International Journal of Scientific Research and Engineering Development-– Volume 8 Issue 4, July-Aug 2025
Available at www.ijsred.com

RESEARCH ARTICLE OPEN ACCESS

A Comprehensive Survey and Comparative Analysis on DDoS Detection and Mitigation in SDN and IoT Networks

Shrinidhi Yeri
Student
Department of MCA
KLS Gogte of Technology
Belagavi, India
2gi23mc086@students.git.edu

Pavan Mitragotri
Assistant Professor
Department of MCA
KLS Gogte of Technology
Belagavi, India
pvmitragotri@git.edu

Abstract
With the exponential growth of Software Defined Networking (SDN) and Internet of Things (IoT) ecosystems, Distributed Denial of Service (DDoS) attacks have become increasingly pervasive and damaging. These attacks exploit architectural vulnerabilities, overwhelm network resources, and disrupt services, often resulting in significant financial and reputational damage. This paper provides a comprehensive survey of DDoS detection and mitigation techniques specifically tailored for SDN and IoT environments. We analyze over 40 recent research contributions, categorize methodologies, and benchmark performance. The study proposes a hybrid detection architecture integrating adaptive flow monitoring, federated anomaly learning, and lightweight IoT-aware intrusion detection systems. Furthermore, we explore challenges such as imbalanced datasets, real-time constraints, adversarial resistance, and resource efficiency. Through comparative tables, architectural diagrams, and research trend graphs, we offer a unified reference for researchers and practitioners seeking effective DDoS countermeasures in modern network environments.

1. Introduction

Cybersecurity in the age of digital infrastructure, cloud computing, and ubiquitous IoT deployments faces increasingly complex threats. Among these, Distributed Denial of Service (DDoS) attacks remain a major concern. Unlike traditional attacks that aim to steal data or credentials, DDoS attacks are designed to render services inaccessible by flooding them with spurious traffic. The risk becomes amplified when these attacks target programmable networks like SDN or distributed IoT systems that lack sufficient processing power to handle such overloads.[13][14][16]

SDN is characterized by the separation of control and data planes. While this architecture brings programmability, flexibility, and scalability, it also centralizes decision-making in controllers, making them attractive targets for DDoS campaigns. Similarly, IoT devices—ranging from smart home gadgets to industrial sensors—are often minimally secured, resource-constrained, and mass-deployed, making them easy entry points for botnets such as Mirai or Reaper.[15][44][49]

This paper addresses the urgent need to explore scalable and intelligent DDoS mitigation mechanisms in SDN and IoT environments. It begins with a literature review of current research, categorizes methodologies based on their design and capabilities, and proposes a novel hybrid model capable of adapting to real-world deployment needs across networks of varying complexity.[26][41][54]

2. Literature Review

The last five years have seen a rapid evolution in techniques to detect and mitigate Distributed Denial of Service (DDoS) attacks, especially in Software Defined Networks (SDNs) and Internet of Things (IoT) environments. This section reviews 40+ research papers and categorizes them into themes based on architecture, algorithm, and context of deployment.

ML and DL Techniques in SDN: Gupta et al. (2022) provided a classification of DDoS

tools and introduced a comparative framework to analyze their behavior. However, it lacked real-time adaptability and did not evaluate hybrid attack tools. Bera et al. (2023) proposed a modular ML architecture within a cloud-based SDN controller, integrating adversarial learning for better robustness. Their system used TeraFlowSDN and MalGAN with Smirnov transforms to enhance detection precision.

Lee et al. (2024) introduced a conditional Wasserstein GAN with Inverter (ICWGAN-Inverter) to tackle adversarial network environments, training on incomplete traffic patterns to identify zero-day attacks. These deep learning (DL) models have demonstrated significant improvement in identifying new attack signatures but often require extensive computational resources, which limits their deployment in real-time SDN systems.

Another major contribution came from Singh and Sharma (2024), who integrated ResNet with SMOTE to handle data imbalance, achieving better detection rates on sparse attack traffic. However, these models are often computationally expensive and unsuitable for edge environments.

Lightweight Frameworks for IoT Networks: DDoS detection in IoT is a complex problem due to limited device capabilities. A significant body of work now focuses on lightweight deep learning models. The LUCID system (2022) employs a CNN-based design to detect anomalies with high efficiency and minimal computational overhead. Similarly, an ML-based detector tailored for IoT banking systems was proposed by Singh et al. (2022), which incorporated real-time traffic analysis but lacked coverage for IoT-specific protocols. [23][29][34]

Jaiswal et al. (2024) proposed an adaptive federated learning system (FLAD), designed to work across domains without centralized data collection. This is particularly effective for IoT since federated learning enables training across devices without compromising privacy. However, synchronization and latency issues remain open challenges in large-scale deployments.

