Multidisciplinary Journal of Science Technology Education and Management
Journal homepage: https://www.mjstem.org

Lightweight Machine Learning Models For Smurf DDos Attack Detection In Software-Defined Networks: A Systematic Review

Musa Asmau Mamah[a*], V. O Waziri[a], S. Ahmed[a], Noel M. D[a]

[a]Department of Cyber Security Science, Federal University of Technology Minna, Nigeria

[*]Correspondence: Musa Asmau Mamah (mamahmusa@gmail.com).

Abstract

Lightweight machine learning models are pivotal in detecting Smurf DDoS attacks within software-defined networks (SDNs), offering an adaptive framework to manage unique traffic patterns and protocol-specific challenges. This paper systematically reviews lightweight machine learning models for Smurf DDoS detection in SDNs, analysing studies published between 2014 and 2025 from ScienceDirect, Web of Science, and Google Scholar. The review identifies key methodologies such as supervised learning, feature selection, and distributed detection architectures, emphasising their scalability and real-time applicability. Despite high reported accuracy levels, challenges persist in computational overhead, latency, and the standardisation of datasets. A significant gap is evident in protocol-specific detection approaches, particularly for ICMP-reflective Smurf attacks, which have critical implications for SDN environments. These gaps highlight the need for specialised, protocol-aware machine learning techniques that can seamlessly integrate into SDN frameworks. This study underscores the necessity of addressing existing limitations to enhance detection systems' efficiency and reliability. Interdisciplinary collaboration and innovative research are essential to developing robust solutions that cater to the dynamic and evolving nature of network security threats. Advanced detection models, capable of adapting to diverse conditions, will be instrumental in reinforcing SDN security and mitigating the impact of Smurf DDoS attacks effectively. The findings contribute to the ongoing discourse on leveraging machine learning for intrusion detection, setting the stage for further advancements in the field.

Keywords: Software-defined networks, Smurf ddos attack, Lightweight machine learning, Intrusion detection systems, Network security

1. Introduction

Software-defined networking (SDN) represents a paradigm shift in modern network architecture through the separation of the control plane from the data plane. This architectural decoupling enables centralised control, enhanced programmability, and improved network agility (Hussain et al., 2022). As a result, SDN has gained significant traction in emerging

Received October 27, 2025 Accepted December 31, 2025

technologies such as 5G, cloud computing, and the Internet of Things (IoT), where dynamic traffic management and adaptive policy enforcement are essential (Nawaz et al., 2024). The flexibility and scalability offered by SDN have positioned it as a core enabler in the evolution of next-generation networks, thereby fostering innovations in various digital domains. However, despite these advantages, the centralised nature of SDN introduces inherent security challenges that make it susceptible to a wide range of cyber threats.

Among these threats, Distributed Denial of Service (DDoS) attacks have emerged as a critical concern due to their potential to incapacitate the SDN controller the central component responsible for orchestrating network operations. A particularly destructive variant of DDoS is the Smurf attack, which exploits the Internet Control Message Protocol (ICMP) in conjunction with IP broadcast mechanisms to launch reflective amplification attacks (Ribeiro et al., 2023). Attackers employ IP spoofing to generate excessive traffic volumes, resulting in resource exhaustion of both the controller and forwarding devices and causing severe degradation in network performance (Hasan et al., 2024). These attack strategies highlight the limitations of traditional defense mechanisms in dynamic and centralised network environments such as SDN. Consequently, there is a growing demand for lightweight and intelligent detection approaches that can provide real-time responsiveness and adaptability beyond the capabilities of Intrusion Detection Systems (IDS).

Intrusion Detection Systems (IDS) are security mechanisms designed to monitor network traffic, detect malicious activities, and alert administrators to potential threats. Conventional IDS, particularly those based on static rules, struggle to address such threats in dynamic SDN environments (Sebopelo et al., 2021). Their dependence on predefined signatures and lack of adaptability hinder their effectiveness against evolving and large-scale attacks. In contrast, Machine Learning (ML) techniques have emerged as promising alternatives, capable of learning behavioural patterns from both historical and real-time network traffic (Dina & Manivannan, 2021). These methods support anomaly detection without requiring explicit rule definitions. Many existing ML-based IDS models, such as Decision Trees, Random Forests, Support Vector Machines (SVM), and Artificial Neural Networks (ANN), have demonstrated strong detection capabilities; however, they often impose substantial computational demands, making them less suitable for real-time detection in resource-constrained SDN environments. Their high complexity often leads to significant memory consumption, longer training durations, and latency during detection processes. These limitations reduce their practicality for real-time deployment in SDN architectures. Lightweight ML models offer a more efficient solution, featuring streamlined algorithmic designs, reduced model sizes, and faster processing times. Design techniques such as dimensionality reduction, model pruning, and shallow network architectures help maintain acceptable detection accuracy while minimising computational overhead. These properties enhance suitability for latency-sensitive and resource-constrained SDN deployments. Figure 1 shows the Ngram trends for the present study.

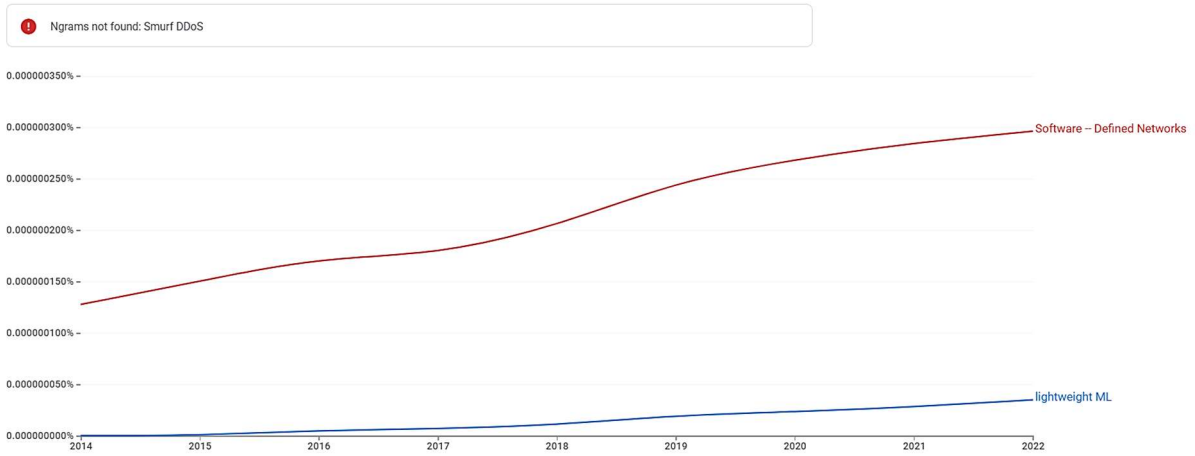

Figure 1: Ngram trends

The observed Ngram trends provide strong justification for the present study. The graph demonstrates a consistent rise in academic interest related to SDNs and a parallel, though more gradual, increase in references to lightweight ML approaches. This trajectory reflects the growing recognition of the need for scalable and resource-efficient security mechanisms in modern network infrastructures. However, the complete absence of the term "Smurf DDoS" from the corpus highlights a critical gap in contemporary scholarly discourse. This lack of attention to Smurf and ICMP-reflective DDoS attacks, despite their relevance as legacy threats with renewed significance in SDN contexts, suggests that these specific attack types have not been adequately explored in recent literature. The omission is particularly significant given that such attacks can exploit SDN vulnerabilities yet are often overshadowed by more generalised or volumetric DDoS categories. Similarly, no standard framework currently exists for comparing lightweight ML techniques specifically aimed at detecting Smurf DDoS attacks within SDN environments. The existing body of research is fragmented, featuring a wide range of datasets, evaluation criteria, and experimental methodologies, which complicates benchmarking and reproducibility.

Accordingly, this systematic literature review addresses the evident gap in current research by conducting a comprehensive analysis of lightweight machine-learning approaches for detecting Smurf and ICMP-reflective DDoS attacks in SDNs. It identifies, synthesises, and evaluates peer-reviewed studies with a focus on balancing detection accuracy and computational efficiency, assessing real-world deployment readiness, and examining the characteristics of datasets employed in existing work. The review aims to uncover prevailing trends, highlight limitations, and outline areas in need of further investigation, thereby contributing to the advancement of robust and efficient SDN security frameworks. Establishing a consistent framework for evaluating lightweight ML models will support researchers and network engineers in designing efficient, scalable, and resilient IDS solutions. These insights are expected to contribute meaningfully to the development of robust SDN security mechanisms against persistent DDoS threats.

1.1 Research Objectives

This systematic review aims to critically examine and synthesise existing research on lightweight machine learning models developed for the detection of Smurf DDoS attacks within SDN environments. Specifically, the study seeks to:

1. Identify and categorise lightweight machine learning models proposed for the detection of Smurf DDoS attacks in SDN environments.
2. Examine the features, datasets, and evaluation metrics commonly employed in these studies.
3. Analyse how the reviewed models achieve a balance between detection accuracy, computational efficiency, and deployment feasibility.
4. Highlight the main limitations, research gaps, and potential directions for future investigation within the existing literature.

2. Methodology

This systematic literature review (SLR) was conducted using a structured and reproducible approach aimed at identifying, evaluating, and synthesising existing research on lightweight machine learning models for Smurf DDoS attack detection in SDNs. The methodology follows the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) guidelines, ensuring transparency, replicability, and academic rigour.

