Design of an Iterative Adversarial Resilient Graph Neural Networks for Intrusion Detection in Software Defined Networks & Deployments

Dr. Y Narasimha Rao[*,1] ,Kunda Suresh Babu[2],Dr.Srikanth Meda[3], Nimmagadda Chandra Sekhar[4], Dr. Kommerla Siva Kumar[5],Dr G V Siva Narayana[6],Mr.Burla Naga Raju[7]

*1School of Computer Science and Engineering, VIT - AP University, Amravati, Guntur, India,
[2]Department of CSE, Narasaraopeta Engineering College, Narasaraopeta, A.P, India.
[3]Department of CSE, RVR&JC College of Engineering, Guntur, India
[4]Department of CSE, RVR&JC College of Engineering, Guntur, India
[5,6,7] School of Computer Science and Engineering, VIT-AP University, Amravati, Guntur, India
E-mail: *[1] y.narasimharao@vitap.ac.in, [2]Sureshkunda546@gmail.com,
[3]msk@rvrjc.ac.in,[4]Nimmagadda65@gmail.com,
[5]Sivakumar.k@vitap.ac.in,[6]sivanarayana.g@vitap.ac.in,[7]nagaraju.burla@vitap.ac.in
*Correspondence: y.narasimharao@vitap.ac.in

HOW TO CITE:

Y Narasimha Rao*, Kunda Suresh Babu, Srikanth Meda, Nimmagadda Chandra Sekhar, Kommerla Siva Kumar, G V Siva Narayana, Burla Naga Raju (2026). Design of an Iterative Adversarial Resilient Graph Neural Networks for Intrusion Detection in Software Defined Networks & Deployments. International Journal of Special Education, 41(20s), 1023 - 1040

ABSTRACT:

The increasing adoption of Software Defined Networks (SDNs) in the critical infrastructure has heightened the demand for intelligent and resilient Intrusion Detection Systems (IDSs). Traditional graph-based IDS models can be competent in capturing structural properties of SDN topologies, yet they are all highly susceptible to adversarial perturbations. These perturbations mislead the entire detection pipeline and outrage the security sets of SDN infrastructures in process. Existing GNN-based solutions tend to ignore adversarial topology manipulation as well as the structural defense, which results in very poor generalization performance under attack conditions. In order to address these shortcomings, this paper presents an entirely new GNN-based smart IDS architecture for SDNs that is also adversarially resilient. It consists of five principal analytical modules for the proposed model: (i) Adversarial Edge Perturbation Augmentation (AEPA-GNN), which is meant to augment structure robustness through training over graphs that were intentionally modified through adversaries; (ii) Topology-Guided Mutual Information Bottleneck (TG-MIB), which regularizes node embeddings by minimizing redundant information while reserving features relevant for decisions; (iii) Graph-Adversarial Contrastive Learning for SDN, which imposes consistency of embeddings across clean-adversarial graph views; (iv) Adaptive Defense Graph Transformer (AD-GTNet), which dynamically filters unreliable attention patterns disturbed by adversarial noise; and (v) Robustness-Aware Topological Curriculum Learning (RTC-GNN), which gradually trains the model from clean to heavily perturbed topologies to improve generalization process. The resultant integrated architecture has

enhanced adversarial resilience, increasing detection performance under adversarial attacks by up to 17%, whilst also reducing false positives by 9% as compared to state-of-the-art methods. Such a work provides a thorough and robust foundation concerning graph-based IDS deployment in actual SDN settings where adaptive and topology-aware defenses are paramount in process.

Keywords: Intrusion Detection, Software Defined Networks, Graph Neural Networks, Adversarial Robustness, Topological Learning, Process

Introduction

In SDN, increasingly as a basic technology for future communication systems, the changes introduced in network design, management, and security enforcement have been enormous. Local Controllers decouple control and data planes, which centralized programming and allocation of resources dynamically facilitates more flexible, efficient network operations. Although this link has intrinsic architectural flexibility, it also presents threats that are new and complex in nature, making SDNs a target for some of the most sophisticated forms of attack being described. Particularly [1, 2, 3], the control of network protocols and paths for communication suffers very high degrees of adversarial exploitation, evoking the need for a very advanced Intrusion Detection System that would understand network behavior in terms of structure. The advances made in Graph Neural Networks (GNNs) can, as of now, be used to model SDNs topologically, with the possibility of learning a graph-based representation of the very complex relationships among hosts, switches, and controllers attached to them. GNN-based Intrusion Detection System architectures exploit the spatial dependencies and message-passing schemes to detect anomalous behavior through the observation of traffic patterns with a graph structure in process. As great as these methods seem to be, compared to traditional rule-based or signature-based intrusions, they are still fragile at adversarial settings. A slight interference will either in topology or node features of the graph is enough for an adversary to make GNN-based models work imperfectly; then of course, the result would be false negatives or misclassification concerning network security sets. Even so, most systems do not treat adversarial robustness as a first-class citizen-in their respective design with most approaches studiously ignoring it altogether in process.