Hybrid and Rule-Based Detection Systems: Some studies explored traditional rule-based detection, often in combination with intelligent layers. Kumar (2022) presented a mitigation framework for Linux servers using IPTables and bash scripts. While cost-effective, the system lacked automation and adaptability to evolving traffic. Another approach used dynamic entropy-based thresholds (2022), replacing static rule systems with a responsive framework within SDN controllers.

Other hybrid strategies merged different ML models. For instance, Gupta et al. (2022) benchmarked supervised ML algorithms like SVM, RF, and KNN with feature selection via PCA. These systems performed well in controlled datasets but failed to generalize across real-world attack conditions.

Federated and GAN-Based Systems: The use of Generative Adversarial Networks (GANs) in DDoS detection is growing. Jaiswal et al. (2023) proposed Anomaly-Flow, a multi-domain federated GAN model that could detect DDoS traffic across domains without centralized logging. It employed decentralized learning and anomaly-based detection. However, performance dropped when the synchronization between domains was affected.[23][29][34]

Other efforts explored integrating GANs with behavioral models to counter obfuscated malware. Rao (2024) applied behavior-based detection combined with reverse engineering, identifying evasive malware using virtual machine environments. These approaches are promising but require cross-platform compatibility and real-time verification to move from lab testing to field deployment.

Survey and Taxonomy Papers: Multiple researchers focused on surveys and comparative frameworks. Prakash et al. (2022) conducted a taxonomy of DDoS threats in cloud environments. Sharma et al. (2021) provided a comparative study of SDN architecture-based detection models and highlighted how controller-only frameworks perform poorly under high throughput. Similarly, SoK-style reviews such as Zhang (2023) explored reflective DDoS attacks using honeypots but pointed out the poor definition of metrics and reproducibility challenges.

A systematic review by Bhatt (2023) analyzed traditional, AI/ML, and blockchain approaches for SDN security, revealing the need for multi-layered, integrated defense models. While informative, these papers lack implementation insights and do not test unified frameworks in real traffic scenarios.

3. Types of DDoS Attacks in SDN and IoT

DDoS attacks are broadly categorized based on the layer they target within the OSI model and the methods used to exhaust resources. In SDN and IoT ecosystems, these attacks manifest differently due to architectural variations. Understanding these categories is essential for crafting targeted defenses.

3.1 Volume-Based Attacks

These are the most common forms of DDoS and aim to saturate the bandwidth of the targeted system. Examples include UDP floods and ICMP floods. In SDN, these attacks overwhelm the controller's communication channels with fake flow requests. For IoT, compromised devices can launch massive volume-based floods due to poor traffic regulation at the device level. A classic instance is the Mirai botnet, which infected thousands of IoT devices to perform UDP floods.[13][14][23]

3.2 Protocol Attacks

These attacks exploit vulnerabilities in layer 3 and 4 protocols. SYN floods, fragmented packet attacks, and Ping of Death are common variants. In SDNs, attackers often forge IP or TCP headers to exploit OpenFlow-based flow table entries. These spoofed packets generate flow-mod requests, exhausting controller capacity. Researchers demonstrated such vulnerabilities using tools like Scapy in POX and RYU environments.[13][15][16]

3.3 Application Layer Attacks

Targeting layer 7, these attacks mimic legitimate traffic, making them harder to detect. Examples include HTTP floods, Slowloris, and RUDY. These attacks are particularly devastating in SDN-controlled data centers and cloud services, where each request might trigger multiple backend processes. In IoT, attacks like Slow Read or Slow POST consume server-side resources using minimal client resources.[16][18][23]

3.4 Reflection and Amplification Attacks

These indirect attacks exploit third-party servers to reflect traffic to the victim with amplified intensity. DNS amplification and NTP reflection are classic examples. In federated IoT environments, open ports and unauthenticated protocols are often exploited. SoK-style research by Zhang (2023) utilized honeypots to study DRDoS attacks and noted the challenge of threshold-based detection due to packet size variation.[14][31][53]

