

A Self-Organizing Map with Temporal Aggregation for DDoS Detection in SDN (SOM-TAD)

Christian F. G. Azonyetin, Iguatemi E. Fonseca

Abstract— This paper proposes "SOM-TAD", a DDoS detection and mitigation framework for Software-Defined Networking (SDN) based on unsupervised learning and temporal anomaly modeling. The architecture extends SDN with Management and Knowledge Planes, decoupling data processing, inference, and control. Self-Organizing Maps (SOM), trained on benign traffic, model normal behavior using statistically normalized quantization error. A multi-resolution ensemble and temporal evidence aggregation improve robustness against distributed and low-rate attacks. The system operates consistently in offline and real-time modes and integrates with an event-driven SDN controller for autonomous mitigation. Experimental results demonstrate high separability and effective detection of multi-vector DDoS attacks.

Keywords— Software-Defined Networking, Temporal Aggregation Detection, DDoS, Artificial Intelligence.

I. INTRODUCTION

The increasing complexity of network attacks has driven the development of more robust, scalable, and secure network architectures. Conventional security tools, including antivirus, anti-spam, and firewall solutions, are effective against known threats but often struggle to detect novel and sophisticated attacks [1]. In this context, Software-Defined Networking (SDN), combined with Machine Learning (ML) and network simulation tools, enables more dynamic and centrally managed network environments than traditional architectures [2].

SDN separates the control and data planes, migrating network intelligence from distributed hardware devices to a logically centralized controller [3]. However, this centralization introduces vulnerabilities across the data, control, and application planes, including DDoS attacks, controller compromise, and man-in-the-middle attacks [4], [5]. DDoS attacks remain particularly challenging because existing solutions may fail to reliably distinguish legitimate from malicious traffic, exposing controllers and forwarding devices to saturation [6]. Moreover, conventional SDN architectures and current ML- and Deep Learning-based security solutions remain predominantly reactive and insufficiently adaptive to dynamic attack scenarios [8]. Structural vulnerabilities, including controller centralization and limited TCAM capacity, further enable low-rate DDoS attacks that cause controller saturation, control-data plane congestion, buffer exhaustion, and flow-table overflow through continuous rule installation [9], [10].

Recent studies advocate redesigning SDN architectures through the integration of a Knowledge Plane (KP) [7]. Accordingly, this work proposes an extended SDN architecture integrating a Knowledge Plane and a Management Plane (MP) to enable automated, intelligent, and adaptive DDoS detection and mitigation. The architecture is experimentally evaluated in a Mininet-based virtual environment using a flow-level Self-Organizing Map (SOM)

combined with temporal evidence aggregation. Unlike conventional SOM-based approaches that treat flows as isolated observations, the proposed method models malicious activity through the temporal persistence and accumulation of anomalous patterns, enabling contextual and behavior-oriented detection from evolving traffic states.

The scientific contributions of this research include a hybrid knowledge-driven SDN architecture extending the conventional model with MP and KP, separating data processing from analytical intelligence and enabling multi-level detection. The proposed unsupervised statistical model uses benign traffic to learn normality through a multi-resolution SOM ensemble and statistical normalization of the quantization error (QE). A temporal intelligence mechanism aggregates anomaly evidence over time to capture persistent behavior and detect distributed and low-rate DDoS attacks. Finally, an offline-online pipeline operationalizes the architecture for real-time detection and mitigation through a reproducible and deployable SDN framework that preserves semantic consistency between training and operation.

The remainder of this paper is organized as follows. Section II presents the related work. Section III describes the proposed methodology. Section IV discusses the experimental results, and Section V concludes the paper.

II. RELATED WORK

Based on the literature review, Tables I and II summarize representative SOM-based approaches in SDN and compare them with the proposed framework in terms of temporal aggregation, low-rate attack detection, SDN integration, and hierarchical decision-making. The comparison highlights the framework's architectural and methodological novelty, while a controlled experimental baseline isolates the contribution of temporal evidence aggregation.