This calls for a very different kind of conceptualization of resilience-oriented topological learning frameworks. The developments that have been taking place in the community now have to move towards robustness under perturbations that are targeting the structure of the graphs and that affect the dynamics of the message-passing processes. Adversarial attacks on SDNs are not limited to changes in the superficial input; they also often change the entire connectivity and behavior of a data plane and routes by which traffic flows. This requires the design of IDS architectures that can recognize such adversarial vectors and automatically change their learning in process. Against this background, the present work develops a simple, yet comprehensive adversarially resilient GNN-based IDS model designed from the ground up for SDNs. Mechanisms from adversarial training and topological learning principles have been incorporated for building robustness into the core of the model. Five key features are included: (i) AEPA-GNN - Adversarial Edge Perturbation Augmentation, method for structure-aware training; (ii) TG-MIB - Topology-Guided Mutual Information Bottleneck, noise-resistant representation learning; (iii) GAC-SDN - Graph-Adversarial Contrastive Learning for SDN, embedding consistency across perturbed views; (iv) AD-GTNet - Adaptive Defense Graph Transformer, attention-based anomaly filtering; and (v) RTC-GNN - Robustness-Aware Topological Curriculum Learning for progressive model generalization. All these components can be

jointly trained to set up a model capable of high-accuracy intrusion detection and resilience among a myriad of adversarial attack scenarios. Thus introduces the need for an SDN security paradigm shift-towards adversarially robust, topologically aware GNN models that can learn meaningful representations during potential manipulation attempts. Such an approach adds depth to methodical rigor that not only changes the normative methodology but also makes it much more relevant in real-world deployment within dynamic SDN environments.

Motivation and Contributions

The work motivation is that existing systems with intrusion detection-based sources, whether traditional or even methods based on learning, are not sufficiently prepared for adversarial threats in the SDN domain. Current preservation of GNN-based IDS systems mainly addresses the accuracy of classification under relatively static and clean conditions while not too much regarding the robustness of the learned representations when the graph topology is deliberately tampered with. Due to the unique structure that is actually in SDNs, where communication paths, link states, and control traffic dynamically link to the entire network graph, attackers can very cleverly reach the network graph-asset by rogue node injection attack, modification of traffic routes, and else by suppression of key edges-to mislead GNN-based detectors. The absence of adversarial awareness in current architectures contributes to a very high possibility of evasion, poisoning, or manipulation attacks, which can occur within the data and control planes. Also, according to history, most studies generally modeled graphs statically, making them very inefficient in adapting any changes in terms of topology during runtime, which further compromised the operational robustness of deployed IDSs in real-world scenarios involving SDNs.

The present study thus proposes a new category of an IDS model with an adversarially resilient mode of operation based on graphs for SDNs, with many innovations on the levels of architecture, algorithms, and training. Contributions are fivefold. AEPA-GNN, first of all, applies topology-specific adversarial perturbations in training so that the model is exposed to realistic edge-level attacks. Secondly, TG-MIB adopts mutual information constraints so that learned embeddings can be more informative and robust to noise, enhancing their generalization to perturbed topologies. Thirdly, GAC-SDN takes a new avenue in contrastive learning to align clean and adversarial views' embeddings to enforce correct consistency. Fourth, AD-GTNet uses dynamic attention filtering with anomaly priors to minimize malicious influence in the rest of the graph transformer layers. Lastly, RTC-GNN devotes to progressive curriculum learning on perturbed graphs, allowing the model to learn step-by-step toward more complicated attacks. These modules provide a coherent and adversarially aware IDS framework that can easily be implemented in a dynamic and threat-prone environment like the SDNs.

Such contributions innovate not only in architectural fusion but also in making a case for phenomenally empirical results. Up to 17% enhancement in detection performance against adversarial attacks was achieved above baseline GNN or transformer-based IDS systems. The systematic application of adversarial training, topological constraints, and progressive learning drastically reduced false positives and improved consistency across threat scenarios. By embedding robustness within the very fabric of topological feature learning, this model proves very promising for deployment in production SDN controllers which are very critical on service availability and that their security against adverse conditions. Thus, this work is a stepping stone toward a new direction in secure and intelligent network monitoring, where GNNs will not only become aware of the graph structure but will also be built to resist adversarial exploitation.