2.1 Information Sources and Search Strategy

A comprehensive and systematic search was conducted across five major academic databases: ScienceDirect, Web of Science, and Google Scholar. The search strategy involved the use of carefully constructed Boolean operators (AND, OR), combining relevant keywords to maximise retrieval of pertinent literature. The primary search string was: ("Smurf attack" OR "Smurf DDoS") AND ("Software Defined Network" OR "SDN") AND ("machine learning" OR "ML") AND ("lightweight" OR "efficient" OR "low complexity") AND ("intrusion detection" OR "attack detection"). Synonyms and alternative phrasings were incorporated where necessary to ensure broad coverage and inclusivity of diverse terminologies used across studies. To enhance the quality and relevance of the results, filters were applied to restrict the search to peer-reviewed articles published in English between January 2015 and 1st June 2025. The search results were exported to Mendeley- Reference Management Software (Version 1.19.8) for deduplication and further screening. The details of the search strategy, including the specific search strings used for each database, were documented to ensure transparency and reproducibility of the systematic review process.

2.2 Inclusion and Exclusion Criteria

The selection of studies for this systematic literature review was guided by a clearly defined set of inclusion and exclusion criteria designed to ensure methodological rigour and thematic

relevance. Studies were included to determine whether they explicitly addressed the detection or mitigation of Smurf attacks or closely related ICMP-based DDoS attacks within SDN environments. Eligible research was further required to employ lightweight or resource-efficient machine-learning techniques. Only peer-reviewed publications, including journal articles, conference papers, and book chapters, were considered. To maintain linguistic consistency and contemporary relevance, only studies published in English between 2015 and 2025 were included.

Exclusion criteria were applied to eliminate studies that did not meet the scope or quality thresholds of the review. Specifically, research focusing solely on general DDoS detection without reference to Smurf or ICMP-based variants was excluded, as were studies relying exclusively on traditional (non-machine learning) methods. Articles that lacked implementation or evaluation in an SDN context were also removed from consideration. Additionally, non-peer-reviewed sources such as whitepapers, theses, technical reports, or blog posts were excluded. These criteria were systematically applied during the screening and eligibility assessment phases to ensure that the final selection comprised only high-quality, contextually relevant studies.

2.3 Study Selection Process

The study selection process followed a structured, multi-stage approach to ensure the relevance and quality of the included literature, encompassing the definition of the study scope and keywords, systematic literature search, critical assessment of selected studies, and the interpretation and synthesis of findings, as illustrated in Figure 2.

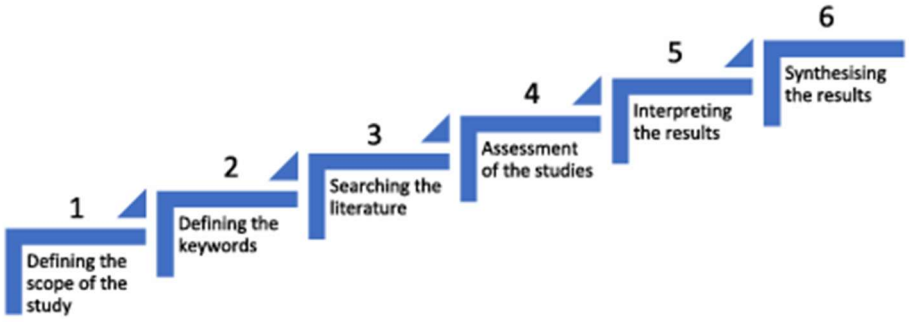

Figure 2: Study Selection Process

Each phase of the selection process was documented using a Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) flow diagram to ensure a strict and organised approach (Mustapha et al., 2024b), as shown in Figure 3.

All studies matching the predefined search criteria were retrieved from the selected digital databases. This initial identification phase was followed by a screening process, during which duplicate records were removed, and the remaining titles and abstracts were reviewed to eliminate clearly irrelevant studies. Full-text articles were assessed in detail to verify their compliance with the established inclusion criteria. The final stage involved the inclusion of studies that satisfied all methodological and thematic quality thresholds for the review.

2.5 Quality Assessment

A structured quality assessment checklist guided the evaluation of methodological rigour and relevance in the selected studies using Microsoft Excel. Key criteria included clarity of research objectives and methodology, justification and suitability of the machine learning models employed, availability of implementation details and datasets, as well as transparency in performance evaluation and reported metrics. Each study received a quality rating of High, Medium, or Low based on these factors (Mustapha et al., 2024a). Studies rated as High (80-100%) clearly articulate their research objectives and methodology, provide appropriate justification for the selection of machine learning models, offer sufficient details regarding implementation and datasets, and transparently report performance results with comprehensive metrics. Those classified as Medium (60-79%) generally present clear objectives and methodology but lack adequate detail in one or more areas, such as model justification, availability of datasets, or transparency in performance evaluation. The studies were retained for inclusion in the synthesis and discussion, ensuring that only rigorously conducted and relevant research contributed to the review's findings. Studies assessed as Low (0-59%) exhibit unclear or poorly defined objectives and methodology, provide insufficient or vague information about implementation and datasets, and/or fail to report performance metrics adequately. These studies were excluded from the synthesis and discussion. Table 1 shows the quality assessment criteria.

Table 1: Quality Assessment Criteria

S/N	Study Design and Methodology	ML Model Justification and Suitability	Performance Evaluation and Metrics	Implementation Details and Dataset Availability	Transparency and Reproducibility	Quality of Reporting and Presentation
i.	Clarity of research objectives and alignment with study goals	Relevance and justification for chosen ML model(s)	Appropriateness of evaluation metrics and methods	Availability and accessibility of datasets used	Transparency in methodology and model training process	Clarity and completeness of result presentation
ii.	Robustness of methodological approach	Suitability of ML model for SDN-based Smurf attack detection	Validity and reliability of performance results	Description of implementation process and experimental setup	Reproducibility based on available information	Proper interpretation and discussion of findings
iii.	Validity of data collection and analysis techniques	Innovation or novelty in ML model application	Consideration of computational efficiency and scalability	Documentation of pre-processing, feature selection, etc.	Disclosure of tools, platforms, and hyperparameters	Use of visualisations and structured reporting of results

2.6 Data Extraction and Synthesis

Information from the selected studies was systematically extracted using a structured coding form designed to ensure consistency and completeness. Extracted data included publication metadata (such as authorship, year), specific machine learning algorithms employed, such as decision tree, random forest, support vector machine, and the lightweight strategies applied (such as model pruning and feature selection). Additionally, dataset characteristics and experimental setup details were recorded. The study's accuracy was collected to enable quantitative comparison. The form also captured reported advantages, trade-offs, and limitations to provide a comprehensive view of each approach.

The synthesis of findings employed both quantitative and qualitative methods. Quantitative data were organised into comparative tables to facilitate direct evaluation of model effectiveness and efficiency across studies. Qualitative analysis involves a thematic examination to identify recurring patterns, emerging research trends, and gaps within the current literature. This dual approach allowed for a thorough exploration of each research question and provided a clear overview of the state of lightweight machine learning techniques for Smurf DDoS detection in SDN.

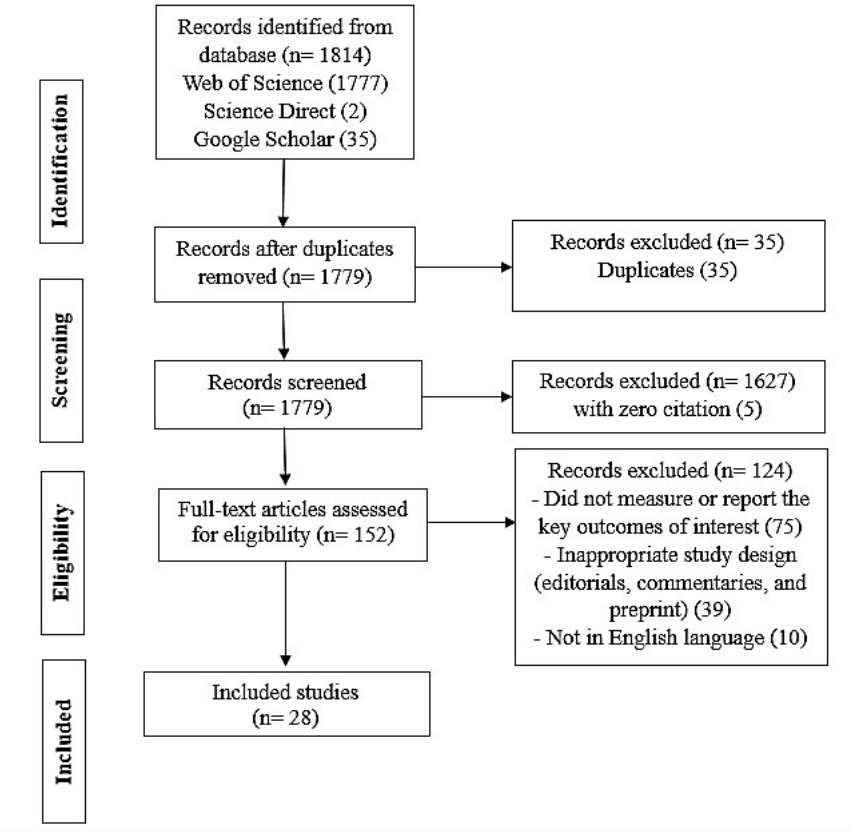

Figure 3: PRISMA flow diagram

The PRISMA flow diagram illustrates the systematic process followed in identifying and selecting studies for inclusion in the review. Initially, 1,814 records were identified through database searches: 1,777 from Web of Science, 2 from Science Direct, and 35 from Google

Scholar. Following the removal of 35 duplicate records, 1,779 unique records were screened. During the screening phase, 1,627 records were excluded, including 5 with zero citations. Of the remaining 152 full-text articles assessed for eligibility, 124 were excluded for various reasons: 75 did not report or measure the key outcomes of interest, 39 had inappropriate study designs such as editorials, commentaries, or preprints, and 10 were not published in English. Ultimately, 28 studies met the inclusion criteria and were incorporated into the final analysis.

