Adaptive Artificial Intelligence Techniques for DoS and DDoS Attack Detection in Modern Networks

Sujit N. Deshpande[1], Bharati S. Ainapure[2,3]
[1] POST DOCTORAL RESEARCH SCHOLAR, LINCOLN UNIVERSITY COLLEGE, MALAYSIA, India;
[2] Adjunct Research Faculty under the Lincoln Global Postdoctoral Researcher (LGPR) Programme at Lincoln University College, Malaysia;
[3] Professor, Department of Computer Engineering, Vishwakarma University, Pune, India.
Email ID - pdf.sujitdeshpande@lincoln.edu.my, ainapuressa@gmail.com

Abstract: The swift rise of connected systems, cloud technology, and widespread Internet of Things (IoT) infrastructure has led to an increased risk of campaigns of Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks. In fact, modern campaigns include elements of volumetric flooding, protocol abuse, application-layer attacks, and hacking of IoT devices while traditional methods based on rules and signatures have trouble with issues like high dimensional traffic and constant changes of behavior, slow speed of attacks, class imbalance, etc. In this review, the authors analyze the latest studies on DDoS detection methods referring to large databases, machine learning and deep learning systems, federated methods, and feature optimization strategies. The studies analyzed show considerable progress achieved after using novel systems, such as CNN, RNN, and others. The researchers note high effectiveness of using these approaches; however, there are still problems with efficient feature extraction and detection of minority classes. The authors further claim that efficient intrusion detection methods should be designed to be able to adapt to emerging threats.

Keywords: DDoS; DoS; Intrusion Detection; Deep Learning; Feature Selection; Class Imbalance; Concept Drift

Introduction

The quick advancement of systems connected to the Internet, online platforms, and the extensive deployment of the Internet of Things (IoT) have greatly boosted the risk of attacks from denial-of-service (DoS) and distributed denial-of-service (DDoS) surroundings on the part of attackers who take advantage of the weaknesses of misconfigured devices. Researchers indicate that during the first half of 2025, the frequency of DDoS attacks has grown by 41% compared to the same time period of the previous year. According to reports, the peak sizes of attacks have surpassed 2 terabits per second [1]. It is also stated that over 20 million instances of DDoS were warded off in the first quarter of 2025 only, which is a 358% year-over-year increase [2].

Current DDoS attacks employ different attack methods such as volumetric flooding attacks, protocol attacks, and application-level attacks against HTTP/HTTPS applications and APIs. The use of DDoS-as-a-Service platforms and hacked IoT devices has made it easier for the attackers to carry out persistent and

coordinated campaigns against the sectors such as financial services, telecommunications, cloud computing, and industry automation [3]. Some consequences of such attacks include downtime, increased mitigation costs, service unavailability, cascading effects, and loss of users' trust [4]–[8].

Traditional approaches for DDoS detection involve the use of static rules or heuristics, but they are ineffective in dealing with complex data patterns and the corresponding pattern of attack [9]. On the contrary, recent innovations have demonstrated that one can use machine learning models capable of recognizing complex time-changing patterns.

Despite these developments, there exist three consistent challenges in the literature: redundant or irrelevant traffic characteristics resulting in extra computational burden; severe class imbalance that distorts the learning towards benign or dominating attack classes; and concept drift due to the changing nature of attack techniques and network behavior [9], [10]. These challenges lead to the idea of analyzing the recent detection techniques and their missed research opportunities in adapting towards efficient and real-time DDoS detection.

Related work

The literature reviews and assesses recent development in detecting and preventing DDoS attacks. Dataset-based studies created numerous widely accepted benchmarks for DDoS attack and intrusion detection studies. Among others, Sharafaldin et al. designed the CICIDS2017 dataset, which contains normal communication traffic and multiple types of malicious activities like DoS and DDoS attacks as well as web-based attacks, botnets, data theft attacks, and many others. Afterward, they created the CICDDoS2019 dataset, which is specially designed for DDoS attacks detection and classification and contains more than 80 groups of attacks classified as UDP, TCP, HTTP, ICMP, DNS, SSDP, and LDAP attacks. The above-mentioned datasets make comparative analysis possible. However, the researchers pointed out that the use of static benchmark datasets can limit the models' ability to achieve their full potential related to the always-changing network environment.