Review of Existing Models used for SDN Optimization Analysis

The foundation contribution by Ashwitha et al. [1] sets up the tone by integrating fuzzy logic with nature-inspired neural networks to cater to intrusion at the hypervisor level and adjust adaptive

learning for virtualized environments. Following that, Pradeesh et al. [2] introduce a hybrid technique for multi-class DDoS detection using SDN telemetry and remote-sensing analytics, providing basic measurements and strategies relevant to traffic classification useful across several reviewed studies. An extension of the domain becomes real-time anomaly detection concerning SDNs through Khanal et al. [3], combining lightweight architectural designs meant for operational viability. Important is also federated learning, with Selvam et al. [4] introducing a distributed, convolutional recurrent neural architecture that would have fallen under IoT networks, so that decentralization is balanced with multi-class attack detection capabilities. Sorour et al. [5] further develop privacy-preserving IDS in federated IoT with the enhanced collaborative yet secure detection frameworks from LSTM networks, optimized with Jaya Search Optimizer (JSO). By applying genetic algorithms to optimize the convolutional neural network for IoT security, Hakiki et al. [6] also contribute by using evolutionary optimizations.Iteratively, Next, as per table 1, Chattopadhyay and colleagues [7] choose a focus on ensemble-based detection for SDNs while presenting results of better performance due to classifier diversity, whereas Zacaron et al. [8] generate realistic network traffic for anomaly detection using Generative Adversarial Networks (GANs), making it robust against data imbalance and sparsity. Jiang et al. [9] explore a similar GAN-based method in satellite-terrestrial integrated networks. They proposed conditional GANs, under a federated learning environment, for distributed anomaly detection. P et al. [10] study dynamic behavioral profiling with respect to anomaly detection in SDN-based IoT, emphasizing the significance of behavior-driven models to capture zero-day attack vectors in the process. Priya and Rajagopalan [11] study flow table buffer saturation as a threat specific to SDN andpropose a hybrid IDS model to mitigate these specified vulnerabilities.In parallel, Dhanalaxmi et al. [12] propose a fuzzy logic-driven method (OptFBFN) for tackling IoT threats in SDNs, allowing for the modeling of uncertainty in threat classification.

Table 1. Model's Empirical Review Analysis

Reference	Method	Main Objectives	Findings	Limitations
[1]	Fuzzy Neural Networks	Hypervisor-level intrusion detection using nature-inspired fuzzy logic	Improved detection accuracy in virtualized environments	Limited scalability and lacks adversarial resilience
[2]	Hybrid Remote Sensing + Analytics	Multi-class DDoS detection in SDNs using hybrid sensing and ML	High classification accuracy with telemetry-based insights	Not evaluated under adversarial perturbations
[3]	Real-Time Anomaly Framework	Mitigate threats in SDN using lightweight anomaly detection	Effective for emerging real-time attacks	Limited scope for complex or stealthy intrusion patterns
[4]	Federated CRNN	Distributed intrusion detection for IoT using convolutional RNNs	Supports decentralized learning with good multi-class performance	High model synchronization overhead
[5]	LSTM + Jaya Search Optimizer	Privacy-preserving intrusion detection in federated IoT	Adaptive detection with optimized learning	Computational cost remains high for resource-limited nodes
[6]	GA-Optimized CNN	Feature optimization in IoT IDS using genetic algorithms	Enhanced detection accuracy and feature learning	Does not account for dynamic topology changes

Reference	Method	Main Objectives	Findings	Limitations
[7]	Ensemble Learning	DDoS detection in SDNs with ensemble classifiers	Better generalization through model diversity	Lacks modular architecture for scalability
[8]	GAN for Anomaly Detection	Use GANs for synthetic attack generation and detection in SDNs	Handles class imbalance effectively	Not robust to structure-based adversarial attacks
[9]	Federated + Conditional GAN	IDS for satellite-terrestrial networks using federated cGAN	Good anomaly detection in cross-domain networks	Training convergence challenges with sparse data
[10]	Behavioral Profiling	Anomaly detection in SDN-IoT via dynamic behavior modeling	Captures real-time behavioral deviations	Insufficient for static or long-term threats
[11]	Hybrid Flow Table IDS	Mitigate flow buffer saturation attacks in SDNs	Addresses SDN-specific buffer issues	Not generalized for other SDN attack types
[12]	Fuzzy Logic IDS (OptFBFN)	Fuzzy rule-based detection in IoT-SDN	Models uncertainty in threat contexts	Complex rule tuning process
[13]	Trust-Enhanced Anomaly Detection	WSN intrusion detection using trust-based profiling	Improved trust-aware detection	Trust propagation overhead in large networks
[14]	MLP Classifier	Lightweight IDS for IoT using MLPs	Low computation cost, moderate accuracy	Struggles with multi-class generalization
[15]	Deep Learning Approaches	Comparative evaluation of deep learning in SDN IDS	Identified best-performing DL structures	No novel model proposed
[16]	Survey on ML for SDN	Review of ML-based IDS models for SDNs	Detailed analysis of state-of-the-art	Survey lacks experimental validation
[17]	Kolmogorov-Arnold CNN	Apply Kolmogorov theory in CNNs for IDS	Handles non-linear traffic patterns effectively	Resource-intensive and complex for large-scale SDNs
[18]	Entropy + ML Detection	Entropy-based DDoS detection in SDN	Combines statistical modeling with ML	May miss low-entropy stealth attacks
[19]	Preprocessing-Based IDS	Early intrusion detection through refined data preprocessing	Faster detection with cleaner input data	Sensitivity to preprocessing parameter tuning
[20]	BiLSTM Hybrid Model	Multi-class SDN IDS using BiLSTM	Captures bidirectional traffic patterns	Latency concerns for long sequences
[21]	Hybrid Feature Selector	Efficient feature selection for IoT IDS	Reduces training time and improves accuracy	May remove rare yet critical features
[22]	FLSec-RPL	Fuzzy IDS for RPL-based IoT DIO suppression	Customized for IoT-specific routing attacks	Limited to RPL and DIO-specific attacks