3. Results

Recent advances in SDN security research have increasingly focused on machine learning and deep learning techniques for detecting DDoS attacks, demonstrating high accuracy across diverse datasets and architectures. However, significant gaps persist in developing lightweight, protocol-specific detection methods tailored to ICMP-based amplification attacks, such as Smurf floods. Most existing studies prioritise generalised detection capabilities and high accuracy, often relying on computationally intensive models optimised for Transmission Control Protocol (TCP) or application-layer threats while neglecting the unique traffic patterns of ICMP-reflective attacks. Furthermore, many solutions do not adequately evaluate scalability or real-time deployment feasibility in resource-constrained SDN environments, which are common in the Internet of Things (IoT) and edge computing contexts where processing power and memory are limited. This study addresses these critical gaps through a systematic review of lightweight machine learning approaches specifically designed for detecting Smurf and ICMP-reflective DDoS attacks in SDNs. Its contribution lies in providing a focused analysis of efficient, protocol-aware defense mechanisms, which remain underexplored in current research, thereby offering valuable insights toward practical and scalable security solutions for modern SDN deployments. Table 2 shows the summary of the selected studies.

Table 2: Selected Studies

Author(s) (Year)	ML Model	Lightweight Strategy	Dataset Used	Accuracy (%)	SDN Context	Findings	Research Gap / Justification	Journal Quartile
Sendil & Rajagopalan (2024)	Decision Tree (DT)	Fast inference, SDN programmability	Custom SDN dataset	99.9	Ryu controller (real-time SDN)	High accuracy with low FAR; fast execution suitable for real-time use	No focus on specific DDoS types like Smurf or ICMP-reflective	Q2
Kavitha & Ramalakshmi (2024)	ML (unspecified)	Distributed detection in IoT-SDN	Custom dataset	99.99	IoT-SDN multi-controller	Robust detection in IoT-SDN using ML; handles infrastructure layer threats	No protocol-level analysis; not optimised for lightweight constraints	Q2
Hirsi et al. (2024)	Random Forest	Custom dataset, scalable classification	Custom + CICDDoS2019	98.97	Centralised SDN	Accurate traffic classification using Random Forest; new SDN-specific dataset	No Smurf/ICMP-specific focus; lightweight performance not prioritised	Q2
Santos-Neto et al. (2024)	Hybrid ML + entropy	Entropy thresholds via ML	DARPA + real traffic	>99	Mininet + hybrid SDN	ML improves threshold precision; faster convergence vs SVM/RF	Still computationally intensive; lacks protocol-targeted detection	Q2
Kapourchali et al. (2024)	ML (unspecified)	In-switch (P4) detection	Custom P4 traffic	Not available	P4-based SDN	Reduced controller CPU overhead and detection delay with in-switch ML	Focuses on HTTP slow rate, not Smurf or ICMP-reflective attacks	Q1
Gadallah et al., (2024)	AE-BGRU (DL)	Layered feature selection	Custom dataset	99.91%	SDN control + data planes	DL model detects both control- and data-plane attacks with custom features	Uses heavy DL architecture; no ICMP or Smurf-specific insight	Q1
Yoon & Kim (2024)	Attention (DCA, DL)	Selective attention	Virtual testbed (ONOS)	Outperforms DLs	ONOS + Mininet	Novel DCA model improves detection over existing DL approaches	Does not explore lightweight ML or ICMP-reflective scenarios	Q1

Received October 27, 2025 Accepted December 31, 2025

Ali et al. (2023)	ML/DL (Review)	Comparative analysis	Multiple datasets	Not available	Broad SDN review	Provides taxonomy of ML/DL DDoS strategies in SDN	Does not focus on lightweight or protocol-level threats	Q1
Setitra et al., (2023)	MLP-CNN	SHAP + Bayesian tuning	CICDDoS-2019, InSDN	99.98	SDN controller layer	Strong detection performance; useful SHAP explanations	Model complexity is not ideal for lightweight deployment	Q3
Mohammadi et al. (2023)	ML (unspecified)	Traffic pattern analysis	Custom SDN testbed	Not available	Ryu controller	Detected HTTP flood; reduced bandwidth and forwarding rule load	Focuses on application layer; not relevant to ICMP-based DDoS	Q2
Ko et al. (2023)	Random Forest	Permutation feature selection	Kaggle (84-feature)	99.97	General SDN	High accuracy using top 20 features; reduced complexity	No low-resource or Smurf/ICMP-specific evaluation	Q1
Ma et al. (2023)	Random Forest	Edge-based parallel computing	CICDDoS-2019	99.99	Edge-SDN	Fast and accurate detection using edge CPU	No ICMP/reflective attack distinction; focus on infrastructure	Q1
Bahashwan et al. (2023)	ML/DL/Hybrid (Review)	Literature synthesis	Mixed	Not available	Broad SDN review	Summarised ML/DL trends; highlighted SDN DDoS gaps	No model proposed; Smurf/ICMP-reflective attacks not addressed	Q2
Fu & Zou, (2023)	Decision Tree (C4.5)	Conditional entropy filtering	Custom dataset	High (unspecified)	SDN architecture	Used entropy for pre-classification; improved performance	Lack of evaluation under Smurf or ICMP conditions	N/A
Nawaz et al. (2023)	Deep Neural Network	Feature correlation, epoch tuning	Custom + advanced datasets	99.80	SDN control-data	High accuracy using deep features; good generalisation	Not suitable for real-time or low-resource constraints	N/A
Ussatova et al. (2022)	Various (RF, XGBoost, etc.)	Feature selection + SMOTE	Custom 22-feature	99–100	SDN simulation	Balanced models performed best with	No specific consideration for	N/A

						decision-tree families	Smurf or ICMP-flood detection	
Wang & Wang, (2022)	CNN + ELM	Lightweight DL hybrid	Custom SDN dataset	95.24	Real-time SDN defense	Achieved good latency and detection results using hybrid DL	Doesn't address protocol-level threats (Smurf/ICMP)	Q2
Yungaicela-Naula et al., (2022)	DL + DRL	Flow sampling + modular IPS	Mininet + Apache	98 (IDS), 100 (IPS)	SDN testbed	Detected and mitigated slow-rate DDoS; strong IPS component	Not tested for Smurf/reflective volumetric DDoS	Q1
Wang (2022)	CNN + ELM	Online DL hybrid	Real-time SDN data	High	Centralised SDN	Same as Liping, achieved effective detection	No ICMP or Smurf-specific focus	Q2
Tang et al., (2022)	ML (unspecified)	PF framework (OpenFlow)	Custom LDoS traffic	96.00	LDoS in SDN	Framework mitigated low-rate TCP attacks with low system cost	Not applicable to ICMP or Smurf DDoS types	Q1
Kaur & Gupta, (2022)	Tuned SVM	Six-tuple optimisation	Custom SDN data	98.00	OpenFlow SDN	Good accuracy and tuning; suitable for early detection	No evidence of ICMP pattern detection or lightweight benchmarking	Q3
Cui et al. (2021)	ML + thresholds (Review)	Taxonomy (46 techniques)	Theoretical	Not available	Broad SDN classification	Detailed categorisation of detection techniques	No ICMP or real-time model analysis included	Q1
Ahuja et al. (2021)	Hybrid SVC + RF	Novel SDN-specific features	Custom SDN dataset	98.80	Custom topology	Achieved low FAR with high accuracy	Doesn't address Smurf or ICMP variants	Q1
Karthika & Karmel, (2021)	Deep learning (unspecified)	Unsupervised feature extraction	Simulated Mininet	Not available	DL in SDN	Reviews unsupervised DL in SDN	No concrete evaluation; lacks attack-specific discussion	Q3
Perez-Diaz et al. (2020)	J48, RF, MLP, SVM, among others	Modular detection	CIC DoS dataset	95	ONOS + Mininet	Identified and mitigated LDoS	No link to reflective ICMP-based threats	Q2
Dong & Sarem (2020)	Improved KNN + DDoS degree	Custom classifier logic	Not available	Not available	SDN traffic	Proposed degree-based method for DDoS	Not validated for Smurf/ICMP scenarios	Q2

Polat et al. (2020)	KNN, SVM, NB, ANN	Wrapper feature selection	Custom SDN dataset	98.30	SDN with overloaded controller	KNN + feature selection worked well for accuracy	Doesn't address inference latency or ICMP flood types	Q3
Swami et al. (2019)	Survey (no model)	SDN self-defense discussion	Theoretical	Not available	SDN architecture	General SDN security review	No empirical testing, no D	Q1

3.1 Selected Studies Features

3.1.1 Publication Year Distribution

The analysis of the reviewed literature concerning ML approaches for DDoS detection in SDNs reveals a notable surge in scholarly activity, especially between 2022 and 2024. Among the 28 examined studies, 15 appeared during this period, reflecting an active and evolving research domain. However, specific applications of lightweight ML strategies targeting emerging and protocol-specific DDoS threats, such as Smurf and ICMP-reflective attacks, remain insufficiently explored. This highlights the necessity and timeliness of conducting a focused, systematic review. Figure 4 shows the annual publication.

