning and Feature-Based Classifiers

In contrast to entropy-centric or hybrid models, pure machine learning (ML) detection systems aim to leverage feature-driven classification techniques that recognize complex traffic patterns without relying on entropy-based metrics. These models are often praised for their adaptability and high accuracy across various attack types, but they also face considerable challenges when deployed in real-world SDN environments particularly in resource-constrained or legacy infrastructure contexts.

Some recent ML-based detection architectures have shifted toward multi-modal traffic analysis to capture the complex spatiotemporal patterns characteristic of DDoS behaviour. Researchers in [22] proposed the Multi-Dimensional DDoS Classifier (MDDCC), which integrates wavelet-based signal decomposition with 3D convolutional neural networks (3D-CNNs). This architecture effectively models temporal evolution alongside spatial traffic correlations, reaching a detection rate of 99.4% on the CIC-IDS2019 dataset. However, its reliance on high-performance GPUs (≥16 GB memory)

during inference phases presents a serious barrier to adoption in resource-constrained SDN contexts, such as edge deployments or legacy controllers.

A more lightweight alternative was demonstrated by Researchers in [23], who prioritized time-series modelling using a distilled set of 25 features including inter-packet variance, burst entropy, and flow duration irregularity. Their XGBoost-based system maintained ~99% accuracy in binary classifications but underperformed in multi-class tasks, where precision fell to ~70%, particularly in distinguishing volumetric attacks like Memcached amplification from other traffic anomalies.

Adaptive thresholding techniques have also entered the ML toolkit. Researchers [24] designed a Random Forest Regression model trained to forecast traffic threshold shifts in real time, aiming to proactively intercept anomalous bursts. Although promising in simulation, the system faltered during flash-crowd events exceeding 50,000 flows per second, where it triggered 43% more incorrect detections, suggesting limitations in its ability to scale under unpredictable demand surges.

A notable disparity becomes evident when examining the practical implementation hurdles of these models. While Wang's graph-based tracing framework excels at localizing attack origins, it remains incompatible with emerging P4-programmable data planes restricting its utility in stateful SDN environments. Likewise, Sanjeetha's dynamic thresholding approach, though conceptually sound, has yet to demonstrate scalability across production-grade network topologies.

ML detectors often reach high accuracy on benchmarks, yet concept drift and real-time integration are persistent challenges [41, 43]. Recent frameworks and surveys emphasize designing controller-centric pipelines carefully to avoid control-plane bottlenecks and to maintain robustness as traffic evolves [22, 24, 41].

3.4. Entropy-Aware Security for Resource-Constrained or Asymmetric SDNs

Recent work has explored entropy-informed techniques tailored for SDN deployments characterized by limited resources, unequal switch-controller access, or distributed control architectures. These settings pose unique challenges to centralized detection logic due to inconsistent latency, bandwidth bottlenecks, or scalability constraints.

https://doi.org/10.59222/ustjet.4.1.3

Authors in [25] proposed a distributed defence mechanism for multi-controller SDNs that integrates destination IP entropy with Packet Window Initiation (PWI) metrics. Their method facilitates early-stage DDoS detection while balancing load across controllers. In simulated environments, the model outperformed conventional entropy-only approaches, achieving detection rates of up to 95%.

Authors in [26] explored a complementary line of inquiry by embedding entropy feedback into cryptographic adaptation. They combined the XTEA encryption algorithm with a dynamic round-adjustment mechanism, further optimized through Selective Forwarding Ratio (SFR) and Bio-inspired Adaptive Hash Chain (BAHC) techniques. While focused primarily on secure packet transmission, their work underscores the broader utility of entropy-driven feedback in optimizing performance and resilience within non-uniform SDN topologies particularly those with high latency variance or hardware constraints. Table 1 includes a summary for the previous studies.