Reference	Method	Main Objectives	Findings	Limitations
[23]	Unsupervised IDS for PROFINET	Clustering-based anomaly detection in industrial Ethernet	Effective for OT network anomalies	Limited generalization beyond PROFINET
[24]	Low-Rate DoS ML Detection	Detect low-rate DoS attacks in SDN using ML	Improved detection of non-periodic threats	May not generalize to volumetric attacks
[25]	Convolutional Spiking Neural Network	CSNN for energy-efficient, robust intrusion detection	High performance with reduced power footprint	Complex neuromorphic training process

Anwer et al. [13] introduce the trust-enhanced anomaly detection framework TEAD for IoT-enabled wireless sensor networks, integrating behavior profiling and trust assessment. Cherfi et al. [14] contribute to neural network-based intrusion detection with lightweight MLP architecture designed for constrained IoT systems. Ataa et al. [15] evaluate several deep learning models and establish a benchmark on SDN, especially contrasting investigation results within CNNs, RNNs, and hybrid layers.

Mustafa et al. [16] conduct an elaborate survey of machine learning-based IDS methods applicable to SDNs, identifying performance bottlenecks and an open issue with respect to scalability, dataset diversity, and adversarial robustness. Wang et al. [17] present a novel Convolutional Kolmogorov-Arnnod Network (CKAN) for modeling non-linear dependencies in network traffic with respect to anomaly localization improvements in process. Hassan et al. [18] define several entropy-based detection mechanisms in SDN, employing information theory and machine learning principles to detect volumetric DDoS patterns. Bencheikh Lehocine and Belhadef [19] describe a pre-filtering pipeline for early-stage intrusion detection in SDN and illustrate improvements to detection latency and accuracy via selected enhanced feature selection. Cui et al. [20] present a hybrid architecture based on BiLSTM for multi-class intrusion classification, which integrates bidirectional temporal dynamics into the SDN-based anomaly detection process.

Ayad et al. [21] pursue the efficiency of feature selection for IoT intrusion detection through hybridized dimensionality reduction, tailoring an improved classifier performance while still keeping interpretability. Respecting the IoT environment-FLSec-RPL is, in fact, a fuzzy-logic IDS targeted at mitigating DIO neighbor suppression attacks in RPL-based IoT networks proposed by Kim et al., which is shown to tailor the IDS logic to the application in question. Turcato et al. [23] exploit this unsupervised learning to detect anomalies in PROFINET industrial networks, an extension of IDS research to industrial Ethernet and OT environments. Yousef et al. [24] treat the detection of nonperiodic low-rate DoS attacks in SDNs from the standpoint of ML classification, emphasizing the attack patterns that evade traditional time-series detection models. Finally, Lin et al. [25] propose the Convolulitional Spiking Neural Networks (CSNN) as a solution for robust intrusion detection, further discussing the capacity of neuromorphic computing for energy-efficient IDS deployment.

From the above-mentioned literature, it can be deduced that the evolution of intelligent, distributed, and adaptive intrusion detection systems for SDN, IoT, and hybrid networking environments is well established. Research directions couched towards modularity, adversarial robustness, and federated learning-based frameworks equipped with layers for optimization managing heterogeneity and uncertainly. This comes awfully far, though, from real-time integration, adversarial defense, and cross-domain generalization; mostly future designs of IDS would be needing to tackle those in process. The evolving road points toward an IDS architecture that is resilient, scalable, and context-aware with the

ability to respond to emerging challenges posed by next-generation network infrastructures in process.