III. METHODOLOGY

A. System Overview.

The proposed multi-plane SDN architecture (Figure 1) transforms captured traffic Data $\rightarrow$ Information $\rightarrow$ Evidence $\rightarrow$ Knowledge $\rightarrow$ Action. The MP collects and preprocesses flows through semantic normalization, data cleaning, feature engineering, and statistical preprocessing to produce the feature vector $\phi(F)$. It exchanges information with the KP, Control Plane (CP), Data Plane (DP), and Application Plane (AP) through Interfaces (6), (5), (7), and (8), respectively.

The KP receives $\phi(F)$ and performs normal-behavior modeling, anomaly quantification, statistical evidence analysis, multi-resolution fusion, temporal aggregation, and knowledge construction, maintaining behavioral states and generating semantic events. It communicates with the MP and CP through Interfaces (6) and (11), respectively. The CP validates and deduplicates semantic events, synchronizes operational state, evaluates policies, selects mitigation strategies, generates and installs rules, and provides rule

consistency, auditing, traceability, and state persistence. It interfaces with the MP (5), KP (11), AP (2), and DP (1).

The AP abstracts service intents into action requests, whereas the DP forwards traffic, collects network metrics and statistics, and maintains the local network view. The AP and DP communicate with the CP through Interface (2) and Interface (1), respectively, while the DP also provides network data to the MP through Interface (7). Thus, the architecture is coordinated by Interfaces (6), (11), (5), (2), (1), (8), and (7), which exchange traffic data, feature vectors, analytical knowledge, control decisions, application requests, and network-state information across the MP, KP, CP, AP, and DP.

In the following equations, X denotes the input space; $\mathbf{x} * t$ the flow feature vector at time t ; d the feature dimension; W the temporal aggregation window; $\phi(\cdot)$ the feature-mapping function; μ and σ the normalization mean and standard deviation; $\mathbf{w} * i, j$ the weight vector of SOM neuron (i, j) ; (i^*, j^*) the Best Matching Unit (BMU); $QE(\mathbf{x})$ the quantization error; $z_k(\mathbf{x})$ the normalized anomaly score of SOM S_k ; $S(\mathbf{x})$ the final ensemble anomaly score; τ the anomaly threshold; A_t the accumulated temporal evidence; θ the decision threshold; and $g(\cdot)$ the mitigation decision function.

B. Data Plane (DP): Traffic Generation and Flow Representation

The DP is responsible for packet forwarding and traffic generation. Raw packets are aggregated into flows defined by the 5-tuple (src_ip, dst_ip, src_port, dst_port, protocol). From a computational perspective, this plane produces the input space:

$$X = \{\mathbf{x}_t\}_{t=1}^T, \mathbf{x}_t \in \mathbb{R}^d \quad (1)$$

in which each $\mathbf{x}_t$ corresponds to a feature vector derived from flow-level statistics over a temporal window.

C. Management Plane (MP): Feature Engineering and Temporal Modeling

The MP implements the transformation:

$$\phi: X_{raw} \rightarrow \mathbb{R}^d \quad (2)$$

This includes:

- 1) Temporal aggregation: flows are grouped per source IP within a sliding window W , producing:

$$\mathbf{x}_t = \phi(\{\text{flows}\}_{t-W}^t) \quad (3)$$

- 2) Feature construction: statistical descriptors such as packet rate, byte rate, flow count, and protocol distribution.
- 3) Normalization: feature scaling is applied:

$$\tilde{x} = \frac{x - \mu}{\sigma} \quad (4)$$

This plane defines the input distribution used by the learning model and ensures consistency between training and inference.

D. Knowledge Plane (KP): SOM-Based Anomaly Detection

The KP implements the core learning and inference mechanisms.

1) Topological Learning

A Self-Organizing Map (SOM) is defined as a grid of neurons with weights $w_{i,j} \in \mathbb{R}^d$, the Best Matching Unit (BMU) is:

$$(i^*, j^*) = \underset{i,j}{\operatorname{argmin}} \|\tilde{\mathbf{x}} - w_{i,j}\| \quad (5)$$

Training is performed using only benign data, enabling the model to approximate the manifold of normal traffic.