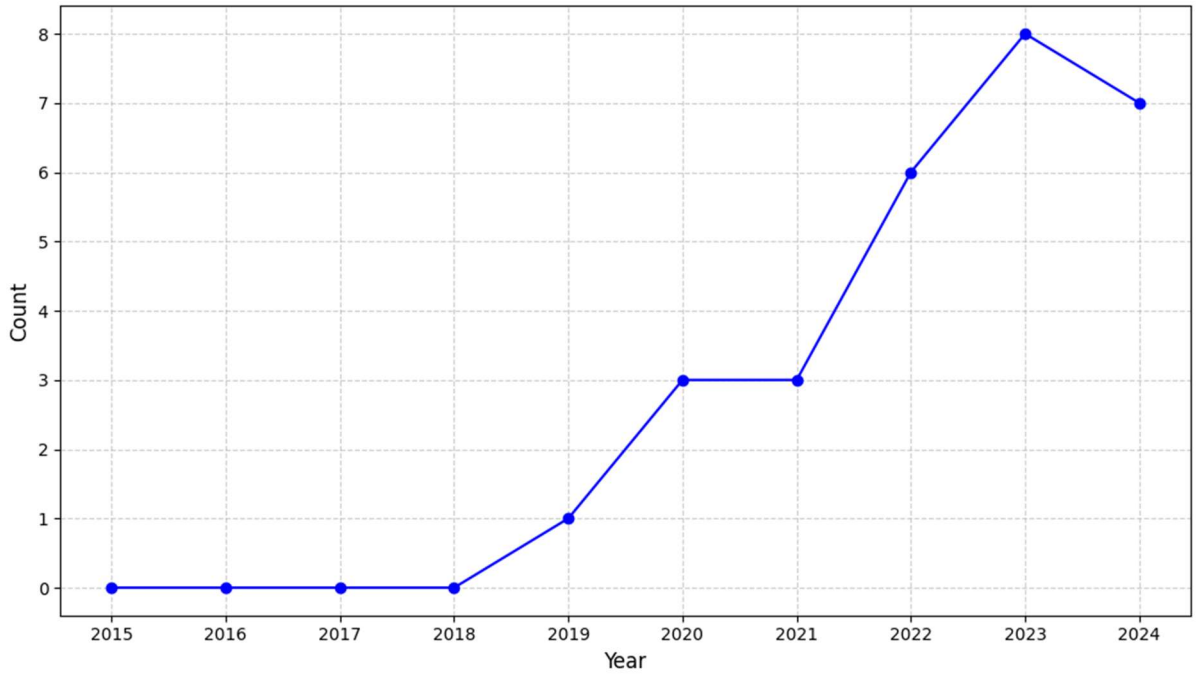

Figure 4: Annual Publication

3.1.2 Machine Learning Model Diversity

Regarding ML model categories, a diverse array emerges. Deep learning methodologies, including Convolutional Neural Networks (CNN) and Autoencoder Bidirectional Gated Recurrent Units (AE-BGRU), appear most frequently, featured in six studies. Random Forest and Decision Tree algorithms also demonstrate significant prevalence. Nonetheless, five studies employed generalised or unspecified ML models, and three were survey or review articles without proposing novel models. Such heterogeneity indicates a lack of consensus and standardised methodologies, particularly in relation to lightweight models optimised for the constraints inherent in SDN environments and reflective DDoS attack detection. Figure 5 shows ML model diversity.

Received October 27, 2025 Accepted December 31, 2025

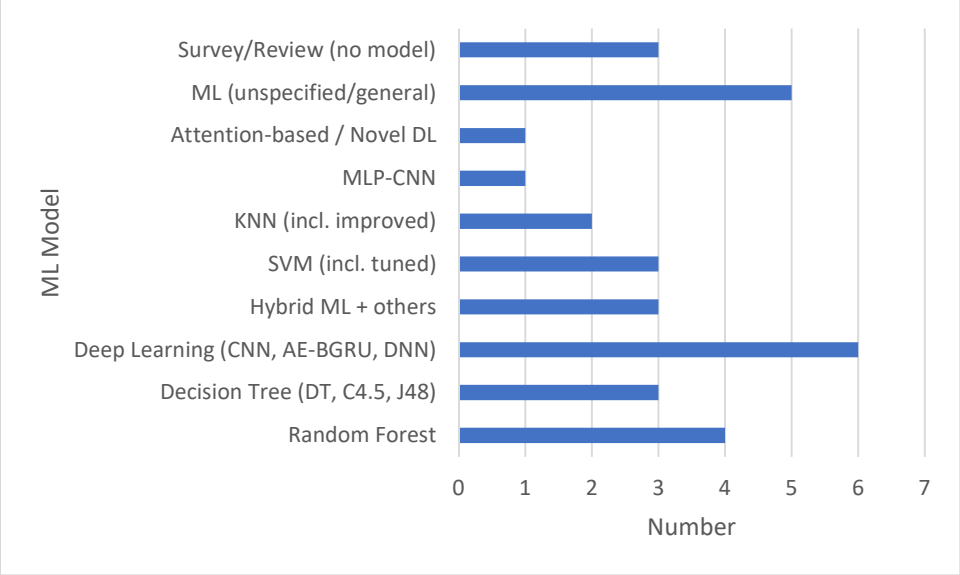

Figure 5: Machine Learning Model Diversity

3.1.3 Adoption of Lightweight Strategies

In terms of lightweight strategies, a minority of studies explicitly implemented feature selection techniques, fast inference mechanisms, or distributed in-switch detection. Thirteen out of 28 studies neither specified nor applied any dedicated lightweight strategy. This gap underscores the ongoing challenge of balancing computational efficiency and detection performance, which represents a critical requirement for real-time deployment within resource-constrained SDN architectures. Figure 6 shows the lightweight strategy.

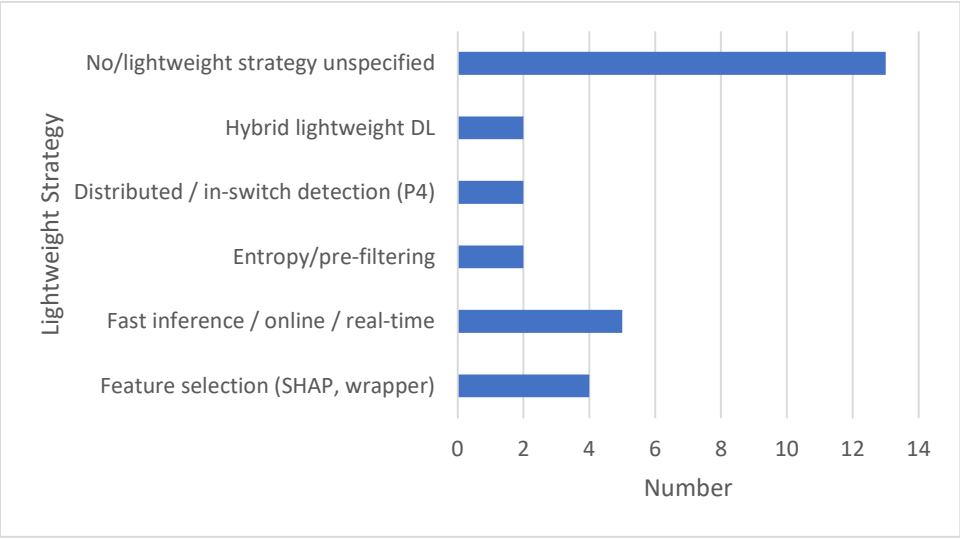

Figure 6: Lightweight Strategy

3.1.4 Dataset Variability and Standardisation Issues

Datasets used across the studies exhibit considerable variability. Custom datasets predominate, appearing in 13 papers, followed by established benchmarks such as CICDDoS and virtual

testbeds like Mininet. The diversity and fragmentation of datasets complicate direct comparison and benchmarking efforts. Additionally, most studies did not focus explicitly on Smurf or ICMP-reflective DDoS attack datasets, indicating a pressing demand for more targeted and standardised data resources. Figure 7 shows the dataset used.

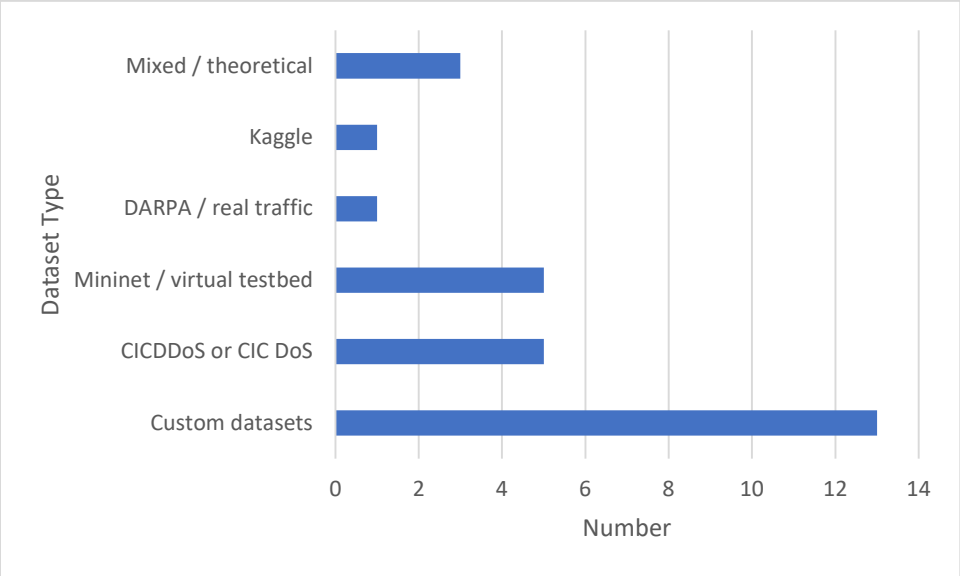

Figure 7: Dataset Used

3.1.5 Accuracy Reporting and Evaluation Consistency

The reported accuracy metrics are generally high, with over one-third of the studies achieving detection accuracies equal to or exceeding 99%. Nonetheless, eight studies lacked accuracy values, reflecting inconsistencies in evaluation reporting. This variability hinders comprehensive assessment of trade-offs between accuracy and computational complexity, a crucial consideration for the practical adoption of lightweight ML models within SDN contexts. Figure 8 shows the accuracy level.