Table 1: Summary of previous studies

Study	Technique Used	Evaluation Metrics	Advantages	Research Gap
Swami et al. (2023) [1]	IQR-based statistical detection	Accuracy (95–100%)	Low complexity, resource-efficient	Limited scalability in diverse SDN setups
Dinh et al. (2023) [2]	Real-time dynamic entropy model	Accuracy (98%, 94%)	Adapts to traffic changes	Challenges with multi-vector attacks
Joshi et al. (2023) [29]	Adaptive entropy thresholding	Precision, false alert rate	Improves precision with dynamic thresholds	Increased processing load, no mitigation
Conti et al. (2017) [7]	Cumulative Sum (CuSum) algorithm	Accuracy on CAIDA/DARPA	Lightweight, real-time	High false alarms
Tsobdjou et al. (2022) [3]	Entropy + Chebyshev's inequality	Perfect accuracy, 0% false positives	Handles traffic volatility well	Needs broader dataset validation
David and Thomas (2015) [28]	Fast Entropy with trends	CAIDA dataset accuracy	Fast, low computational demand	Only volumetric attacks covered

Study	Technique Used	Evaluation Metrics	Advantages	Research Gap
Zahra et al. (2022) [10]	Statistical entropy thresholds	False positive rate	Self-adjusting mechanism	No attack-type classification
Saharan et al. (2022) [33]	Sliding window + flexible thresholds	Effectiveness on CICDDoS2019	Detects DNS-DrDoS & Portmap	Needs real-time validation
Li and Wu (2020) [8]	φ-entropy technique	Responsiveness benchmarked	Better early-stage detection	Focused only on high-intensity threats
Koay et al. (2019) [30]	Multiple entropy types	Feature detection accuracy	Protocol/packet entropy strong	Limited test with window sizes
Mishra et al. (2021) [32]	Entropy shift monitoring	98.2% detection, 0.04% FP	Lightweight, POX-based	Limited dynamic test scenarios
Li et al. (2007) [31]	Cumulative, time-sensitive entropy	Anomaly detection stability	Persistent anomaly detection	Old dataset usage
Batool et al. (2022) [5]	MMSA (Entropy + moving avg + SD)	3 sec reaction time	Fast, stable controller response	Only SYN flood detection
Zhou et al. (2017) [9]	EPS (Expected Packet Size)	Differentiation effectiveness	Robust to low-rate attacks	Static parameter tuning
Aladaileh et al. (2022) [6]	Rényi + EWMA entropy	Accuracy, false alarm	High responsiveness	Limited cross-validation
Subasi et al. (2021) [35]	Linear regression + entropy	3% false positives	Progression-based accuracy	Needs more adaptive models
Shohani et al. (2021) [34]	Regression + EWMA on flow-table miss	Minimal false alarms	Early detection, real-time	Focus on random-target only

4. Key Challenges and Open Research Issues Related to Securing SDN Environments against DDoS Attacks

Protecting Software-Defined Networking (SDN) infrastructures from Distributed Denial-of-Service (DDoS) threats remains challenging due to inherent design trade-offs and limitations within current detection methods.

https://doi.org/10.59222/ustjet.4.1.3

At the core of SDN's architectural innovation is the centralized controller, whose pivotal role introduces vulnerabilities such as susceptibility to packet-in storms and flow-table flooding both of which can rapidly degrade overall network responsiveness. Traditional detection systems, especially those based on static thresholds or entropy measurements, often struggle to handle unpredictable and heterogeneous traffic conditions, leading to elevated false alarms or failures to identify stealthy, low-rate attacks.

Machine learning (ML)-driven detection methods promise enhanced accuracy by leveraging complex traffic patterns, but these too encounter significant barriers in practical deployment. High computational requirements and dependence on specialized hardware restrict their applicability, particularly within legacy or resource-constrained SDN environments. Additionally, ML systems often exhibit reduced accuracy when faced with previously unseen attack patterns or adversarial input scenarios, further complicating real-world use.

Another critical obstacle in advancing SDN security is the absence of standardized benchmarking datasets and evaluation procedures tailored specifically for SDN scenarios. Without common metrics or universally recognized test environments, objectively comparing the effectiveness of different detection methods remains difficult. Compounding this, large-scale and distributed SDN architectures introduce further complexities due to variable switch-controller latencies and inconsistent inter-controller coordination mechanisms.

Collectively, these challenges underscore an urgent need for detection frameworks that not only perform effectively under varied network conditions but also scale efficiently across diverse topologies. Future research directions should focus on developing lightweight, adaptive models capable of real-time anomaly detection and mitigation, incorporating advanced traffic modelling techniques, programmable data-plane technologies like P4, and systematic evaluation standards that mirror the operational complexity of actual SDN deployments.

5. Conclusion

Software-Defined Networking fundamentally reshapes network management by separating control logic from data-forwarding operations, thus providing administrators with centralized oversight and programmable policy enforcement. While SDN's architectural shift delivers substantial operational

benefits, it simultaneously creates vulnerabilities chief among them, increased exposure to targeted DDoS attacks against the centralized controller.