Machine learning methods show great effectiveness in many cases. For instance, Hirsi et al. utilized supervised machine learning method for DDoS attacks detection and achieved accuracy of 98.97% and false alarm rate of 0.023 using random forest model.

On CICDDoS2019, CNSGA required only 16-dimensional features to detect more than 70% of sample types [14].

Federated and distributed approaches address heterogeneous and privacy-sensitive environments. FedLAD used federated learning for DDoS detection in large-scale SDN and achieved accuracy exceeding 98% on InSDN, CICDDoS2019, and CICDoS2017, with real-time SDN evaluation showing high accuracy and low resource consumption [15]. Belachew et al. evaluated K-NN, random forest, XGBoost, and FFNN on CICIDS2017 and Edge-IIoTset; XGBoost achieved accuracy, precision, recall, and F1-score above 99.997% for binary DDoS detection on Edge-IIoTset and was subsequently deployed at the SDN-IoT edge for live traffic classification [17].

Hybrid and deep learning models have also been explored. GRU-ResCBANet combined residual convolutional feature extraction, convolutional block attention, and GRU-based temporal modelling. On NSL-KDD, UNSW-NB15, and CICIDS2017, it achieved binary classification accuracies of 99.70%, 99.16%, and 99.83%, respectively, while multi-class accuracies were 99.69%, 98.23%, and 99.79% [19]. A packet-

grouping method used online data-flow processing and a lightweight CNN; it reported 99.99% accuracy on CICIDS2017 offline data and 99.86% accuracy with 1.05-second latency in online testing [20]. F-OSFA combined CNN and decision trees for traditional DDoS attacks, few-shot learning with a contractive autoencoder for zero-day attacks, and a signature-based resource usage analyzer. It achieved 99.72% on CICDDoS2019 and 99.96% on CICIDS2017, with zero-day accuracies of 96.77% and 95.98%, respectively [21].

Recent studies increasingly address imbalance, adaptation, and real-time operation. Nigar and Mustafa combined Extra Trees-based feature selection with SMOTE and targeted undersampling; XGBoost and Decision Tree achieved balanced accuracy and F1-scores of up to 99.99% and 99.96%, respectively, on CICIDS2017 [31]. Yang et al. combined enhanced CNN and optimized LightGBM in an Ryu SDN controller and reported 99.98% accuracy, an average response time below one second, and restoration of normal traffic within three seconds in real-network tests [32]. Wei et al. investigated incremental learning for vehicular intrusion detection, while Yang et al. explored drift-adaptive online learning and AutoML for dynamic networking environments [27], [33]. Shafir et al. used normalizing flows and Shapley-based feature selection for unsupervised anomaly detection and reported 0.9951 accuracy on CICIoT-2023 using only normal traffic for training [37].

Table 1. Comparative summary of selected studies

Ref.	Approach	Dataset / Environment	Reported finding
[13]	Random Forest	SDN traffic	98.97% accuracy; FAR 0.023
[14]	CNSGA: causal inference + NSGA-III	Four real-world datasets; CICDDoS2019	16 features detected >70% of sample types
[15]	FedLAD federated learning	InSDN, CICDDoS2019, CICDoS2017	Accuracy >98%; low resource consumption in real-time SDN
[17]	XGBoost and other ML models	CICIDS2017, Edge-IIoTset	XGBoost >99.997% on binary Edge-IIoT set detection
[19]	GRU-ResCBANet	NSL-KDD, UNSW-NB15, CICIDS2017	Binary accuracy up to 99.83%; multi-class up to 99.79%
[20]	Packet grouping + lightweight CNN	CICIDS2017	99.99% offline; 99.86% online with 1.05 s latency
[21]	F-OSFA hybrid ML/DL	CICDDoS2019, CICIDS2017	99.72% and 99.96%; zero-day 96.77% and 95.98%
[31]	Extra Trees + SMOTE/under sampling	CICIDS2017	Balanced accuracy up to 99.99%; F1 up to 99.96%
[32]	En-CNN + OptiLGBM	SDN / Ryu controller	99.98%; <1 s response; normal traffic restored within 3 s