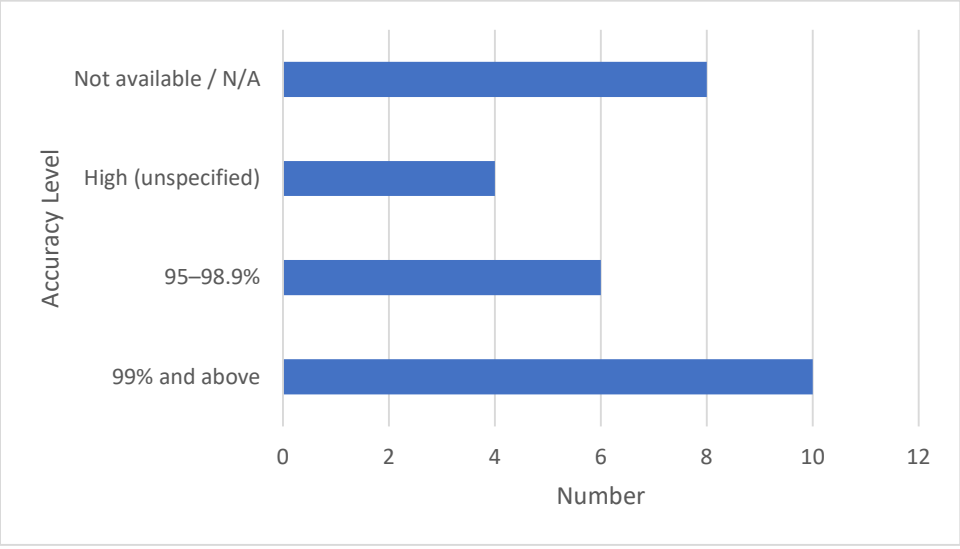

Figure 8: Accuracy Level

3.1.6 SDN Deployment Contexts

Regarding SDN operational environments, the majority of studies concentrated on centralised controller architectures such as Ryu and ONOS (12 studies), with fewer investigations into distributed or in-switch detection paradigms. Given the architectural vulnerability of SDN controllers against volumetric DDoS attacks, including Smurf variants, exploring lightweight detection mechanisms deployed at multiple network points remains imperative. Figure 9 shows the SND deployment context.

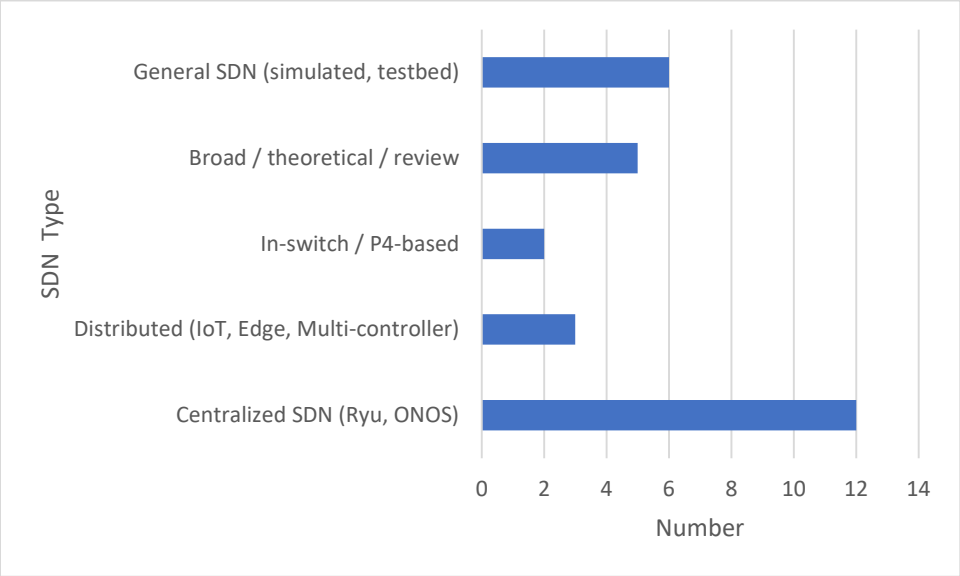

Figure 9: SDN Deployment Context

3.1.7. Quality and Dissemination of Research

Journal quartile distribution reveals that most studies published in the first and second quartile (Q1 and Q2) journals reflect high-quality research. Nevertheless, this observation also indicates an ongoing need for rigorous investigation and wider dissemination of findings, especially concerning lightweight ML models and protocol-specific attack types. Figure 10 shows the journal quartile.

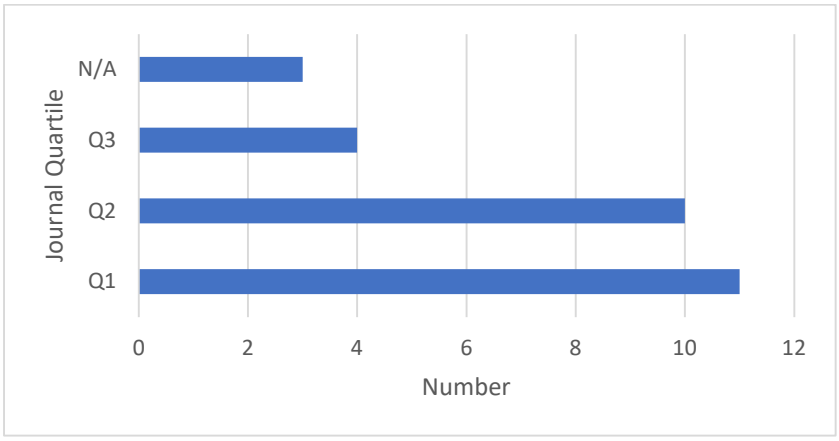

Figure 10: Journal Quartile

3.1.8 Identified Research Gaps and Limitations

A critical analysis of the reviewed literature reveals notable research gaps that substantiate the need for targeted investigation. Specifically, the detection of Smurf and ICMP-reflective DDoS attacks remains markedly underexplored, with 14 studies explicitly acknowledging this limitation. Furthermore, eight studies report inadequate consideration of lightweight or resource-constrained implementations, which are an essential requirement for real-time deployment in SDN environments. Additional limitations include the absence of protocol-specific analysis and evaluations concerning detection latency, both of which are pivotal for assessing the operational viability of proposed models. Although detection accuracy is consistently prioritised across studies, comparatively few investigations examine aspects such as real-time performance, hybrid model optimisation, or enhancements in controller efficiency. This disproportionate focus suggests that practical deployment challenges related to computational overhead and system responsiveness remain insufficiently addressed. These observed deficiencies underscore the necessity of a systematic review centered on lightweight machine learning techniques explicitly designed for the detection of Smurf and ICMP-reflective DDoS attacks within SDN architectures. Figure 11 shows the research gaps/ limitations.

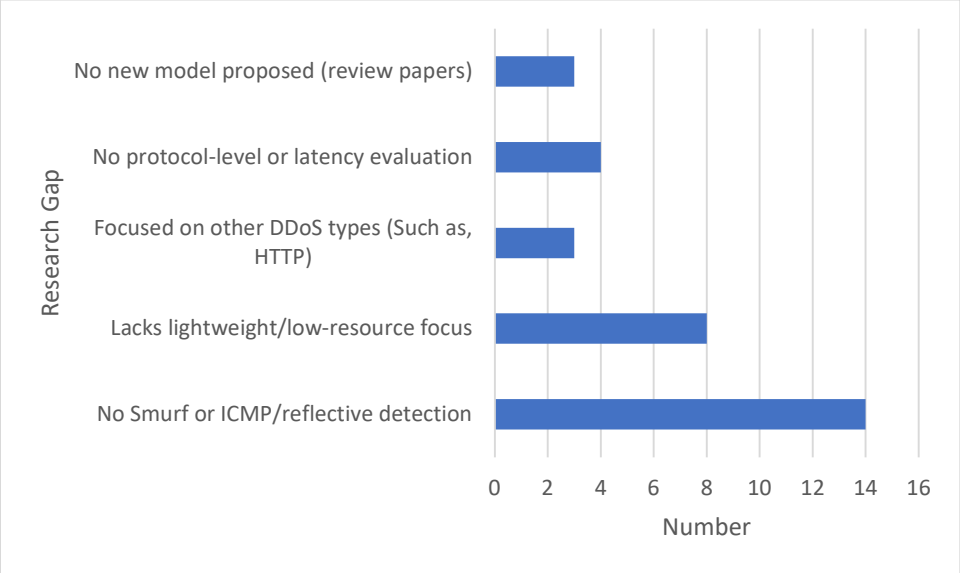

Figure 11: Research Gaps / Limitations

3.2 Research Objective 1: Proposed lightweight machine learning models for detecting Smurf DDoS attacks in SDN environments

The existing body of literature reveals a significant gap in the development of ML models explicitly designed for the detection of Smurf DDoS attacks within SDN environments. Numerous studies have proposed ML-based methods for detecting general DDoS threats. However, none of the reviewed works directly address the distinctive characteristics of Smurf attacks, particularly the exploitation of ICMP echo requests sent to broadcast addresses using spoofed source IPs to achieve amplification and network disruption (CERT, 1998).