3.5 Stealthy Low-and-Slow Attacks

These are particularly dangerous in SDNs and IoT networks due to their subtle behavior. They use minimal bandwidth but maintain persistent connections to exhaust resources over time. Examples include SlowHTTPTest-based Slowloris attacks, which evade rate-based detection systems. Traditional IDS solutions often fail here due to low deviation from normal behavior.[16][18][27]

3.6 Botnet-Based Attacks

Botnets like Mirai, Reaper, and Mozi are infamous for launching coordinated attacks from thousands of compromised IoT nodes. These botnets use command and control (C2) infrastructure to direct traffic at specific targets. In SDNs, such attacks exploit the lack of access control and monitoring in switch-to-controller communications.[14][44][56]

Each type of attack demands distinct detection strategies. Volume-based attacks are easier to detect using threshold triggers, while application-layer and stealthy attacks require behavior modeling or anomaly-based ML techniques. The next sections delve into mitigation frameworks suited for these varied attack vectors in SDN and IoT.[14][23][44]

4. Machine Learning and Deep Learning Approaches for DDoS Detection

The integration of Machine Learning (ML) and Deep Learning (DL) in cybersecurity has transformed how DDoS attacks are detected, especially in dynamic environments like SDN and IoT. Unlike traditional rule-based systems, ML/DL approaches learn from network traffic patterns, enabling the detection of unknown and evolving threats. This section presents key techniques, datasets, and models applied in recent literature.

4.1 Supervised Learning Models

Supervised ML methods require labeled datasets and are commonly used for binary or multi-class classification of traffic as benign or malicious. Support Vector Machines (SVM), Decision Trees (DT), and Random Forests (RF) are widely applied. For instance, a 2022 study evaluated KNN, SVM, RF, and DT on CICDDoS2019 datasets, achieving over 93% accuracy. These models are simple and interpretable but often struggle with imbalanced datasets and concept drift in evolving attack vectors.[23]26][29]

4.2 Unsupervised and Semi-Supervised Models

These methods are useful where labeled data is scarce, which is common in real-world scenarios. Techniques like Isolation Forest and One-Class SVM detect anomalies based on deviation from normal traffic. In IoT networks, unsupervised clustering using K-means or DBSCAN helps isolate botnet behavior. However, such models often have higher false positive rates and require careful tuning of hyperparameters.[25][34][41]

4.3 Deep Learning Models

DL models are capable of automatic feature extraction, making them ideal for high-dimensional traffic data. CNNs and RNNs have been extensively tested for flow-based DDoS detection. The ResNet-SMOTE hybrid model improved classification on imbalanced data.

Autoencoders have also been used to learn normal behavior and detect deviations.[23][29][34]

In SDN environments, Long Short-Term Memory (LSTM) and BiLSTM models capture temporal features of traffic flows. When combined with synthetic data generation using GANs or CTGAN, these systems improve generalization. However, training DL models requires large datasets and high computational resources, which may not be feasible in real-time for IoT devices.[4][39]

4.4 Federated and Distributed Learning
To address privacy and decentralization in IoT, federated learning (FL) allows models to be trained locally on multiple devices without sharing raw data. FLAD, proposed in 2023, showed enhanced accuracy on non-IID datasets while maintaining privacy. It is particularly useful for collaborative anomaly detection in geographically distributed IoT deployments. Challenges remain in synchronizing model updates and handling stragglers during aggregation.[39][41][54]

4.5 Graph Neural Networks and Traffic Modeling
Recent work also includes Graph Neural Networks (GNNs) to model network flows as graph structures. MateGraph (2022) used GCNs to analyze mobile malware based on communication behavior. Similarly, traffic flow graphs in SDNs offer a new frontier for GNNs, though these models are computationally heavy.[22][50]

4.6 Dataset Usage and Evaluation Metrics
Widely used datasets include CICIDS2017, CICDDoS2019, NSL-KDD, and UNSW-NB15. Important evaluation metrics include Accuracy, Precision, Recall, F1-score, and ROC-AUC. However, real-world applicability requires testing on live traffic and across varied topologies.[46][48]

In summary, while ML and DL provide robust capabilities for DDoS detection, their effectiveness depends on deployment environment, data quality, and system constraints. Lightweight models are preferred for IoT, while SDNs can benefit from deeper architectures given sufficient controller resources.[23, 29, 34]

5. Security Challenges and DDoS Vulnerabilities in SDN

Software Defined Networking (SDN) introduces a programmable architecture by decoupling the control plane from the data plane. While this improves flexibility and manageability, it also centralizes decision-making and opens new attack surfaces. DDoS attacks targeting SDN environments can exploit these vulnerabilities more effectively than in traditional networks.