This review critically examined the existing body of research addressing DDoS detection in SDN environments, categorizing approaches into statistical and entropy-based techniques, hybrid entropy-ML frameworks, purely ML-driven systems, and specialized entropy-aware methods designed for resource-constrained or asymmetric networks. Each category has distinctive strengths: entropy-based solutions offer lightweight operation but falter in dynamic conditions, hybrid systems balance accuracy and computational complexity but face practical integration barriers, and pure ML models excel in detailed pattern recognition yet demand considerable hardware resources. Specialized approaches for uneven-access topologies hold promise, though often lack comprehensive validation in realistic scenarios.

Looking ahead, the field requires detection models that can dynamically adapt to evolving attack patterns, operate under stringent resource constraints, and integrate seamlessly with diverse SDN deployments. Prioritizing advancements in scalable detection architectures, developing robust and representative benchmarking frameworks, and exploiting programmable data-plane capabilities like P4 can significantly enhance SDN's resilience against sophisticated and emerging DDoS threats. Such directions represent essential next steps in bridging the gap between theoretical effectiveness and operational deployment in contemporary SDN infrastructures.

References

[1] M. Swami, R. Tiwari, and A. Kumar, "IQR-based approach for DDoS detection and mitigation in SDN," *Defence Technology*, vol. 25, no. 1, pp. 76–87, 2023, doi: 10.1016/j.dt.2022.10.006.

[2] T. T. M. Dinh, T. D. Nguyen, M. B. Pham, Q. T. Can, and T. T. Nguyen, "DDoS attacks detection using dynamic entropy in software-defined network practical environment," *International Journal of Computer Networks & Communications*, vol. 15, no.3, 2023.

[3] A. M. Tsobdjou, Y. Khamlichi, and S. El Kafhali, "Online entropy-based DDoS flooding attack detection system with dynamic threshold," *IEEE Transactions on Network and Service Management*, vol. 19, no. 1, pp. 34–47, 2022, doi: 10.1109/TNSM.2022.3142254.

[4] R. M. A. Ujjan et al., "Entropy-based features distribution for anti-DDoS model in SDN," *Sustainability*, vol. 13, no. 3, p. 1522, 2021, doi: 10.3390/su13031522.

https://doi.org/10.59222/ustjet.4.1.3

[5] R. Batool, M. A. Khan, and A. Ghafoor, "Lightweight statistical approach towards TCP SYN flood DDoS attack detection and mitigation in SDN environment," *Security and Communication Networks*, vol. 2022, Article 2593672, 2022, doi: 10.1155/2022/2593672.

[6] M. A. Aladaileh et al., "Rényi joint entropy-based dynamic threshold approach to detect DDoS attacks against SDN controller with various traffic rates," *Applied Sciences*, vol. 12, no. 12, p. 6127, 2022, doi: 10.3390/app12126127.

[7] M. Conti, S. Tanimoto, and K. Satoshi, "A comprehensive and effective mechanism for DDoS detection in SDN," in *Proc. IEEE WiMOB*, 2017, pp. 1–8, doi: 10.1109/WiMOB.2017.8115796.

[8] J. Li and B. Wu, "Early detection of DDoS based on φ-entropy in SDN networks," in *Proc. 2020 IEEE 4th Information Technology, Networking, Electronic and Automation Control Conf. (ITNEC)*, 2020, pp. 1–5, doi: 10.1109/ITNEC48623.2020.9084885.

[9] L. Zhou, M. Liao, C. Yuan, and H. Zhang, "Low-rate DDoS attack detection using expectation of packet size," *Security and Communication Networks*, vol. 2017, Article 3691629, 2017, doi:10.1155/2017/3691629.

[10] A. Zahra, S. Khan, and M. Ahmed, "Adaptive entropy thresholding for DDoS detection in SDN," in *Proc. 6th Int. Conf. Signal Processing and Information Security (ICSPIS)*, 2022, pp.1–6, doi:10.1109/ICSPIS54653.2021.9729355.

[11] A. V. Kachavimath and D. G. Narayan, "A hybrid deep learning model with consensus-based feature selection for DDoS attacks detection in SDN," *Procedia Computer Science*, vol. 252, pp. 643–652, 2025, doi: 10.1016/j.procs.2024.12.329.