Nonetheless, certain ML approaches exhibit indirect relevance through their focus on low-rate or reflective attack behaviours. Notably, models that emphasise protocol-layer traffic features or analyse temporal anomalies such as packet inter-arrival time variations and irregular control plane utilisation may be inherently capable of identifying Smurf-type activity, even if not explicitly validated for this use case. For instance, decision tree-based classifiers presented by Sendil & Rajagopalan (2024) and Ussatova et al. (2022) and in-switch detection frameworks utilising programmable data planes, such as those proposed by Kapourchali et al. (2024), show promise in this regard. Figure 12 illustrates the conceptual differences between Smurf attacks and other volumetric or low-rate DDoS methods in SDN topologies. In the Smurf scenario, an attacker transmits ICMP echo requests to a network's broadcast address while spoofing the victim's IP address. As a result, all hosts on the network reply to the spoofed IP, creating a significant amplification effect. In contrast, traditional volumetric DDoS attacks, such as TCP/UDP floods, typically originate directly from malicious hosts and target either the SDN controller or data plane devices without leveraging broadcast mechanisms.

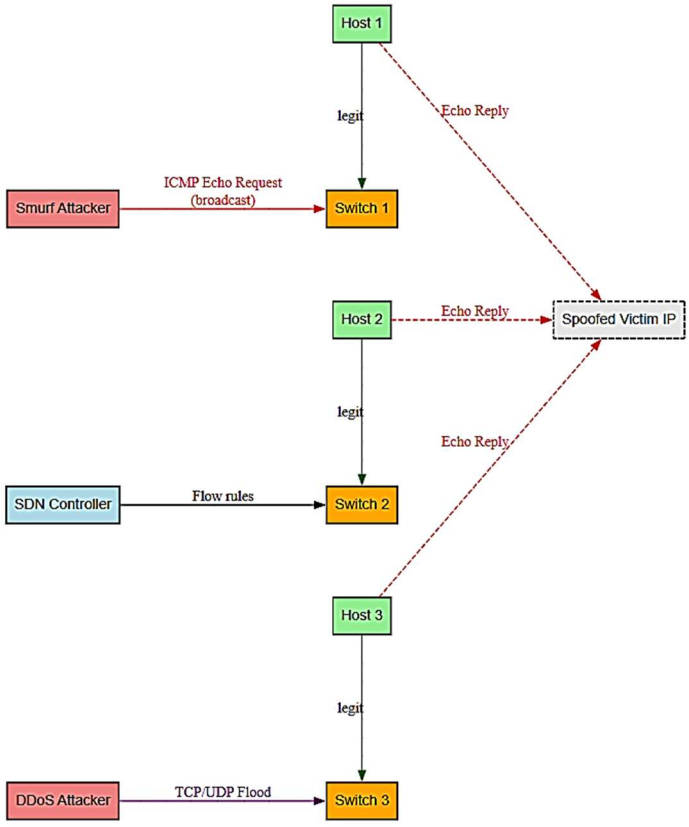

Figure 12: Smurf Attack vs Other DDoS in SDN Topology

The conceptual diagram illustrates the flow of legitimate and malicious traffic within SDN topology, emphasising how Smurf and other DDoS attacks exploit network components. The layout follows a left-to-right structure, beginning with three hosts, Host 1, Host 2, and Host 3, each connected respectively to Switch 1, Switch 2, and Switch 3 via legitimate green-labeled paths. These switches represent the data plane; a central SDN controller connects to Switch 2, issuing control instructions that govern traffic handling across the network. A Smurf attacker sends an ICMP Echo Request with a spoofed victim IP address to Switch 1, targeting the

broadcast domain. As a result, all three hosts reply with ICMP Echo Replies, which are forwarded toward the spoofed victim IP, producing an amplification effect characteristic of Smurf attacks. These reply paths are marked with red dashed arrows, showing how benign hosts unwittingly contribute to overwhelming the victim.

Conversely, a DDoS attacker on the right initiates a TCP/UDP volumetric flood directed specifically at Switch 3, simulating traditional resource-exhaustion attacks. This distinction helps highlight the protocol-level differences between reflective Smurf attacks and direct-volume attacks. The SDN controller's involvement in governing Switch 2 through OpenFlow rules underscores the centralised control capabilities and vulnerabilities of SDN architecture. This visual distinction reinforces the need for lightweight and protocol-aware detection mechanisms in SDN environments to address both reflective and volumetric DDoS threats effectively.

3.3 Research Objective 2: Features, datasets, and evaluation metrics are commonly used in these studies

The reviewed studies consistently prioritise traffic features that reflect control-plane activity and flow-level behaviours. Commonly used input features include packet size, destination IP entropy, packet inter-arrival time, flow duration, and protocol type. A few studies, such as those by Fu & Zou, (2023) and Gadallah et al. (2024), introduce additional features specific to SDN environments, including switch-buffer size, unknown destination rates, and custom transport layer headers.

Regarding feature selection, methods such as Information Gain, F-test, and Chi-square statistics are widely employed to reduce dimensionality and improve model interpretability. Feature importance analysis, particularly via SHAP or permutation-based methods, has also been applied in recent works such as Ko et al. (2023) and Setitra et al. (2023).

In terms of datasets, the CICDDoS2019 dataset is the most frequently utilised benchmark across empirical evaluations. A limited number of studies generate custom datasets using SDN emulation platforms such as Mininet or ONOS (Ma et al., 2023; Sendil Vadivu & Rajagopalan, 2024). However, none of the examined datasets include synthetic or real Smurf-type attacks, which restricts the applicability of conclusions regarding ICMP-reflective detection.

Evaluation metrics predominantly include classification accuracy, precision, recall, and F1-score. A smaller number of studies also report inference time, false alarm rate, and system resource consumption, especially those asserting lightweight characteristics. Figure 13 shows the heatmap illustrating metric performance distribution across the reviewed literature. (1 = reported, 0 = not reported)

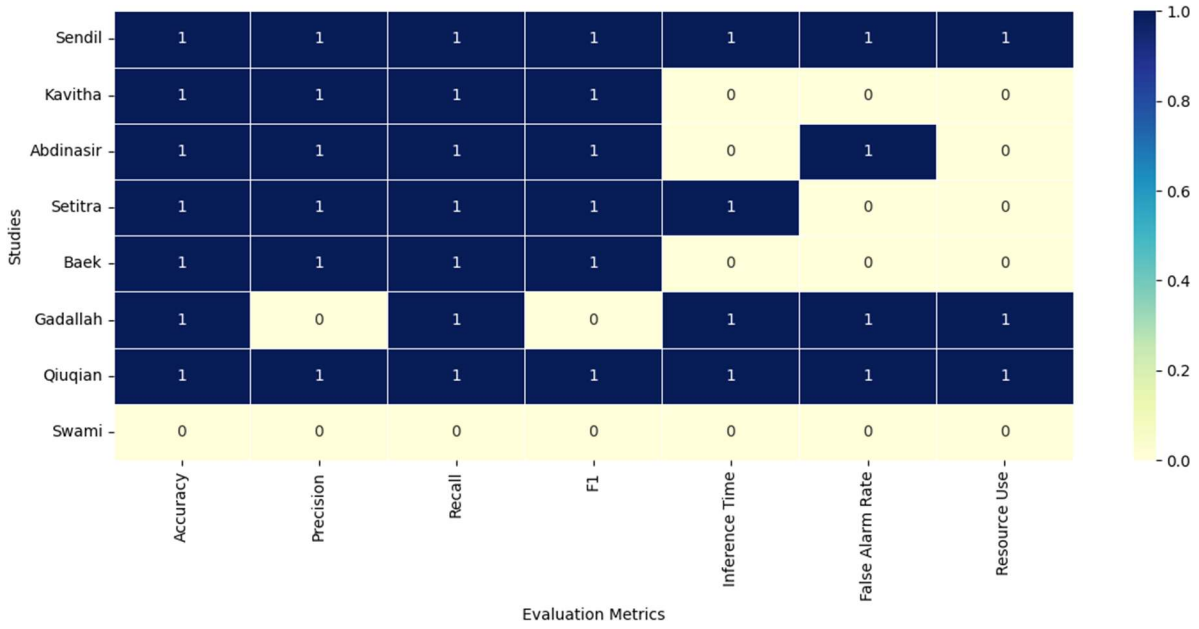

Figure 13: heatmap illustrating metric performance distribution across the reviewed literature

3.4 Research Objective 3: Reviewed models balance detection accuracy with computational efficiency and deployment feasibility.

High classification accuracy is consistently reported across studies, with many models achieving performance above 98 percent. However, claims regarding computational efficiency and real-time feasibility are less frequently substantiated. Only a limited number of studies report explicit metrics on inference time or controller resource utilisation. For example, the work by Ma et al., (2023) indicate that their edge-deployed model achieved predictions within 0.4 seconds. The study by Kapourchali et al., (2024) reports significant reductions in bandwidth and CPU consumption due to the use of P4-based in-switch detection. Although these efforts indicate progress, most studies still employ deep learning architectures (such as DNNs or GRU-based models) that inherently involve significant computational overhead. These include the AE-BGRU model by Gadallah et al. (2024) and the attention-based DCA model by Yoon & Kim, (2024), both of which prioritise detection capability over lightweight performance.