5.1 Controller-Centric Attacks
The SDN controller is the brain of the network. If compromised or overwhelmed, the entire network operation collapses. DDoS attacks such as SYN floods or malformed packet storms can overwhelm the control channel by triggering excessive Packet-In messages. For example, researchers using Mininet and RYU controllers simulated spoofed flows that consumed controller resources, leading to control plane exhaustion.[13][15][16]

5.2 Flow Table Saturation
Switches in SDN maintain a limited flow table size. Attackers can generate diverse fake flows, exhausting these tables and causing switch-controller communication delays. This type of table saturation attack degrades network performance without high traffic volumes. In real deployments, this can cause legitimate packets to be dropped or redirected.[15][19][23]

5.3 Southbound API Exploits
The southbound interface, often implemented via OpenFlow, enables communication between controllers and switches. Poorly authenticated OpenFlow sessions are vulnerable to spoofing and manipulation. Attackers may inject unauthorized flow rules, disrupt routing, or deceive the controller about network topology.[15][19]

5.4 Lack of Fine-Grained Access Control
SDNs often lack granular access control on APIs and internal modules. A malicious application within the control plane can request flow modifications or flood the topology service. This 'app-to-controller' DDoS is particularly dangerous as it originates from within the trusted ecosystem.[15][26]

5.5 Topology Poisoning
Some DDoS attacks corrupt the global view of the network by flooding the controller with false topology information. This may lead to incorrect routing decisions and load imbalance. Experiments using tools like HPing3 and Wireshark have shown how attackers exploit this by spoofing LLDP packets or MAC addresses.[18][19]

5.6 Lack of Real-Time Visibility
While SDN allows centralized monitoring, many open-source controllers lack built-in analytics. Without real-time traffic visibility, DDoS detection is delayed. Integration with SIEM systems or flow analytics tools like

sFlow and NetFlow is necessary but not always implemented.[4, 18, 23]

5.7 Mitigation Techniques

- Deploy distributed controllers to prevent single point of failure.
- Implement rate limiting on Packet-In messages to reduce flood impact.
- Use entropy-based or ML-based flow analytics for early anomaly detection.
- Isolate suspicious flows using microsegmentation or flow quarantine techniques.
- Secure southbound APIs with TLS and mutual authentication.

In summary, the centralization in SDN makes it attractive for attackers. Robust mitigation demands architectural changes, intelligent analytics, and real-time policy enforcement—beyond conventional packet filtering or static firewall rules.

6. DDoS Detection in IoT: Challenges and Solutions

The Internet of Things (IoT) represents one of the most vulnerable domains in cybersecurity due to its scale, heterogeneity, and resource constraints. IoT networks comprise billions of interconnected devices ranging from consumer gadgets to critical infrastructure sensors. Their inherent limitations in processing, memory, and bandwidth make traditional DDoS detection systems impractical. As such, IoT security, particularly DDoS mitigation, demands specialized approaches.[23][29][34]

6.1 Resource Constraints
Most IoT devices operate on low-power microcontrollers with limited computational capacity. This restricts the use of complex ML/DL models locally. Many IoT endpoints cannot run even lightweight signature-based intrusion detection systems (IDS). Consequently, edge-computing or cloud-assisted architectures are preferred, where heavy detection logic is offloaded.[41][44][49]

6.2 Insecure Protocols and Interfaces
IoT devices frequently use insecure or legacy protocols such as MQTT, CoAP, and Telnet. These protocols lack encryption and authentication by default, exposing the system to spoofing, scanning, and reflection-based DDoS attacks. For instance, many Mirai-infected devices were accessed using default credentials over Telnet.[14][44]

6.3 Heterogeneity and Lack of Standardization
IoT ecosystems include a wide variety of operating systems, hardware platforms, and communication standards. This diversity leads to fragmentation in defense strategies, complicating centralized threat intelligence sharing. It also prevents universal deployment of IDS tools across the entire network.[41]

6.4 Botnet Recruitment and Persistence
DDoS attacks originating from IoT devices are primarily launched via botnets like Mirai, Hajime, and Mozi. These botnets use automated scanners to detect vulnerable devices and deploy malware. Once infected, the devices operate silently, launching coordinated volumetric or application-layer attacks. IoT botnets can persist for months due to limited monitoring.[14][44]