2) Anomaly Scoring

TABLE I
COMPARATIVE SUMMARY OF SOM-BASED APPROACHES IN SDN

Authors	Scope	Method / Algorithm	Architecture	Key Contribution	Limitations
[9] saidane et al. 2023	Secure routing under DDoS in SDN	ML-based Suspicion Risk Factor (SRF)	SDN (Data + Control)	Security-aware routing avoiding suspicious nodes; improved throughput over OSPF	Depends on classifier quality; routing-focused approach
[11] Liu et al. (2023)	Real-time DDoS detection	LDA + Supervised SOM (LSSOM)	Centralized SDN	98.2% accuracy with reduced classification time	Requires labeled data
[12] Marleau et al. (2024)	IP spoofing-based DDoS mitigation	BCP 38 + SDN filtering	SDN Edge-Control architecture	Efficient spoofing prevention with low computational cost	Cannot mitigate attacks from legitimate IPs
[13] Saravanan et al. (2024)	Cyberattack detection in SDN	ESN + Deep Learning	Centralized SDN	97.78% detection rate with reduced false positives	Limited real-time validation
[14] Jie Ma et al. (2025)	Collaborative DDoS defense in SD-ALoT	Federated Learning + SMPC + Semi-supervised Detection	Distributed SDN / Edge	Privacy-preserving and scalable collaborative defense	High coordination and computational complexity
[15] Thorig, Ibrahim et al (2025)	DDoS detection in SDN	Autoencoder + Deep Forest + GAN	Centralized SDN	Detection accuracy above 99% with robust feature learning	Possible overfitting and limited dataset validation
Proposed Work	Detection of distributed/low-rate DDoS attacks in SDN	SOM-based behavioral analysis + temporal aggregation	SDN + KP and MP	Temporal behavioral analysis + separated management + intelligence layers	Requires evaluation under large-scale + heterogeneous traffic conditions

TABLE II
COMPARATIVE ANALYSIS BETWEEN EXISTING SDN-BASED DDoS DETECTION APPROACHES AND THE PROPOSED ARCHITECTURE.

Architectural Dimension	Conventional SDN DDoS Detection	SOM/GH-SOM Approaches	Aggregation-Based Approaches	Proposed Architecture
Temporal Evidence Aggregation	Limited	No	Partial	Explicit Multi-Stage Aggregation
Detection of Distributed and Low-Rate Attacks	Limited	No	Partial	Explicitly Supported
Training-Inference Consistency	Limited/Partial	No	Limited	Unified Processing Pipeline
Integration with SDN Control Infrastructure	Basic	Partial	Partial	KP-MP-Controller Integration
Knowledge Plane and Management Plane Separation	No	No	No	Formally Defined
Hierarchical Analytical Decision Process	No	Limited	Partial	Explicit Decision Realization
Separation Between Feature Engineering and Intelligence	No	No	Partial	Architecturally Separated

The anomaly score is computed as the Quantization Error:

$$QE(x) = \|\tilde{x} - w_{i^*, j^*}\| \quad (6)$$

This score is statistically normalized:

$$z(x) = \frac{QE(x) - \mu_{QE}}{\sigma_{QE}} \quad (7)$$

3) Multi-Resolution Ensemble

Multiple SOMs S_k with different grid sizes are used. The final score is:

$$S(x) = \max_k z_k(x) \quad (8)$$

4) Temporal Evidence Aggregation

To incorporate persistence, anomaly evidence is accumulated over a window:

$$A_t = \sum_{t'=t-W}^t \mathbb{I}(S(x_{t'}) > \tau) \quad (9)$$

A flow is classified as anomalous if: $A_t \geq \theta$. This mechanism models temporal consistency and improves robustness against noise and low-rate attacks.