[12] H. Hu, G. Ahn, and Z. Zhang, "Detecting and mitigating DDoS attacks in software-defined networks with correlation analysis," in *Proc. IEEE GLOBECOM*, 2017, pp. 1–6, doi:10.1109/GLOCOM.2017.8254023.

[13] H. Zhang, X. Chen, Y. Li, and Z. Wang, "Autoencoder-SVM hybrid model for SDN anomaly detection," *Computers & Security*, vol. 117, p. 102604, 2022, doi: 10.1016/j.cose.2022.102604.

[14] L. Zhou, Y. Zhu, Y. Xiang, and T. Zong, "A novel feature-based framework enabling multi-type DDoS attacks detection," *World Wide Web*, vol. 26, no. 1, pp. 163–185, 2023, doi:10.1007/s11280-022-01040-3.

[15] R. M. A. Ujjan et al., "Entropy-based features distribution for anti-DDoS model in SDN," *Sustainability*, vol. 13, no. 3, p. 1522, 2021, doi: 10.3390/su13031522.

[16] M. B. Dehkordi, M. Soltanaghaei, and M. Conti, "The DDoS attacks detection through machine learning and statistical methods in SDN," *The Journal of Supercomputing*, vol. 76, no. 8, pp. 6023–6045, 2020, doi: 10.1007/s11227-020-03323-w.

[17] K. Kanodia, H. Kumar, and S. Patel, "DDoS detection based on PCA and Rényi entropy to secure SDN," *Procedia Computer Science*, vol. 218, pp. 3177–3186, 2024, doi: 10.1016/j.procs.2023.11.354.

[18] D. G. Narayan, W. Heena, and A. Kumar, "A collaborative approach to detecting DDoS attacks in SDN using entropy and deep learning," *Journal of Telecommunications and Information Technology*, vol. 97, no. 3, pp. 79–87, 2024, doi: 10.26636/jtit.2024.3.1609.

[19] R. Sato, T. Ohshima, and T. Kitagawa, "Real-time two-stage detection and mitigation system for DDoS attacks in SDN," *Computer Networks*, vol. 240, p. 110096, 2025, doi: 10.1016/j.comnet.2024.110096.

[20] ONOS Project, "ONOS SDN controller," 2024. [Online]. Available: https://onosproject.org (accessed: 21 Sep. 2025).

[21] Open Networking Foundation, "OpenFlow switch specification," 2023. [Online]. Available: https://opennetworking.org (accessed: 21 Sep. 2025).

[22] X. Wang, Y. Liu, and H. Chen, "Detection and mitigation of DDoS attacks based on multi-dimensional characteristics in SDN," *Scientific Reports,* vol. 14, no. 1, p. 66907, 2024, doi: 10.1038/s41598-024-66907-z.

[23] J. Halladay, T. Doleck, and S. Lemay, "Detection and characterization of DDoS attacks using time-based features," *IEEE Access*, vol. 10, pp. 49 794–49 807, 2022, doi: 10.1109/ACCESS.2022.3172595.

[24] A. K. Sanjeetha, N. Kumar, and P. S. Rao, "Real-time DDoS detection and mitigation in software-defined networks using machine learning techniques," *International Journal of Computing*, vol. 21, no. 3, pp. 76–91, 2022, doi: 10.47839/ijc.21.3.2691.

[25] M. Valizadeh and M. Taghinezhad-Niar, "DDoS attacks detection in multi-controller-based software-defined network," in *Proc. 2022 IEEE 12th Annual Computing and Communication Workshop and Conf. (CCWC)*, 2022, pp. 1–6, doi: 10.1109/CCWC54503.2022.9731368.

[26] N. Shah, A. Mehta, M. Qureshi, and S. Raza, "Adaptive entropy-based lightweight encryption framework for SDN-enabled smart cities," *Transactions on Emerging Telecommunications Technologies*, advance online publication, 2025, doi: 10.1002/ett.5056.

https://doi.org/10.59222/ustjet.4.1.3

[27] G. Baldini and I. Amerini, "Online distributed denial of service intrusion detection based on adaptive sliding window and morphological fractal dimension," *Computer Networks*, vol. 210, p. 108923, 2022, doi: 10.1016/j.comnet.2022.108923.

[28] J. David and M. Thomas, "DDoS attack detection using fast entropy approach on flow-based network traffic," *Procedia Computer Science*, vol. 50, pp. 30–36, 2015, doi: 10.1016/j.procs.2015.04.006.