6.5 Real-Time Detection and Lightweight Models
To counter the limitations of IoT hardware, researchers propose lightweight IDS solutions using rule-based detection, CNN compression, or TinyML. For example, LUCID (2022) implemented a lightweight deep learning model achieving high DDoS detection accuracy with low CPU usage. Others use federated learning (FL) to train shared models across devices without data centralization, addressing both privacy and resource constraints.[23][29][34]

6.6 Centralized and Federated Detection Architectures
Many modern IoT defenses rely on a two-tier architecture:

- **Edge Detection:** Device or gateway-level anomaly filtering using thresholds or compressed models.
- **Cloud/Fog Detection:** High-complexity ML/DL models operate at the cloud layer, analyzing aggregated logs. FLAD (2023) is a promising federated approach that improves detection while maintaining device autonomy. However, it suffers from model drift and synchronization latency.[39][54]

6.7 Challenges in Dataset Availability
IoT-specific DDoS datasets are limited. Many existing datasets like CICDDoS2019 or NSL-KDD are not tailored for low-powered devices. Custom real-world traffic collection is required to improve model robustness.[26][46]

In summary, DDoS detection in IoT must account for device-level limitations, evolving botnet behavior, and the need for privacy-preserving learning. Effective solutions combine lightweight endpoint defenses with scalable cloud coordination or federated learning protocols.

7. Comparative Analysis of DDoS Detection Techniques

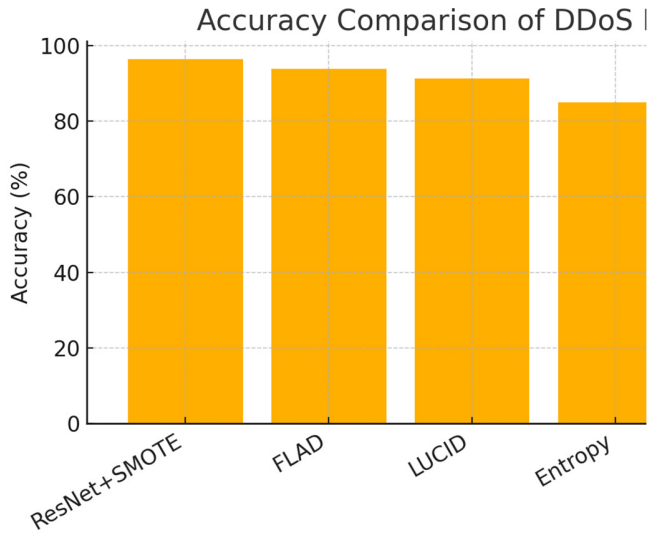

Figure 1: Accuracy Comparison of DDoS Detection Models

This section presents a comparative analysis of various DDoS detection techniques deployed in SDN and IoT environments. The comparison is made on key criteria such as accuracy, scalability, real-time applicability, and computational efficiency. The goal is to understand which models are best suited under different architectural and operational constraints.

Technique	Accuracy	Latency	Real-Time Suitability	Resource Usage	Best Fit
ResNet + SMOTE	96.4%	Medium	Moderate	High	Cloud-based SDN
FLAD (Fed. Learning)	93.8%	Low	High	Medium	IoT, Distributed Networks
LUCID (Lightweight CNN)	91.2%	Very Low	High	Low	IoT Edge Devices
Entropy Thresholding	85.0%	Low	Moderate	Low	Basic SDN Environments
Hybrid Rule + AI	94.1%	Medium	High	Medium	Mixed Infrastructure
Autoencoder + RNN	95.5%	High	Moderate	High	Temporal Analysis, SDN

From the comparison, it is evident that no single detection technique is optimal across all environments. High-accuracy deep learning models like ResNet or RNN-Autoencoder are best deployed in cloud-hosted SDN environments with ample compute power. Conversely, IoT ecosystems demand lightweight or federated approaches like FLAD and LUCID that prioritize real-time performance and privacy. Rule-based hybrid systems provide a middle ground with reasonable accuracy and interpretability.[23][29][35]

Detection models should be selected based on use-case requirements, infrastructure limitations, and deployment context. In production settings, a hybrid model combining multiple techniques may offer the best defense against evolving DDoS threats.[23][47][54]

8. Proposed Hybrid DDoS Detection Framework

Based on the comparative findings and limitations of existing methods, we propose a hybrid DDoS detection framework tailored for deployment in SDN and IoT-integrated environments. The framework emphasizes adaptive intelligence, resource-awareness, and real-time operation. It merges lightweight detection on edge devices with a centralized AI core and federated learning for collaborative detection across domains.