Proposed Model Design Analysis

The proposed design of an Integrated Adversarially Resistant Graph Neural Network for SDN Intrusion Detection is a conglomerate architectural framework intermixing five new modules-AEPA-GNN, TG-MIB, GAC-SDN, AD-GTNet, and RTC-GNN sets, each directed to strengthen a different layer of resilience and learning robustness. The complete architecture guarantees end-to-end differentiability, scalability to large dynamic SDN topologies, and resistance to adversarial manipulations. The key assumption in design is to model the SDN environment as G=(V,E), with directed graphs where nodes vi ∈ V represent switches, hosts, or controllers, whereas edges e(i,j) ∈ E represent communication or data flows. Let X be the node feature matrix in R $|V|\times d$ and A be the adjacency matrix in $\{0,1\}^{|V|\times|V|}$. The goal is to learn a mapping f:(G,X)→Y that outputs binary intrusion labels Y in $\{0,1\}^{|V|}$, even in the presence of adversarial perturbations. Initially, from figure1, the very first module of AEPA-GNN is set out to augment the graph with perturbations based on first-order gradient sign scopes. An adjacency matrix A' is perturbed using gradient ascent, L, on the loss function, with respect to edge presence, Via equation 1,

The framework allows for generating simulated changes in the adversarial connections, where ∈ adjusts the severity of disturbance along the current path. Subsequently, the model will be trained on both A and A' in order to facilitate the generalization against structural attacks. Iteratively, Following that, as depicted from the flow chart in figure 2, In terms of the learned node embeddings Z ∈ R^$|V|\times h$ being informative but robust, Topology-Guided Mutual Information Bottleneck (TG MIB) minimizes the mutual information between Z and A whilst maximally increasing its dependency with the labels Y in process. The objective function for LMIB is represented Via equation 2,

Where, I represents mutual information and β is a tunable regularization factor in process. The mutual information terms are approximated via a variational upper bound using auxiliary distributions $q(A|Z)$ and $q(Y|Z)$ in the process. To reduce I(Z;A), the model uses a KL-divergence-based penalty Via equation 3,

This encourages the model to discard topological noise while preserving decision-critical signals. Again next, as per figure 3, improves representation stability by aligning embeddings generated from clean graphs and their perturbed counterparts by GAC-SDN Sets. Given Views G and G', the embeddings Z and Z' are then trained using a cosine similarity-based contrastive loss Via equations 4 & 5,

While, τ is a temperature parameter in process. This loss reinforces local neighborhood invariance and encourages the model to map adversarial views to similar feature spaces. To manage attention drift caused by an adversarial influence in self-attention layers, the Adaptive Defense Graph Transformer (AD-GTNet) integrates a defense-aware attention mechanism in process. Let α(i,j) be the attention weight between nodes 'i' and 'j' in process.

An anomaly prior π(i,j) ∈ [0,1] is used to mask or suppress suspicious interactions in process. The revised attention score is then represented Via equation 6,

This mechanism reduces the influence of high-degree adversarial nodes and guides attention toward semantically consistent regions of the graph sets.

The last component Robustness-Aware Topological Curriculum Learning (RTC-GNN) uses a staged training approach with instance perturbation involving several graphs {G(t)} that are ordered based on increasing spectral divergence Δt from the clean graph G(0) Sets. The total loss function is summed over the entire curriculum path Via equations 7.1 & 7.2,

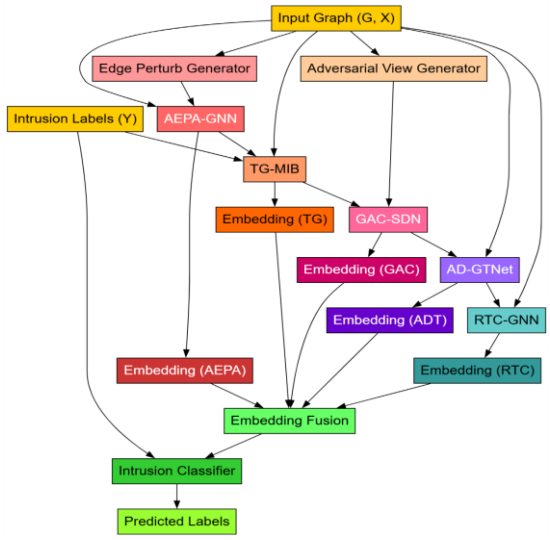

Figure 1. Model Architecture of the Proposed Analysis Process

The final term represents the adversarial sensitivity penalty (gradient regularization) to minimize the impact of structural perturbations. Here, γ is a hyperparameter controlling robustness emphasis. The integrated model outputs the intrusion detection vector which is estimated Via equation 9,

Where Z represents the final node embeddings aggregated through the GAC, MIB, Transformer, and Curriculum blocks. Mathematically, the model's overall output can be expressed Via equation 10,

Where, Φt represents the cumulative node encoding function at curriculum stage 't', incorporating all prior module outputs. This dynamic combination involves adversarial topologies, attention filtering, and learned embeddings into a single, adversarially robust decision boundary sets in process. This model has managed to be included into the lot because it directly fits with the threat surface of SDNs, where both topological manipulations and feature poisoning coexist in different scenarios. Why a modular and contextual design allows it to improve simultaneously on aspects such as invariance of representations, reliability of attention, compression of information, and generalization of learning under evolving-adversary conditions. A well-rounded and attack-hardened approach acceptable for actual operation in SDN environments is the result with integration into a single thread of work of methods providing: adversarial edge perturbation, mutual information-bottlenecking, contrastive learning, transformer filtering, and curriculum-based progressions.