[29] B. K. Joshi and M. C. Joshi, "Comparative study of dynamic-threshold-based distributed denial-of-service attack detection techniques in software-defined network," *Advances and Applications in Mathematical Sciences*, vol. 22, no. 5, pp. 1013–1023, 2023.

[30] A. Koay, I. Welch, and W. K. G. Seah, "Effectiveness of entropy-based features in high- and low-intensity DDoS attacks detection," in *Advances in Information and Computer Security*, 2019, pp. 196–203, doi: 10.1007/978-3-030-31511-5_16.

[31] L. Li, J. Zhou, and N. Xiao, "DDoS attack detection algorithms based on entropy computing," in *Information and Communications Security*, 2007, pp. 452–466, doi: 10.1007/978-3-540-77048-0_35.

[32] A. Mishra, N. Gupta, and B. B. Gupta, "Defense mechanisms against DDoS attack based on entropy in SDN-cloud using POX controller," *Telecommunication Systems*, vol.77, no.1, pp.47–62, 2021, doi:10.1007/s11235-020-00747-w.

[33] S. Saharan, V. Gupta, N. Vora, and M. Maheshwari, "Detection of distributed denial of service attacks using entropy on sliding window with dynamic threshold," in L. Barolli, A. Poniszewska-Maranda, and H. Enokido, Eds., *Advanced Information Networking and Applications*, 2022, pp. 424–434, doi: 10.1007/978-3-030-99584-3_37.

[34] S. Shohani, R. Javidan, and M. K. Rafsanjani, "Statistical model for early detection of random-target DDoS attacks in software-defined networking," *Wireless Personal Communications*, vol. 121, no. 1, pp. 1–20, 2021, doi: 10.1007/s11277-021-08465-5.

[35] O. Subasi, J. Manzano, and K. Barker, "Denial-of-service attack detection via differential analysis of generalized entropy progressions," arXiv preprint, 2021.

[36] C. 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, 2021, doi: 10.3390/app12010370.

[37] X. Ma and Y. Chen, "DDoS detection method based on chaos analysis of network traffic entropy," *IEEE Communications Letters*, vol. 17, no. 1, pp. 114–117, 2013, doi: 10.1109/LCOMM.2012.110312.122123.

[38] M. A. Aladaileh, M. Anbar, I. H. Hasbullah, Y.-W. Chong, and Y. K. Sanjalawe, "Detection techniques of distributed denial-of-service attacks on software-defined-networking controller–a review," *IEEE Access*, vol. 8, pp. 143985–143995, 2020, doi: 10.1109/ACCESS.2020.3014544.

[39] G. Shang, P. Zhe, X. Bin, H. Aiqun, and R. Kui, "FloodDefender: Protecting data and control plane resources under SDN-aimed DoS attacks," in *Proc. IEEE INFOCOM*, 2017, pp. 1–9.

[40] A. Mayoral, R. Vilalta, R. Muñoz, R. Casellas, and R. Martínez, "SDN orchestration architectures and their integration with cloud computing applications," *Optical Switching and Networking*, vol. 26, pp. 2–13, 2017, doi: 10.1016/j.osn.2017.07.001.

[41] V. Mittal, A. Sharma, and A. Gupta, "Deep learning approaches for detecting DDoS attacks: A systematic review," *Journal of Network and Computer Applications*, vol. 175, p. 102917, 2021, doi: 10.1016/j.jnca.2021.102917.

[42] F. Alanazi, K. Jambi, F. Eassa, M. Khemakhem, A. Basuhail, and K. Alsubhi, "Ensemble deep learning models for mitigating DDoS attack in software-defined network," *Intelligent Automation & Soft Computing*, vol. 33, no. 2, pp. 1–12, 2022, doi: 10.32604/iasc.2022.023456.

[43] Q. Yan, F. R. Yu, Q. Gong, and J. Li, "Software-defined networking (SDN) and distributed denial of service (DDoS) attacks in cloud-computing environments: A survey, some research issues, and challenges," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 1, pp. 602–622, 2015, doi: 10.1109/COMST.2015.2487361.

[44] H. Zhang and X. Chen, "Autoencoder-SVM hybrid model for SDN anomaly detection," *Sensors*, vol. 24, no. 2, pp. 139–154, 2024, doi: 10.3390/s24020139.

https://doi.org/10.59222/ustjet.4.1.3