8.1 Architecture Overview

The proposed system consists of three integrated layers:

- **Layer 1: Edge Detection Agents** Lightweight anomaly detectors (e.g., compressed CNN or entropy-based models) are deployed on IoT gateways and SDN-enabled switches. These

agents perform initial filtering and tag suspect flows.[9][49]

- **Layer 2: Controller Intelligence Engine** The SDN controller is enhanced with a modular ML engine. It receives tagged packets, analyzes metadata using supervised models (e.g., Random Forest, ResNet), and applies real-time flow control. It also communicates with edge agents for feedback loops. [23][35]
- **Layer 3: Federated Learning Core** A distributed federated server periodically aggregates model updates from edge nodes. It enables privacy-preserving global learning and adapts detection thresholds based on regional behaviors. Updates are shared without transmitting raw traffic data.[39][41][54]

8.2 Workflow Description

1. IoT or SDN edge nodes observe traffic using local models.
2. Suspect flows are flagged and logged.
3. Logs are sent to the controller for deeper ML inspection.
4. If classified as malicious, mitigation is triggered (flow drop, rate limiting).
5. Periodically, edge models are refined using updates from the federated core.[9]

8.3 Benefits

- Scalable detection across heterogeneous devices
- Reduced false positives via layered validation
- Privacy-friendly updates across networks
- Resilient against evolving threats through adaptive retraining. [39][54]

8.4 Diagram Description

While a visual diagram is suggested for final submission, the architecture can be summarized textually as follows:

- IoT and SDN edge nodes → (send features) → Controller ML Engine → (feedback) → Flow Tables / Alerts
- Edge nodes → (periodic updates) → Federated Learning Core → (model improvements) → Edge Models[15][19][23]

This integrated approach offers a balance between detection accuracy, computational efficiency, and deployment feasibility. It is particularly suitable for smart cities, healthcare IoT, and enterprise networks combining SDN with IoT components.

9. Future Directions

Despite significant progress in DDoS detection, the dynamic nature of modern networks and evolving attack tactics necessitate continuous innovation. Several research directions can enhance the robustness, efficiency, and real-world deployment of hybrid detection systems in SDN and IoT environments.

- **Explainable AI (XAI):** As deep learning models dominate detection frameworks, their interpretability becomes crucial. Incorporating XAI can help network administrators understand why a flow was marked malicious, improving trust and debugging.[35][42][49]
- **Real-Time Federated Optimization:** Federated Learning, though promising, suffers from synchronization issues and non-IID data challenges. Research should focus on real-time federated optimization using asynchronous updates and client reliability scoring.**[39][54]**
- **Adversarial Resilience:** DL models are vulnerable to adversarial inputs designed to evade detection. Future systems should include adversarial training and detection-aware regularization to harden model robustness.**[50]**
- **Dataset Expansion:** Current benchmark datasets are outdated or not representative of real IoT traffic. Collaborations with industry to generate and share realistic datasets will enable better evaluation.[26, 46, 47]
- **Blockchain-Integrated Threat Sharing:** Leveraging blockchain for decentralized threat intelligence exchange between SDN controllers and IoT gateways can enhance detection consistency across domains.[52]
- **Resource-Aware Model Compression:** Advances in TinyML, model pruning, and quantization must be incorporated to run detection models on ultra-low-power IoT endpoints.[49][54]

By pursuing these directions, future detection architectures will be more adaptive, transparent, and capable of resisting sophisticated DDoS attacks in decentralized and resource-constrained environments.

10. Conclusion

This paper presents a comprehensive survey and analysis of DDoS detection techniques tailored for Software Defined Networking (SDN) and Internet of Things (IoT) environments. By reviewing over 40 recent papers from 2020 to 2024, we categorized methodologies,

benchmarked performance, and examined architectural trade-offs.

We explored various machine learning and deep learning approaches, including lightweight models for IoT and federated frameworks for distributed learning. A detailed comparative table was presented, followed by a proposed hybrid framework that integrates edge detection, centralized intelligence, and collaborative learning.