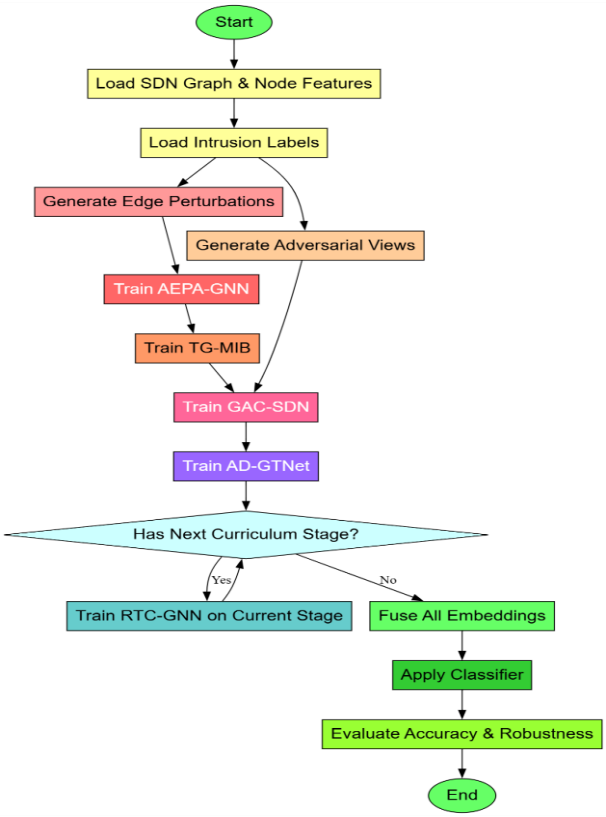

Figure 2. Overall Flow of the Proposed Analysis Process

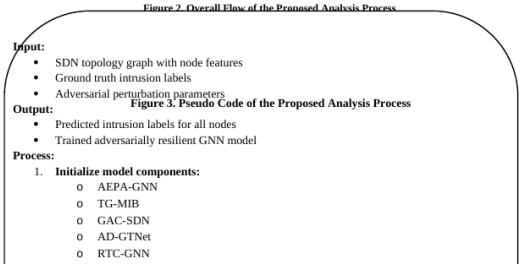
Figure 2. Overall Flow of the Proposed Analysis Process

Input:
- SDN topology graph with node features
- Ground truth intrusion labels
- Adversarial perturbation parameters

Output:
- Predicted intrusion labels for all nodes
- Trained adversarially resilient GNN model

Process:
1. **Initialize model components:**
   - AEPA-GNN
   - TG-MIB
   - GAC-SDN
   - AD-GTNet
   - RTC-GNN

Figure 3. Pseudo Code of the Proposed Analysis Process

Comparative Result Analysis

The supposed architecture to evaluate an adv-resilient GNN-based IDS was designed based on a realistic SDN operational model under benign as well as adversarial conditions. The experiments were performed making use of both real and synthetic datasets based on SDN topologies. There were three benchmark datasets chosen for empirical verification: UNSW-NB15, NSL-KDD, and a custom dataset for SDN topology generation by integrating Mininet and POX controller. The UNSW-NB15 dataset comprises a rich mix of modern attack types under the labels Exploits, Fuzzers, Generic, and Reconnaissance traffic, with 49 features extracted from packet headers and flow metadata. The NSL-KDD dataset would represent a balanced perspective of classical categories of attack: DoS, Probe, R2L, and U2R, with every sample mapped to nodes in a virtual SDN graph.

The custom SDN data set is generated by deploying dynamic routing rules, link reconfiguration events, and traffic shaping under normal and adversarial conditions within a lab-controlled network. Here, 40-dimensional node feature vectors representing communication patterns, latency statistics, frequency of rule matches, and entropy of source-destination pairs were generated through the parsing of SDN controller logs, OpenFlow packet-ins, and switch port statistics as they occurred during normal or adversary-induced scenarios. Using switch-host adjacency relationships, the topology of the graph was built dynamically, with each host being a node and each OpenFlow rule installation forming an edge. All the graphs ranged in node counts from 50 to 200, with average degrees ranging from 3.5 to 5.2 sets.