Key Contribution

The literature that has been assessed indicates that the process of identifying DDoS attacks has evolved from analyzing statistics and flow characteristics towards hybrid and deep extraction features, federated learning, techniques to remedy the imbalance problem, methods of online learning, and methods of adaptive security. The survey reveals that the different studies progressed in areas such as feature optimization [14], [35], class imbalance handling [31], [32], and concept drift adaptation [27], [33]. However, very few studies address the three challenges at once. As a result, a conclusion is made regarding the necessity of an adaptive, efficient, and imbalance-aware IDS system that would be able to change according to new attack patterns.

Review Synthesis and Comparative Findings

The mentioned techniques perform well, but there may be variations in tests and goals. Research about datasets can deal with various types of attacks while supervised ML models can classify attacks successfully in the conditions of a specific network. While some architectures get better representation of both spatial and temporal traffic characteristics, federated techniques can solve issues of distributed data and privacy. Feature selection methods eliminate unnecessary information and techniques which deal with imbalance aim to assure detectors detect rare attacks better.

As such, having a high overall accuracy does not inherently solve the problem of the minority class. As noted in the literature, minority classes like SSDP- or LDAP-based attacks in CICDDoS2019 are often wrongly classified [12], [32] and even the sophisticated methods can have reduced sensitivity to rare but devastating attacks [19], [21]. Concept drift is another hurdle because models that were trained in the offline environment on CICIDS2017 or NSL-KDD will not perform as expected in the network that is continually evolving [17], [21]. Incremental learning and drift-aware AutoML can put a dent into this problem, but all the rapidly evolving or hybrid attacks are complicated still [27], [33].

Resource efficiency and real-time deployment are both things that come up again and again. The literature discusses things like lightweight systems, packet grouping, edge deployment, federated learning, and real-time applications of SDN [15], [17], [20], [32]. Still, it is pointed out in the literature that there is still a gap in the field of continuous assessment of the solutions and lack of standardization inhibits further development of scalable DDoS detection systems.

Research Gap

Machine learning and deep learning methods persist in their limitations when it concerns relevant feature extraction. Early statistical methods and flow-level approaches deliver rather coarse-grained representations, without mapping advanced temporal as well as spatial relationships. Newer hybrid and deep feature extraction approaches enhance the process of representation learning but can be accompanied with much reliance on convoluted high-dimensional feature spaces, and the investments can be significant [13], [14], [19]. Optimization-based methods can solve issues with redundant features, yet there are also concerns that they might not work properly, since very fine or low-frequency signals could be eliminated when it comes to detection of new multi-vector DDoS attacks as well as unknown attacks.

Class imbalance is another problem, as some types of attacks as well as benign traffic outnumber others within datasets. Even though adaptive Borderline-SMOTE as well as over- and under-sampling methods have been considered, class detection is still not satisfactory [31], [32]. This means high accuracy of results may be combined with low representation rates of rare attacks [19], [21].

Concept drift brings about changes in time in attack patterns and normal traffic. Static datasets and model predictions that are done offline may no longer work well with novel traffic patterns. Although federated learning gives promise of flexibility in the use of distributed and heterogeneous data sources, installation of real-time drift detection and timely updates of the model is challenging in constrained environments of IoT, SDN, and UAV [27], [28], [33], [36].

Altogether, the paper reveals the critical gap in research that calls for developing a framework for uniformly efficient in terms of volumes of data the newly devised IDS.

Discussions

The research shows a clear evolution in terms of smart and adaptive DDoS detection. Various deep learning techniques, such as CNN, RNN, LSTM, graph, federated, online, and hybrid methods, have shown considerable efficiency. Even so, the studies analyzed in this review have, to a great extent, dealt with the issues of improving the features, the problem of class imbalance, the issue of concept drifting, the maintenance of privacy, or the implementation of real-time detection in isolation. For this reason, it could be concluded that the research presented in this paper stands out as it addresses the issues of feature optimization, awareness of class imbalance, and adaptability to concept drifting united.