E. Training and Inference Consistency

The methodology is divided into:

- Offline phase: estimation of $\mu, \sigma, \mu_{QE}, \sigma_{QE}, \tau, \theta$ and training of SOM models.

- Online phase: real-time computation of $S(x)$ and A_t

Both phases share identical preprocessing and feature mappings:

$$\phi_{train} = \phi_{test}.$$

F. Control Plane: Decision and Mitigation:

The Control Plane maps detection outputs to network actions. Let:

$$e = (src_ip, S(x), t)$$

The decision function:

$$g(e) \rightarrow \text{flow rule}$$

G. Application/Interface Layer: System Integration

An event-driven interface connects the Knowledge Plane to the Control Plane. Alerts are generated when:

$$S(x) > \tau \text{ and } A_t \geq \theta$$

These events are transmitted to the controller, ensuring real-time response and synchronization between analytical inference and control execution. The proposed architecture extends SDN into a five-plane model: Data, Control, Application, Management, and Knowledge, integrating a complete machine learning pipeline for DDoS detection and mitigation.

IV. EXPERIMENTAL RESULTS

A. Scenarios and Experimental Setup

The network comprises six hosts: h1 acts as the HTTP target server; h2 and h3 implement MP and KP, respectively. h4 and h5 generate multi-protocol DDoS traffic (ICMP, UDP, and TCP); and h6, legitimate ping traffic. The physical host executing Mininet assumes the function of the POX controller. The attack script intensity is statistically determined from the empirical packet-count distribution of the input flows. For each malicious flow, the number of generated packets is sampled from a Gaussian distribution centered at three times the original packet count and clipped to the interval $[Q_{90}, 3.Q_{99}]$; ($\approx 125MB/s$). The resulting packets are transmitted without an explicit inter-packet delay, while a 10-s pause is introduced between consecutive flows.

During the offline phase, SOM models are trained using a previously collected dataset [11]. Different grid configurations (10×10, 20×20, and 30×30) are evaluated. This stage aims to identify the most suitable model configuration and to define the detection thresholds. For all “Quantization Error Convergence of SOM” graphs, the X-axis represents Training Epochs, while the Y-axis (QE) represents the Euclidean distance between the input vector and the BMU weight vector.

1) *Description of SOM Training Results:* The Figure 2 illustrates the convergence behavior of the 10×10 SOM, where the quantization error progressively decreases from approximately 3.2–3.4 to nearly 1.5 after about 900 training epochs, indicating stable self-organization and good generalization without significant overfitting. However, despite this convergence, the limited grid resolution restricts its ability to accurately represent complex and highly variable traffic patterns, such as multi-vector DDoS scenarios.

The Figure 3 of The SOM with a 20×20 grid, shows an initial quantization error around 3.2, followed by a smoother and more gradual reduction, converging to approximately 1.0–1.1 after about 2000 epochs. This behavior reflects a richer representation space and improved fine-tuning of neuron prototypes, while the strong alignment between training and validation curves indicates robust generalization. The increased grid dimensionality significantly enhances the model’s ability to discriminate between legitimate and malicious traffic, particularly in detecting subtle and distributed DDoS patterns.

The Figure 4 of the SOM with a 30×30 grid, exhibits an initial quantization error consistent with previous models, followed by a more prolonged and continuous reduction, converging to approximately 0.8–0.9 after about 2800–3000 epochs. The minimal gap between training and validation curves indicates excellent generalization, while the slower convergence reflects a more detailed learning process. This higher grid resolution provides superior representational capacity, enabling more accurate modeling of network traffic and improved detection of subtle patterns associated with sophisticated DDoS attacks.

B. Experimental (inference) Results

In the online phase, four scenarios were evaluated: legitimate ICMP traffic generated by host h6; malicious traffic generated by hosts h4 and h5 using the **attack-generator-mininet.py** script; a hybrid scenario combining legitimate and malicious flows; and a final scenario using sustained ICMP traffic from host h6 to evaluate the **Temporal Evidence Aggregation** module. In this phase, TP and TN represent correctly classified attack and legitimate traffic, while FP and FN correspond to classification errors.