Models that utilise shallow classifiers, including decision trees and random forests, tend to provide better alignment with lightweight deployment objectives (Ko et al., 2023; Sendil & Rajagopalan, 2024). However, systematic trade-off analyses comparing detection performance with inference time or memory footprint are largely absent across the reviewed literature. The Figure shows scatterplot mapping models by accuracy versus efficiency (such as inference time or computational cost), which would substantially enhance understanding in this section. This helps distinguish high-performing lightweight models from deep models requiring substantial resources (Figure 14).

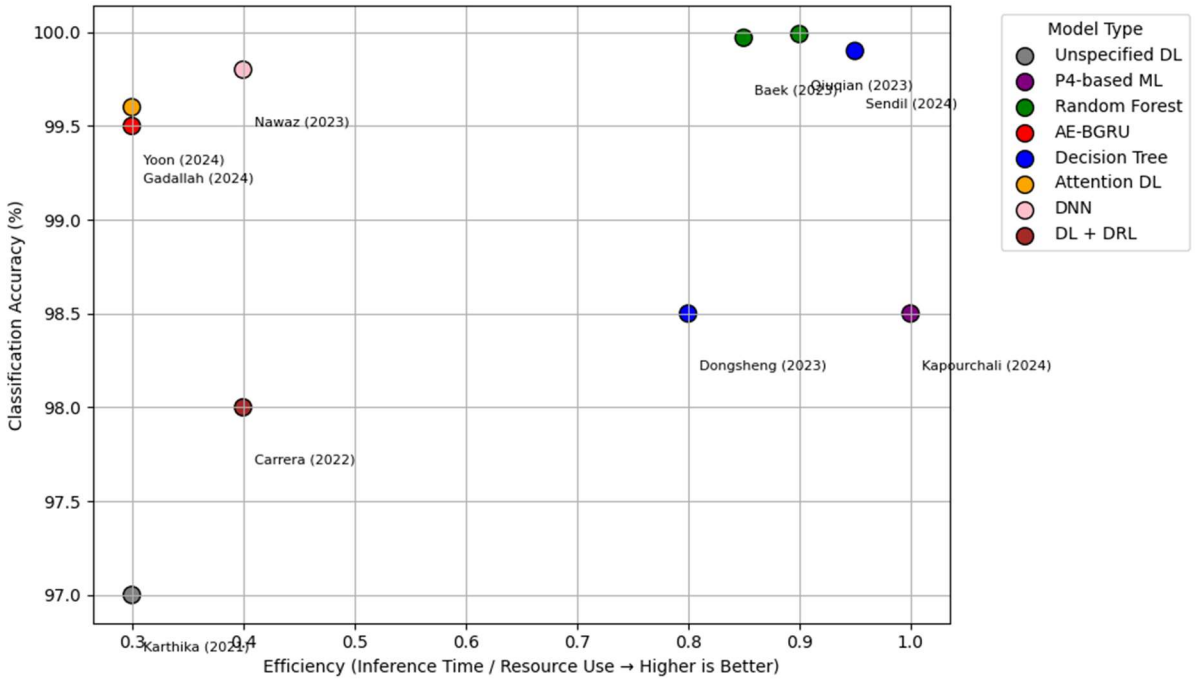

Figure 14: Accuracy vs Efficiency of SDN DDoS Detection Models

3.5 Research Objective 4: Main limitations, gaps, and future opportunities identified in the literature

Multiple limitations are recurrent across the reviewed studies. First, there is a critical lack of research explicitly targeting Smurf or ICMP-reflective DDoS detection in SDN environments. Although some models demonstrate a technical capacity for low-rate detection, the absence of protocol-specific evaluation restricts their applicability to this class of attacks. Second, no standardised benchmarking framework exists for assessing the lightweight nature of proposed models. Although some studies claim real-time capability, many omit key metrics such as memory usage, CPU load, and power efficiency, which are particularly relevant for edge- or controller-level deployment in SDN. Third, the generalizability of most reviewed models remains limited due to the overreliance on a small number of datasets. Many studies use CICDDoS2019 or generate isolated synthetic data without modeling realistic SDN traffic scenarios, reflective amplification, or complex mixed-attack strategies. Fourth, there is an underutilisation of adaptive or reinforcement learning techniques that could provide continuous learning in dynamic SDN environments. Only one study incorporates deep reinforcement learning for slow-rate DDoS mitigation (Yungaicela-Naula et al., 2022).

Figure 15 shows a conceptual roadmap that outlines these research gaps and maps them to potential future opportunities that would clarify this section's implications for both researchers and practitioners.

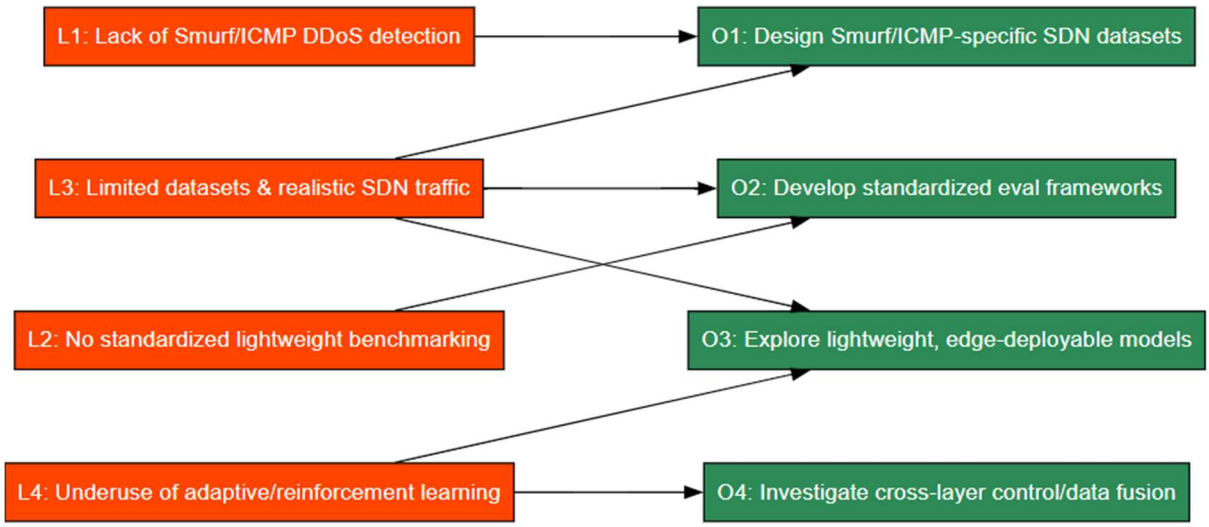

Figure 15: Conceptual roadmap

4. Conclusions and Future Work

This systematic review demonstrates that substantial advancements have been made in the application of machine learning techniques for DDoS detection in SDNs; however, the specific detection of Smurf and ICMP-reflective attacks remains significantly underrepresented in current literature. Lightweight models such as decision trees, Naive Bayes, and optimised ensemble methods exhibit considerable potential, particularly when integrated with feature selection techniques and hybrid architectures. Despite this progress, the adoption of these models in practical SDN environments is constrained by limitations, including inadequate data availability, the absence of protocol-specific datasets, insufficient benchmarking of lightweight strategies, and minimal attention to deployment metrics such as inference latency and controller resource consumption. Standardised evaluation frameworks capable of supporting meaningful cross-study comparisons are also lacking, which hampers the development of scalable and deployable solutions. Addressing these challenges requires focused research on ICMP-specific datasets, unified performance evaluation protocols, and the design of adaptive, resource-efficient detection systems that can operate effectively within dynamic SDN contexts. Such advancements will significantly strengthen the ability of SDN infrastructures to detect and mitigate Smurf-type threats.

Future work should therefore focus on:

1. Designing Smurf/ICMP-specific datasets that accurately simulate reflective attacks within SDN topologies.
2. Developing standardised evaluation frameworks that balance detection accuracy with runtime efficiency and deployment feasibility.
3. Exploring lightweight, incremental, or edge-deployable learning models to accommodate real-time detection needs.

4. Investigating cross-layer data fusion that leverages both control and data plane metrics for enhanced detection fidelity.

Conflict of Interest

The authors do not have conflict of intrest.

Author Contributions

Musa Asmau Mamah: Conceptualization, Methodology, Data curation, Formal analysis, Investigation, Writing – original draft. **V. O. Waziri**: Conceptualization, Supervision, Validation, Writing – review & editing. **S. Ahmed**: Methodology, Data curation, Investigation, Writing – review & editing. **Noel M. D**: Investigation, Visualization, Synthesis of findings, Writing – review & editing.

Funding

No funding received for this study.

Acknowledgments

The authors sincerely acknowledge all researchers whose articles were selected and analysed in this study. Their scholarly contributions provided the foundation for this systematic review and significantly enriched the insights presented. The authors also appreciate the support and academic environment provided by the Department of Cyber Security Science, Federal University of Technology, Minna, Nigeria.

Ethical Statements

This study relied solely on previously published literature and did not involve human participants or animals; therefore, ethical approval was not required.

Data and Code Availability

All data used in this study were obtained from publicly available sources, and no new datasets or custom code were generated during the course of the research.