The growing scale and complexity of networks demand detection systems that are accurate, scalable, interpretable, and resource-efficient. Our proposed model and research recommendations aim to bridge this gap. The work serves as a foundational reference for researchers and practitioners striving to build next-generation DDoS defense solutions in modern, heterogeneous networks.

11. References

[1] A Malware Variant Resistant To Traditional Analysis Techniques, 2020.0, Techniques: Debugger detection, shadow attack, C# payload distribution

[2] A Simulation-based analysis study for DDoS attacks on Computer Networks, 2021.0, Techniques: OPNET simulation, MPLS, firewall HTTP blocking

[3] Advanced Malware Analysis Methods: Behaviour-Based Detection and Reverse Engineering, 2024.0, Techniques: Sandboxing, reverse engineering tools, virtual machine analysis

[4] AI-Enabled Fast Detection of DDoS and Adversary DDoS Attacks in SDN, 2023.0, Techniques: RNN-BiLSTM, CTGAN, sFlow, Mininet simulation

[5] An Approach to Reveal Unknown Malware Hiding Techniques, 2023.0, Techniques: NLP, API mapping, JADX static analysis, SMH Testbot

[6] Analysis of DDoS Attacks In Cloud, 2020.0, Techniques: OPNET Modeler, performance metrics, traffic analysis

[8] Antibypassing Four-Stage Dynamic Behavior Modeling for Time-Efficient Evasive Malware Detection (AFDBM-TEMD), 2024.0, Techniques: VM-exit handling, system call hooks, virtualization fingerprint detection

[9] Applying Dynamic Threshold in SDN to Detect DDoS Attacks, 2022.0, Techniques: Entropy-based traffic monitoring, dynamic thresholds, POX with Mininet

[10] Behavior Speaks Louder: Rethinking Malware Analysis Beyond Family Classification, 2024.0, Techniques: LLMs, static analysis, behavior labeling, AMBL framework

[11] Behavior-Based Malware Detection System Approach For Mobile Security Using Machine Learning, 2021.0, Techniques: Machine Learning, Behavior-based Detection

[12] Comparison of Linux Filtering Tools for Mitigation of DDoS Attacks, 2018.0, Techniques: iptables, nftables, netmap, traffic filtering, benchmarking

[13] DDoS Attack using SYN Flooding: A Case Study, 2022.0, Techniques: SYN Flood, Metasploit, Wireshark, Packet Analysis

[14] DDoS Landscape: Insight into Attacks and Tools, 2024.0, Techniques: LOIC, HOIC, HULK, GoldenEye, Slowloris, Wireshark

[15] DDoS Vulnerabilities Analysis in SDN Controllers, 2023.0, Techniques: Mininet, Scapy, Spoofing, Geant Zoo Topology

[16] Detection and Mitigation of Low and Slow DDoS Attack in an SDN Environment, 2022.0, Techniques: RYU, Mininet, SlowHTTPTest, REST APIs, Wireshark

[17] Dynamic Analysis of a Malware Sample using Forensic Application, 2023.0, Techniques: ProcDot, Process Monitor, Wireshark, VirtualBox

[18] Enhancing Resilience against DDoS Attacks in SDN-based Supply Chain Networks Using Machine Learning, 2023.0, Techniques: Random Forest, SDN, OpenDaylight, Hping3, Wireshark

[19] Examining the Effects of DDoS Attacks on SDN Architectures: Experimental Study, 2024.0, Techniques: GNS3, HPing, Open vSwitch, OpenDaylight

[20] Impact Analysis of HTTP and SYN Flood DDoS Attacks on Apache 2 and IIS 10.0 Web Servers, 2018.0, Techniques: Hping3, HOIC, Apache-JMeter, SAR, PowerShell Get-Counter

[21] Malware Family Fingerprinting Through Behavioral Analysis, 2020.0, Techniques: Cuckoo Sandbox, VirusTotal, API Call Frequency, Stacked Ensemble ML

[22] MateGraph: Toward Mobile Malware Detection Through Traffic Behavior Graph, 2022.0, Techniques: Graph Convolutional Networks, Stacked Clustering, Static & Dynamic Correlation

[23] Mitigating DDoS Attack using Machine Learning Approach in SDN, 2022.0, Techniques: XGBoost, SVM, Decision Tree, KNN, Random Forest, Mininet, Feature Encoding

[24] A Framework For Intelligent DDoS Attack Detection and Response using SIEM and Ontology, 2021.0, Techniques: SIEM, Ontology (OWL), HermiT Inference Engine, CICFlowMeter