Under Scenario 1 (Figure 5), which consists exclusively of ICMP traffic **considered legitimate**, the framework achieved an accuracy of 77.42%, with TN = 120, FP = 35, TP = 0, and FN = 0, corresponding to a False Positive Rate (FPR) of 22.58%. Since no attack instances are present, Precision, Recall, and F1-score for the attack class are not applicable. Although most legitimate observations are correctly classified, a non-negligible fraction is incorrectly identified as anomalous. This result should be interpreted in the context of the evaluated traffic pattern, which consists of highly repetitive and temporally persistent ICMP echo traffic and differs from the more heterogeneous traffic typically generated by legitimate users. The ablation between temporal aggregation and no temporal aggregation indicates that the increase in false positives is introduced by the temporal aggregation mechanism. The repeated ICMP pattern generates

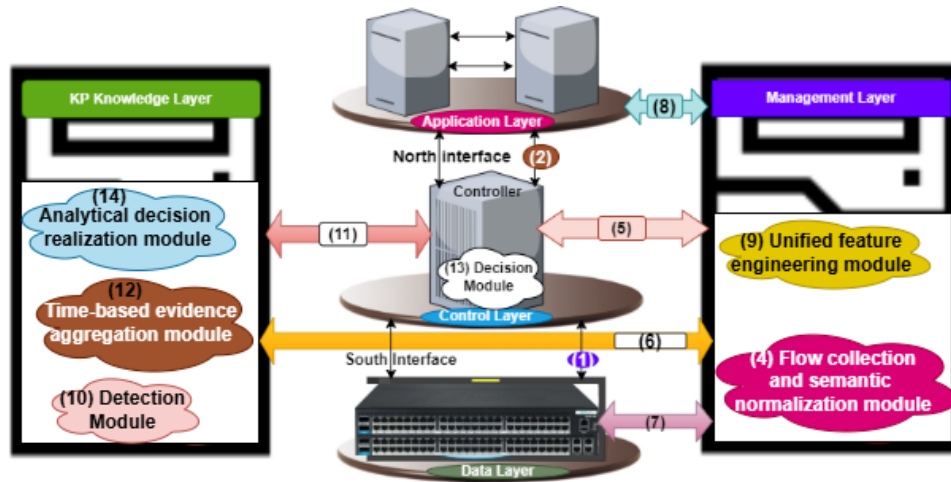


Fig. 1. Proposed Architecture.

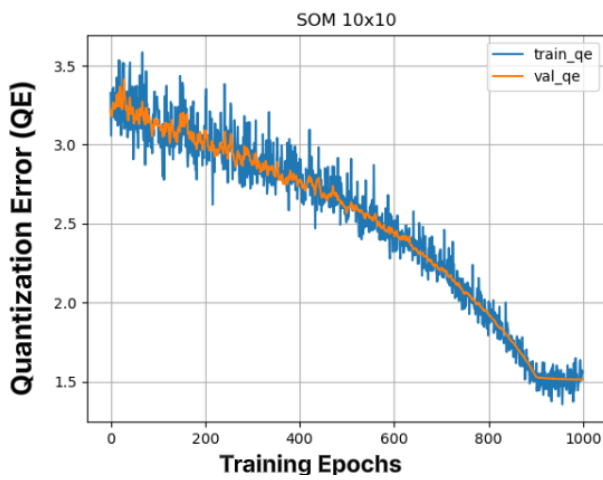


Fig. 2. Som 10x10 training curve.