References

Ahuja, N., Singal, G., Mukhopadhyay, D., & Kumar, N. (2021). Automated DDOS attack detection in software defined networking. *Journal of Network and Computer Applications*, *187*. https://doi.org/10.1016/j.jnca.2021.103108

Ali, T. E., Chong, Y. W., & Manickam, S. (2023). Machine Learning Techniques to Detect a DDoS Attack in SDN: A Systematic Review. *Applied Sciences (Switzerland)*, *13*(5). https://doi.org/10.3390/app13053183

Bahashwan, A. A., Anbar, M., Manickam, S., Al-Amiedy, T. A., Aladaileh, M. A., & Hasbullah, I. H. (2023). A Systematic Literature Review on Machine Learning and Deep

Learning Approaches for Detecting DDoS Attacks in Software-Defined Networking. *Sensors*, *23*(9). https://doi.org/10.3390/s23094441

Cui, Y., Qian, Q., Guo, C., Shen, G., Tian, Y., Xing, H., & Yan, L. (2021). Towards DDoS detection mechanisms in Software-Defined Networking. *Journal of Network and Computer Applications*, *190*, 103156. https://doi.org/10.1016/j.jnca.2021.103156

Dina, A. S., & Manivannan, D. (2021). Intrusion detection based on Machine Learning techniques in computer networks. *Internet of Things (Netherlands)*, *16*. https://doi.org/10.1016/j.iot.2021.100462

Dong, S., & Sarem, M. (2020). DDoS Attack Detection Method Based on Improved KNN with the Degree of DDoS Attack in Software-Defined Networks. *IEEE Access*, *8*, 5039–5048. https://doi.org/10.1109/ACCESS.2019.2963077

Fu, Y., & Zou, D. (2023). A DDoS attack detection method based on conditional entropy and decision tree in SDN. *Chongqing Daxue Xuebao/Journal of Chongqing University*, *46*(7), 1–8. https://doi.org/10.11835/j.issn.1000.582X.2023.07.001

Gadallah, W. G., Ibrahim, H. M., & Omar, N. M. (2024). A deep learning technique to detect distributed denial of service attacks in software-defined networks. *Computers and Security*, *137*. https://doi.org/10.1016/j.cose.2023.103588

Hasan, A., Iqbal, T., Naseer, M., Sarwar, N., Ali, A., & Shabir, M. (2024). Advanced Detection and Mitigation of Smurf Attacks Using AI and SDN. *2024 International Conference on Decision Aid Sciences and Applications, DASA 2024*. https://doi.org/10.1109/DASA63652.2024.10836590

Hirsi, A., Audah, L., Salh, A., Alhartomi, M. A., & Ahmed, S. (2024). Detecting DDoS Threats using Supervised Machine Learning for Traffic Classification in Software Defined Networking. *IEEE Access*, *12*, 166675–166702. https://doi.org/10.1109/ACCESS.2024.3486034

Hussain, M., Shah, N., Amin, R., Alshamrani, S. S., Alotaibi, A., & Raza, S. M. (2022). Software-Defined Networking: Categories, Analysis, and Future Directions. *Sensors*, *22*(15). https://doi.org/10.3390/s22155551

Kapourchali, R. F., Mohammadi, R., & Nassiri, M. (2024). P4httpGuard: detection and prevention of slow-rate DDoS attacks using machine learning techniques in P4 switch. *Cluster Computing*, *27*(6), 8047–8064. https://doi.org/10.1007/s10586-024-04407-5

Karthika, P., & Karmel, A. (2021). Analysis of Different Attacks on Software Defined Network and Approaches to Mitigate using Intelligent Techniques. *International Journal of Advanced Computer Science and Applications*, *12*(9), 338–348. https://doi.org/10.14569/IJACSA.2021.0120938

Kaur, G., & Gupta, P. (2022). A robust tuned classifier-based distributed denial of service attacks detection for quality of service enhancement in software-defined network. *Journal of Intelligent and Fuzzy Systems*, *43*(3), 2693–2710. https://doi.org/10.3233/JIFS-212946

Kavitha, D., & Ramalakshmi, R. (2024). Machine learning-based DDOS attack detection and mitigation in SDNs for IoT environments. *Journal of the Franklin Institute*, *361*(17). https://doi.org/10.1016/j.jfranklin.2024.107197

Ko, K. M., Baek, J. M., Seo, B. S., & Lee, W. B. (2023). Comparative Study of AI-Enabled DDoS Detection Technologies in SDN. *Applied Sciences (Switzerland)*, *13*(17). https://doi.org/10.3390/app13179488

Ma, R., Wang, Q., Bu, X., & Chen, X. (2023). Real-Time Detection of DDoS Attacks Based on Random Forest in SDN. *Applied Sciences (Switzerland)*, *13*(13). https://doi.org/10.3390/app13137872

Mohammadi, R., Lal, C., & Conti, M. (2023). HTTPScout: A Machine Learning based Countermeasure for HTTP Flood Attacks in SDN. *International Journal of Information Security*, *22*(2), 367–379. https://doi.org/10.1007/s10207-022-00641-3

Mustapha, A., Abdul-Rani, A. M., Saad, N., & Mustapha, M. (2024a). Advancements in traffic simulation for enhanced road safety: A review. *Simulation Modelling Practice and Theory*, *137*. https://doi.org/10.1016/j.simpat.2024.103017

Mustapha, A., Abdul-Rani, A. M., Saad, N., & Mustapha, M. (2024b). Ergonomic principles of road signs comprehension: A literature review. *Transportation Research Part F: Traffic Psychology and Behaviour*, *101*(May 2023), 279–305. https://doi.org/10.1016/j.trf.2023.12.020

Nawaz, G., Junaid, M., Akhunzada, A., Gani, A., Nawazish, S., Yaqub, A., Ahmed, A., & Ajab, H. (2023). Detecting and Mitigating DDOS Attacks in SDNs Using Deep Neural Network. *Computers, Materials and Continua*, *77*(2), 2157–2178. https://doi.org/10.32604/cmc.2023.026952

Nawaz, H., Ali, M. A., Rai, S. I., & Maqsood, M. (2024). Comparative Analysis of Cloud based SDN and NFV in 5g Networks. *The Asian Bulletin of Big Data Management*, *4*(1). https://doi.org/10.62019/abbdm.v4i1.114

Perez-Diaz, J. A., Valdovinos, I. A., Choo, K. K. R., & Zhu, D. (2020). A Flexible SDN-Based Architecture for Identifying and Mitigating Low-Rate DDoS Attacks Using Machine Learning. *IEEE Access*, *8*, 155859–155872. https://doi.org/10.1109/ACCESS.2020.3019330

Polat, H., Polat, O., & Cetin, A. (2020). Detecting DDoS attacks in software-defined networks through feature selection methods and machine learning models. *Sustainability (Switzerland)*, *12*(3). https://doi.org/10.3390/su12031035

Ribeiro, M. A., Pereira Fonseca, M. S., & de Santi, J. (2023). Detecting and mitigating DDoS attacks with moving target defense approach based on automated flow classification in SDN networks. *Computers and Security*, *134*. https://doi.org/10.1016/j.cose.2023.103462

Santos-Neto, M. J., Bordim, J. L., Alchieri, E. A. P., & Ishikawa, E. (2024). DDoS attack detection in SDN: Enhancing entropy-based detection with machine learning. *Concurrency and Computation: Practice and Experience*, *36*(11). https://doi.org/10.1002/cpe.8021

Sebopelo, R., Isong, B., Gasela, N., & Abu-Mahfouz, A. M. (2021). A Review of Intrusion Detection Techniques in the SDN Environment. *2021 3rd International Multidisciplinary Information Technology and Engineering Conference, IMITEC 2021*. https://doi.org/10.1109/IMITEC52926.2021.9714581

Sendil Vadivu, D., & Rajagopalan, N. (2024). RyuGuard—Combining Ryu and machine learning for proactive DDoS defense in software-defined networks. *Concurrency and Computation: Practice and Experience*, *36*(28). https://doi.org/10.1002/cpe.8289

Setitra, M. A., Fan, M., Agbley, B. L. Y., & Bensalem, Z. E. A. (2023). Optimized MLP-CNN Model to Enhance Detecting DDoS Attacks in SDN Environment. *Network*, *3*(4), 538–562. https://doi.org/10.3390/network3040024

Swami, R., Dave, M., & Ranga, V. (2019). Software-defined Networking-based DDoS Defense Mechanisms. *ACM Computing Surveys*, *52*(2). https://doi.org/10.1145/3301614

Tang, D., Yan, Y., Zhang, S., Chen, J., & Qin, Z. (2022). Performance and Features: Mitigating the Low-Rate TCP-Targeted DoS Attack via SDN. *IEEE Journal on Selected Areas in Communications*, *40*(1), 428–444. https://doi.org/10.1109/JSAC.2021.3126053

Ussatova, O., Zhumabekova, A., Begimbayeva, Y., Matson, E. T., & Ussatov, N. (2022). Comprehensive DDoS Attack Classification Using Machine Learning Algorithms. *Computers, Materials and Continua*, *73*(1), 577–594. https://doi.org/10.32604/cmc.2022.026552

Wang, J., & Wang, L. (2022). SDN-Defend: A Lightweight Online Attack Detection and Mitigation System for DDoS Attacks in SDN. *Sensors*, *22*(21). https://doi.org/10.3390/s22218287

Yoon, N., & Kim, H. (2024). Detecting DDoS based on attention mechanism for Software-Defined Networks. *Journal of Network and Computer Applications*, *230*. https://doi.org/10.1016/j.jnca.2024.103928

Yungaicela-Naula, N. M., Vargas-Rosales, C., Pérez-Díaz, J. A., & Carrera, D. F. (2022). A flexible SDN-based framework for slow-rate DDoS attack mitigation by using deep reinforcement learning. *Journal of Network and Computer Applications*, *205*. https://doi.org/10.1016/j.jnca.2022.103444