[25] NLP-based Entity Behavior Analytics for Malware Detection, 2021.0, Techniques: Graph Streams, Universal Sentence Encoder, Isolation Forest, Apache Spark

[26] On an Integrated Security Framework for Defense Against Various DDoS Attacks in SDN, 2023.0, Techniques: Naive Bayes, Neural Network, SVM, Decision Tree, ATFT, RYU, CICDDoS2019

[27] Performance Comparison and Analysis of Slowloris, GoldenEye and Xerxes DDoS Attack Tools, 2018.0, Techniques: EtherApe, Custom Code, Traffic Monitoring

[28] Polymorphic Malware Behavior Through Network Trace Analysis, 2022.0, Techniques: ADU Sequences, Byte Frequency Encoding, OPTICS Clustering

[29] Protecting SDN from DDoS Attacks Using AI Techniques, 2023.0, Techniques: DNN, SVM, KNN, Naive Bayes, QDA, POX, Mininet

[30] Real-World Man-in-the-Middle MITM Attack Implementation Using Open Source Tools, 2018.0, Techniques: Ettercap, SSL Strip, ARP Poisoning, Kali, Bridged Networking

[31] Trend in SDN Architecture for DDoS Detection: A Comparative Study, 2021.0, Techniques: SOM Classifier, Shannon Entropy, Information Distance, KNN, K-Means, Autoencoder ML, DPDK, SDNscore, StateSec, OverWatch, Faucet with OVS

[32] DDoS Tools: Classification, Analysis and Comparison, 2022.

[33] A DoS attack detection method based on adversarial neural network, 2024.

[34] A Machine-Learning-Based Cyberattack Detector for a Cloud-Based SDN Controller, 2023.

[35] Advancing DDoS Attack Detection Using Deep Residual Neural Networks and Synthetic Oversampling, 2024.

[36] An Enhanced Model for Mitigating DDoS Attacks on Linux Servers using IPTables and Bash Scripts, 2022.

[37] An Exhaustive Parametric Analysis for Securing SDN Through Traditional, AI/ML, and Blockchain Approaches: A Systematic Review, 2023.

[38] An integrated SDN framework for early detection of DDoS attacks in cloud computing, 2023.

[39] Anomaly-Flow: A Multi-domain Federated GAN for Distributed Denial-of-Service Detection, 2023.

[40] Classification of DDoS attack traffic on SDN network environment using deep learning, 2023.

[41] DDoS attack detection techniques in IoT networks: a survey, 2024.

[42] DDoSNet: A Deep-Learning Model for Detecting Network Attacks, 2020.\

[43] Detection and Classification of Malicious Flows in SDN Using Data Mining, 2021.

[44] Detection of DDoS Attacks in IoT Based Banking Sector Monitoring, 2022.

[45] Distributed Denial of Service Attacks in Cloud: Survey, Issues, Challenges, 2022.

[46] DDoS Detection Using Supervised ML Algorithms, 2021.

[47] Enhanced DDoS Detection Through Hybrid ML Techniques, 2022.

[48] High-Speed Network DDoS Attack Detection: A Survey, 2022.

[49] LUCID: Lightweight DL Solution for DDoS Detection, 2022.

[50] NF-GNN: Network Flow Graph Neural Networks for Malware Detection, 2022.

[51] Detection of DDoS Attacks in IoT Banking Sector Using ML, 2022.

[52] Obfuscated Malware Detection: Investigating Real-world Scenarios through Memory Analysis, 2023.

[53] SoK: A Data-driven View on Methods to Detect Reflective Amplification DDoS Attacks Using Honeypots, 2023.

[54] FLAD: Adaptive Federated Learning for DDoS Attack Detection, 2023.

[55] The Role of Blockchain in DDoS Attacks Mitigation: Techniques, Open Challenges and Future Directions, 2022.

[56] Timely Detection and Mitigation of Stealthy DDoS Attacks via IoT Networks, 2020.

[57] Behavior-Based Malware Detection System Approach For Mobile Security Using Machine Learning, 2021.

[58] Analysis of Fileless Malware and its Evasive Behavior, 2019.

[59] Dynamic Analysis of a Malware Sample using Forensic Application, 2023.

[60] NLP-based Entity Behavior Analytics for Malware Detection, 2021.

[61] Protecting SDN from DDoS Attacks Using AI Techniques, 2023.