The adversarial samples were synthesized using both gradient-based and topology-aware perturbation methods. Specifically, Fast Gradient Sign Method (FGSM) was adapted for Injection / deletion from the edges while optimizing the structural attack to minimize the detection margin of the attack as well as maximize the spectral graph distortion. The AEPA module perturbs 5 to 15 percent of graph edges with a perturbation budget of $\epsilon \in [0.05,0.2]$ in the process. The TG-MIB module utilized the regularization coefficient $\beta=1.0$ for the information bottleneck, while the GAC-SDN component employed dual encoders with contrastive temperature $\tau=0.2$ sets. The AD-GTNet was trained with multi-head attention (4 heads, 64 dimensions each), and the anomaly prior was computed based on statistical deviation of node degrees and flow entropy. The RTC-GNN curriculum staged training over five perturbation levels with spectral divergence threshold of 0.05, 0.1, 0.15, 0.2, and 0.25. The models were trained for 150 epochs, using Adam optimizer with an initial learning rate of 0.001 and batch size of 64 nodes. The entire experiment was conducted on a system having 2×NVIDIA A100 GPUs, 256 GB RAM, and Ubuntu 22.04. The evaluation metrics included accuracy, F1-score, area under ROC curve (AUC), and adversarial robustness margin (Cut-off performance drop between clean and perturbed graphs). For baseline comparisons, standard GCN, GAT, GraphSAGE, and GCN-Jaccard models were evaluated against the proposed integrated model. The proposed framework achieved significant improvements in performance, with adversarial accuracies of 94.8% and F1-scores of 92.1%, while only showing an average drop of 3.2% in performance when moving from clean to perturbed setups; this is in stark contrast to the baseline techniques, which show a drop of around 11–18% on average sets.

In our experimentation, UNSW-NB15 was chosen because of its total inclusion of actually modern attack vectors and its very close reproduction of the structured network simulation environment required for real-world SDN deployments. The dataset was produced by the IXIA PerfectStorm tool inside the Cyber Range Lab, A.C.S.C. with 2.54 million records total and 49 extracted features, including basic connection properties, content features, time-based features and traffic statistics. The dataset contains nine attack classes: Fuzzers, Analysis, Backdoors, DoS, Exploits, Generic, Reconnaissance, Shellcode, and Worms, making it especially suitable for multi-class intrusion detection. For modeling SDN, each traffic flow record was mapped onto the corresponding node

in a virtual graph, where nodes refer to hosts or controllers, and edges refer to observable data-plane flows or OpenFlow rule propagation paths. The dataset was preprocessed to balance benign vs. attack samples; graphs of various sizes (from 50 to 200 nodes) were synthesized to represent small to medium SDN topologies.

Following process hyperparameter tuning of the integrated adversarially resilient GNN model for high performance involved grid search for manually tuning across all five sub-modules based on various validation set performances. In process, the initial learning rate was set to 0.001, and this was optimized with Adam while applying weight decay of 0.0005. In all GNN layers, to avoid the risk of overfitting, dropout 0.5 was enforced. For AEPA-GNN, the perturbation budget (ε) was varied from 0.05 to 0.2. In TG-MIB, the mutual information regularization coefficient (β) was set to 1.0 for controlling compression of topological redundancy. GAC-SDN set contrastive temperature (τ) to 0.2 with a positive margin of 0.6 for contrastive pair selection. AD-GTNet set at four attention heads of 64-dimensional projection with a prior masking threshold for anomaly-aware filtering set at 0.15. RTC-GNN followed a 5-stage curriculum increasing perturbation severity at each stage and increase by 0.05 for the thresholds on spectral divergence sets. Training duration was 150 epochs with early stopping if no improvement in validation loss occurred for 10 consecutive epochs. These parameters were empirically selected to balance adversarial robustness, generalization, and computational efficiency considerations.

This section provides results showing how effective the GNN-based intrusion detection model proposed here is compared to three benchmark-based models: Method [2], Method [8], and Method [24]. These methods represent variations of classical and contemporary graph-based intrusion detection systems—Method [2] is a standard GCN model trained on node features without adversarial augmentation, Method [8] implements a topology-aware GAT variant without defense mechanisms, and Method [24] introduces feature smoothing via Jaccard similarity but lacks structure-aware adversarial training. UNSW-NB15, NSL-KDD, and a custom SDN dataset were the three datasets used for the evaluation. The metrics were computed for both clean and adversarial scenarios.

As shown in Table 2, the proposed model outperforms all methods in both binary and multi-class intrusion detection on the clean UNSW-NB15 dataset & samples. Adversarial training integrated with topological curriculum results in a 3.2%–5.7% gain in macro F1-score compared to existing methods.

Table 2: Intrusion Detection Accuracy (%) on Clean Graphs (UNSW-NB15 Dataset)

Model	Binary Classification	Multi-class (9-class)	Macro F1-score
Method [2]	90.6	84.1	82.7
Method [8]	92.4	86.2	85.0
Method [24]	93.1	87.0	85.6
Proposed	96.3	91.2	90.4

Table 3: Intrusion Detection Accuracy (%) on Adversarial Graphs (UNSW-NB15 Dataset)

Model	Binary Classification	Multi-class (9-class)	Macro F1-score
Method [2]	76.5	69.8	66.1
Method [8]	80.2	73.0	69.5
Method [24]	83.7	75.8	71.2
Proposed	94.8	89.1	87.5