This becomes important for such domains as IoT, software-defined networks, UAV systems, and cyber-physical networks, where the existence of heterogeneous traffic and limited resources, as well as the nature of evolving attacks, may influence the long-term efficacy of detection. The results allow affirming that it is important to continue the research aimed at a combination of deep learning techniques for feature extraction and techniques for addressing class imbalance and concept drifting.

Conclusions

Modern DoS/DDoS attacks are becoming more complicated and sophisticated, as well as difficult to detect by means of conventional techniques. The literature review looked at various subjects, including datasets, machine learning and deep learning, as well as federated and hybrid models and strategies for real-time deployment. The studies have found out that ML, DL, online, explainable, federated, hybrid, and imbalance-aware methods are efficient, but the problem of feature efficiency, minority class detection, and drift adaptation continues to exist. Only few studies focus on feature efficiency, class imbalance, and drift adaptation at the same time, while continuous evaluation of DDoS systems in varying traffic conditions is still lacking. Therefore, the proposed study is intended to create an adaptive, resource-aware, and unified DDoS detection system.

References

[1] “Gcore Radar Report Reveals 41% Surge in DDoS Attack Volumes,” Global Cyber Security Network, 2025.

[2] M. Khalil, “DDoS Attack Statistics: How Attacks Are Escalating Worldwide,” DeepStrike, Jun. 24, 2025.

[3] “2025 Global DDoS Threat Report: 12.3M Weapons Tracked,” A10 Networks, Jul. 31, 2025.

[4] M. R. Kadri, A. Abdelli, J. Ben Othman, and L. Mokdad, “Survey and classification of Dos and DDos attack detection and validation approaches for IoT environments,” Internet of Things, vol. 25, p. 101021, Apr. 2024, doi: 10.1016/j.iot.2023.101021.

[5] M. Ouhssini, K. Afdel, M. Akouhar, E. Agherrabi, and A. Abarda, “Advancements in detecting, preventing, and mitigating DDoS attacks in cloud environments: A comprehensive systematic review of state-of-the-art approaches,” Egyptian Informatics Journal, vol. 27, p. 100517, Sep. 2024, doi: 10.1016/j.eij.2024.100517.

[6] M. Gelgi, Y. Guan, S. Arunachala, M. S. S. Rao, and N. Dragoni, “Systematic Literature Review of IoT Botnet DDOS Attacks and Evaluation of Detection Techniques,” Sensors, vol. 24, no. 11, p. 3571, Jan. 2024, doi: 10.3390/s24113571.

[9] A. O. Otiko, E. A. Edim, G. A. Iyang, and E. Oyo-Ita, “A Survey of AI Methods for Detection of DDoS Attacks on Networks,” Advances in Research, vol. 25, no. 5, pp. 256–271, Oct. 2024, doi: 10.9734/air/2024/v25i51159.

[10] X. Fu et al., “Deep learning techniques for DDoS attack detection: Concepts, analyses, challenges, and future directions,” Expert Systems with Applications, vol. 291, p. 128469, Jun. 2025, doi: 10.1016/j.eswa.2025.128469.

[11] I. Sharafaldin, A. Habibi Lashkari, and A. A. Ghorbani, “Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization,” Proceedings of the 4th International Conference on Information Systems Security and Privacy, 2018, doi: 10.5220/0006639801080116.

[12] I. Sharafaldin, A. H. Lashkari, S. Hakak, and A. A. Ghorbani, “Developing Realistic Distributed Denial of Service (DDoS) Attack Dataset and Taxonomy,” 2019 International Carnahan Conference on Security Technology (ICCST), Chennai, India, 2019, pp. 1–8, doi: 10.1109/CCST.2019.8888419.