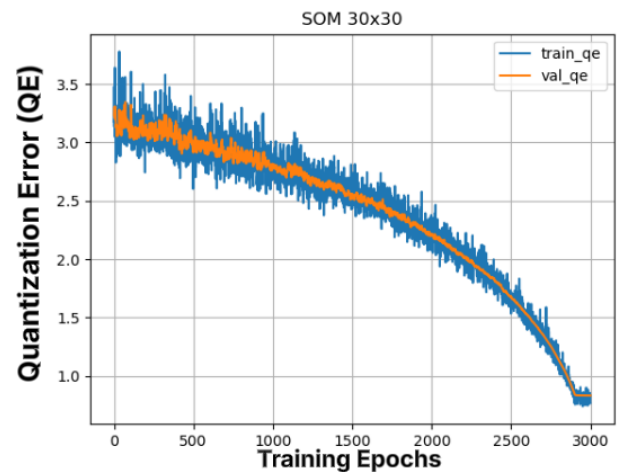


Fig. 4. Som 30x30 training curve.

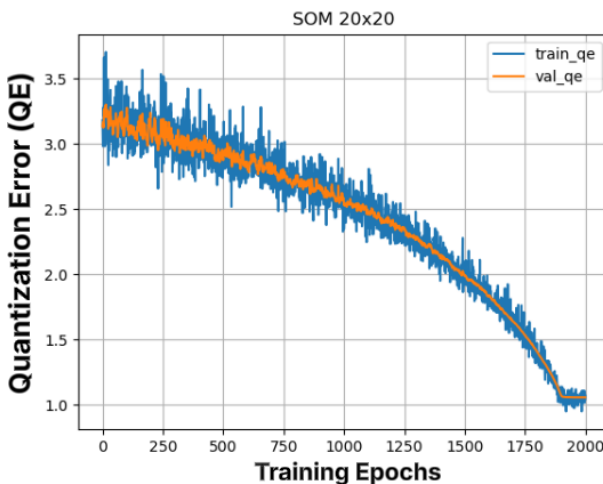


Fig. 3. SOM 20x20 training curve.

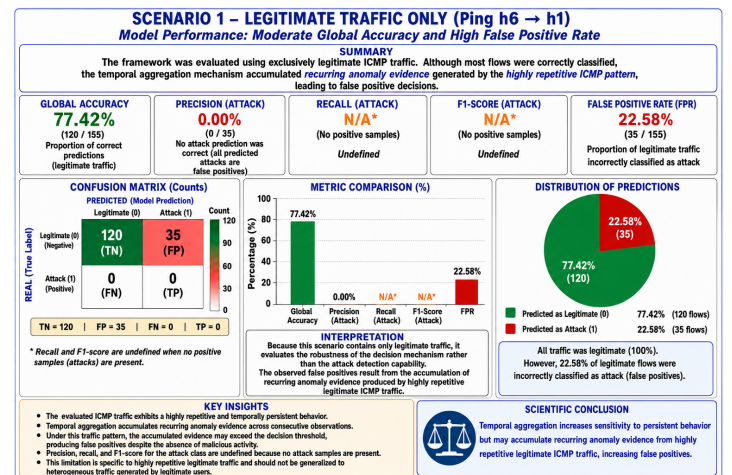


Fig. 5. Graphs of Scenario 1.

Under Scenarios 2 and 3 (Figure 6), corresponding to pure attack and hybrid traffic, respectively, the proposed framework consistently converges to anomaly decisions. In Scenario 2, all 57 attack instances are correctly detected (TP = 57, FP = 0, TN = 0, FN = 0), achieving a 100% Detection Rate; negative-class metrics are not applicable because no legitimate traffic is present. In Scenario 3, the framework

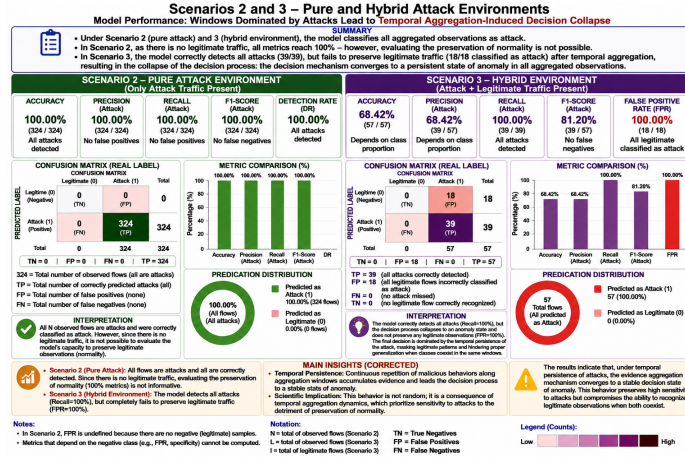


Fig. 6. Graphs of Scenario 2 and 3.