[13] A. Hirsi, L. Audah, A. Salh, M. A. Alhartomi, and S. Ahmed, “Detecting DDoS Threats Using Supervised Machine Learning for Traffic Classification in Software Defined Networking,” IEEE Access, vol. 12, pp. 166675–166702, Oct. 2024, doi: 10.1109/ACCESS.2024.3486034.

[14] Z. Zeng et al., “Causal Genetic Network Anomaly Detection Method for Imbalanced Data and Information Redundancy,” IEEE Transactions on Network and Service Management, vol. 21, no. 6, pp. 6937–6952, Dec. 2024, doi: 10.1109/TNSM.2024.3455768.

[15] Y. S. N. Fotse, V. K. Tchendji, and M. Velempini, “Federated Learning Based DDoS Attacks Detection in Large Scale Software-Defined Network,” IEEE Transactions on Computers, vol. 74, no. 1, pp. 101–115, Jan. 2025, doi: 10.1109/TC.2024.3474180.

[17] H. M. Belachew, M. Y. Beyene, A. B. Desta, B. T. Alemu, S. S. Musa, and A. J. Muhammed, “Design a Robust DDoS Attack Detection and Mitigation Scheme in SDN-Edge-IoT by Leveraging Machine Learning,” IEEE Access, vol. 13, pp. 10194–10214, Jan. 2025, doi: 10.1109/ACCESS.2025.3526692.

[19] C. Ji, H. Liu, and W. Dai, “Hybrid Model for Network Traffic Anomaly Detection Based on Parallel Two-Stage Feature Fusion,” IEEE Access, vol. 13, pp. 27310–27324, Feb. 2025, doi: 10.1109/ACCESS.2025.3538319.

[20] M. He, X. Zhao, and X. Wang, “An Efficient DDoS Detection Method Based on Packet Grouping via Online Data Flow Processing,” IEEE Transactions on Sustainable Computing, vol. 10, no. 2, pp. 202–216, March-April 2025, doi: 10.1109/TSUSC.2024.3409712.

[21] M. Rashid Minhas et al., “F-OSFA: A Fog Level Generalizable Solution for Zero-Day DDOS Attacks Detection,” IEEE Access, vol. 13, pp. 75157–75170, Apr. 2025, doi: 10.1109/ACCESS.2025.3557822.

[27] L. Wei, J. Yang, H. Jin, J. Cui, J. Li, and D. He, “Sustainable Learning-Based Intrusion Detection System for VANETs,” IEEE Transactions on Intelligent Transportation Systems, vol. 26, no. 7, pp. 10080–10091, July 2025, doi: 10.1109/TITS.2025.3562226.

[31] N. Nigar and R. Mustafa, “Enhanced Intrusion Detection via Hybrid Data Resampling and Feature Optimization,” IEEE Access, vol. 13, pp. 149100–149120, Aug. 2025, doi: 10.1109/ACCESS.2025.3602562.

[32] G. Yang et al., “Real-Time DDoS Attack Detection in SDN Based on En-CNN and OptiLGBM,” IEEE Access, vol. 13, pp. 161453–161471, Sept. 2025, doi: 10.1109/ACCESS.2025.3608205.

[33] L. Yang, S. Naser, A. Shami, S. Muhaidat, L. Ong, and M. Debbah, “Toward Zero Touch Networks: Cross-Layer Automated Security Solutions for 6G Wireless Networks,” IEEE Transactions on Communications, vol. 73, no. 9, pp. 7650–7679, Sept. 2025, doi: 10.1109/TCOMM.2025.3547764.

[35] M. Z. Hussain, Z. M. Hanapi, A. A. Hussain, M. Hussin, and M. I. H. Ninggal, “Hybrid-CNNTree- A Convolutional Neural Network and Decision Tree Fusion Model for Wormhole Attack Detection,” IEEE Access, Oct. 2025, doi: 10.1109/ACCESS.2025.3626225.

[37] L. Shafir, R. Giryes, and A. Wool, “Explainable Anomaly Detection in Network Traffic Using Normalizing Flows,” IEEE Transactions on Networking, Oct. 2025, doi: 10.1109/TON.2025.3617580.