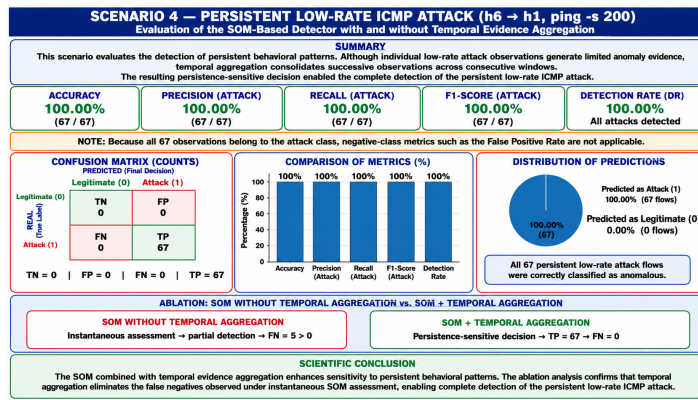


Fig. 7. Graphs of Scenario 4.

yields $TP = 39$, $FP = 18$, $TN = 0$, and $FN = 0$, resulting in 68.42% Accuracy and Precision, 100% Recall, an F1-score of 81.2%, and a 100% False Positive Rate. In this results, the confusion matrices and associated visualizations indicate **a collapse of discriminative capacity caused by temporal aggregation, where high-volume attack traffic dominates the feature space, masks legitimate patterns, and induces a majority-driven constant anomalous classification behavior regardless of traffic heterogeneity.**

Under Scenario 4 (Figure 7), which consists exclusively of a persistent low-rate ICMP attack, the proposed framework correctly classified all 67 malicious flows, yielding $TP = 67$, $FP = 0$, $TN = 0$, and $FN = 0$, with 100% Accuracy, Precision, Recall, F1-score, and Detection Rate. Since the scenario contains exclusively attack instances, negative-class metrics such as the False Positive Rate are not applicable. The ablation between the SOM-based detector with and without temporal aggregation showed that the SOM alone detected only part of the attack flows, resulting in false negatives, whereas the combined SOM–temporal aggregation framework correctly detected all malicious flows. These results provide experimental evidence that temporal aggregation enhances the detection of persistent behavioral patterns by incorporating temporal persistence into the decision process, consequently enabling the complete detection of the persistent low-rate attack evaluated in this scenario. In contrast to Scenario 1, where highly repetitive legitimate ICMP traffic led to the accumulation of recurring anomaly evidence and increased false positives, Scenario 4 demonstrates the beneficial effect of the same persistence-sensitive mechanism for detecting

a genuinely persistent malicious behavior.

V. CONCLUSIONS

This paper proposes a hybrid, multiplanar SDN architecture for DDoS detection and mitigation based on an unsupervised of-line–online pipeline. Detection is performed at three levels through an ensemble of SOMs, combining individual flow analysis, temporal evidence aggregation, and behavioral analysis of coordinated flows originating from different sources. The results demonstrate effective detection under both controlled and high-intensity attack scenarios. The approach also identifies persistent low-rate anomalies that may remain inconclusive when individual flows are analyzed in isolation. The architecture progressively transforms raw data into information, evidence, and behavioral knowledge. Based on this knowledge, it enables autonomous and adaptive mitigation through the SDN controller, with mitigation actions adjusted according to the identified risk level. The current evaluation is limited to a Mininet-based emulation environment. Future work will evaluate the architecture in larger-scale and more realistic SDN environments.

REFERENCES

- [1] DEEPA, V.; RADHA, N. A survey on network intrusion system attacks classification using machine learning techniques. In: IOP Conference Series: Materials Science and Engineering. IOP Publishing, 2021. p. 012036.
- [2] SINGH, Jagdeep; BEHAL, Sunny. Detection and mitigation of DDoS attacks in SDN: A comprehensive review, research challenges and future directions. Computer Science Review, v. 37, p. 100279, 2020.
- [3] CHICA, Juan Camilo Correa; IMBACHI, Jenny Cuatindioy; VEGA, Juan Felipe Botero. Security in SDN: A comprehensive survey. Journal of Network and Computer Applications, v. 159, p. 102595, 2020.
- [4] L. H. d. Melo, G. d. C. Bertoli, M. Nogueira, A. L. d. Santos and L. A. Pereira, "Anomaly-Flow: A Multi-Domain Federated Generative Adversarial Network for Distributed Denial-of-Service Detection," in IEEE Network, vol. 40, no. 2, pp. 269-277, March 2026
- [5] YUREKTEN, Ozgur; DEMIRCI, Mehmet. SDN-based cyber defense: A survey. Future Generation Computer Systems, v. 115, p. 126-149, 2021.
- [6] Islam, Md Jahidul and Rahman, Anichur and Kabir, Sumaiya and Khatun, Ayesha and Pritom, Ahmed Iqbal and Chowdhury, Mehrab Zaman. Sdot-nfv: a distributed sdn based security system with IoT for smart city environments. GUB Journal of Science and Engineering, v.110, p. 27-35, 2020
- [7] CLARK, David et al. FARA: Reorganizing the addressing architecture. In: Proceedings of the ACM SIGCOMM workshop on Future directions in network architecture. 2003. p. 313-321.
- [8] Túlio A. Pascoal, Iguatemi E. Fonseca, Vivek Nigam, Slow denial-of-service attacks on software defined networks, Computer Networks, Volume 173, 2020, 107223, ISSN 1389-1286,
- [9] A. Saidane, A. E. Kamel and H. Youssef, "Towards DDoS-aware Routing in SDN using Cross-layer Knowledge Transfer," 2023 International Conference on Innovations in Intelligent Systems and Applications (INISTA), Hammamet, Tunisia, 2023, pp. 1-6,
- [10] Ahuja, Nisha and Singal, Gaurav and Mukhopadhyay, Debajyoti. DDOS attack SDN dataset. Mendeley Data, Bennett University. v.1. p. 17632, 2020
- [11] S. Liu, H. Fukuda and P. Leger, "Real-time DDoS Attack Defense System in SDN Using LSSOM," 2023 26th Conference on Innovation in Clouds, Internet and Networks and Workshops (ICIN), Paris, France, 2023, pp. 69-73.
- [12] S. Marleau, P. Rahman and C. Lung, "DDoS Flood Detection and Mitigation using SDN and Network Ingress Filtering - an Experiment Report," 2024 IEEE 4th International Conference on Electronic Communications, Internet of Things and Big Data (ICEIB), Taipei, Taiwan, 2024, pp. 67-72,
- [13] S. N and M. PA, "SDN-Enabled Networks: A Deeper Learning-Based Echo State Neural Network for Cyber Threat Detection," 2024 7th International Conference on Circuit Power and Computing Technologies (ICCPCT), Kollam, India, 2024, pp. 1356-1360,
- [14] Jie Ma, Wei Su, Collaborative DDoS defense for SDN-based AIoT with autoencoder-enhanced federated learning, Information Fusion, Volume 117, 2025, 102820, ISSN 1566-2535,
- [15] THORIG, Ibrahim; ZAHILAH, Raja; SIRAJ, Maheyyah Md. A Hybrid Autoencoder-Deep Forest Model for Ddos Detection in Software-Defined Networks. In: 2025 2nd International Conference on Innovations in Engineering, Science and Technology for Sustainable Development (ICEST). IEEE, 2025. p. 1-4.