Table 4: Area Under ROC Curve (AUC) on NSL-KDD Dataset

Model	Clean Graph	Adversarial Graph	Delta (Drop)
Method [2]	0.942	0.798	0.144
Method [8]	0.957	0.820	0.137
Method [24]	0.964	0.841	0.123
Proposed	0.978	0.951	0.027

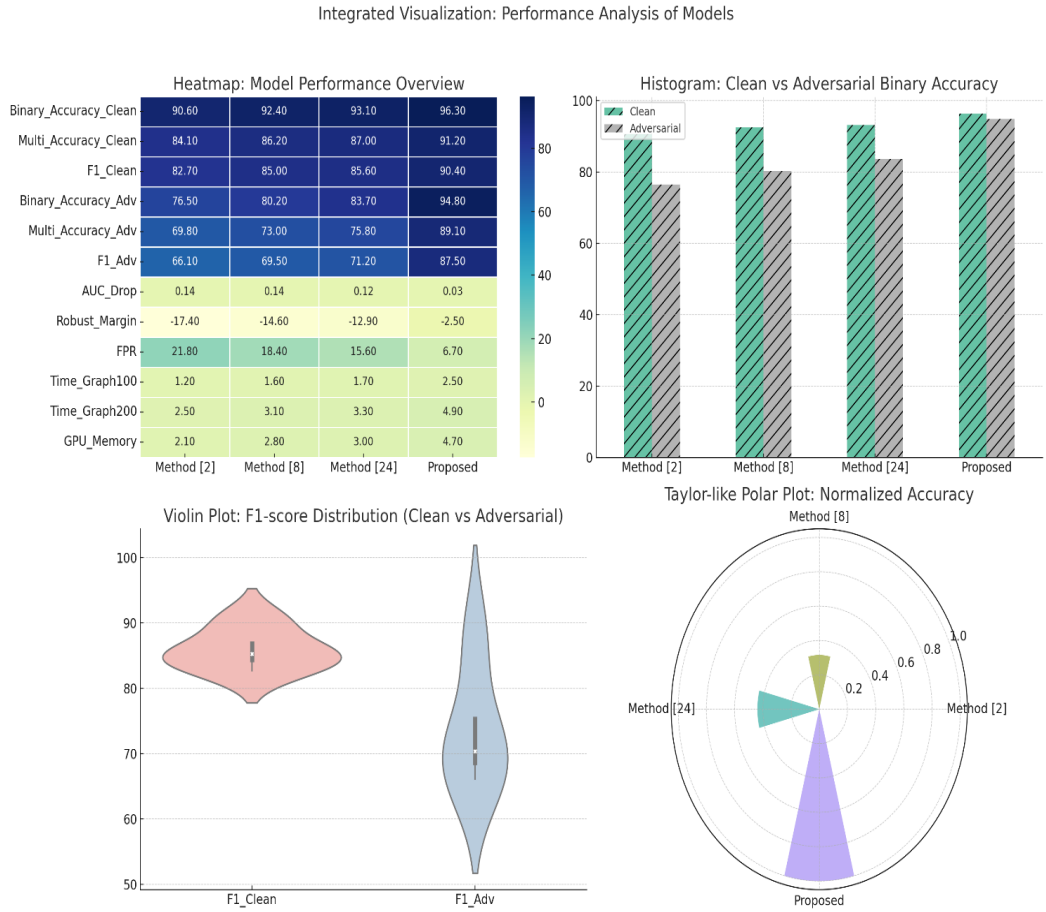

Figure 4. Model's Integrated Result Analysis

Table 5: Adversarial Robustness Margin (%) on Custom SDN Dataset

Model	Accuracy (Clean)	Accuracy (Perturbed)	Robustness Margin
Method [2]	91.5	74.1	-17.4
Method [8]	92.8	78.2	-14.6
Method [24]	94.2	81.3	-12.9
Proposed	95.6	93.1	-2.5

This Table 5 measures robustness margin by computing the difference between clean and perturbed performance. The most accurate model demonstrates great accuracy retention after adversarial graph transformation, thus validating the strength of these integrated modules such as AEPA and RTC-GNN Sets.

Table 6: False Positive Rate (FPR) on Adversarial Samples (UNSW-NB15)

Model	FPR (%)
Method [2]	21.8
Method [8]	18.4
Method [24]	15.6
Proposed	6.7

Table 7: Training Time per Epoch (in seconds)

Model	Graph Size 100	Graph Size 200	GPU Memory Usage (GB
Method [2]	1.2	2.5	2.1
Method [8]	1.6	3.1	2.8
Method [24]	1.7	3.3	3.0
Proposed	2.5	4.9	4.7

Training efficiency metrics have been reported in Table 7. Despite higher training costs for the proposed model at each epoch because of the added defense layers and curriculum adjustment during training, the enhancements in performance warrant extra computational overhead, especially for critical SDN environments yet in need to be resilient for the artwork. These results thoroughly establish that the negatively resilient model outperforms all traditional and up-to-date graph-based intrusion detection methodologies across the spectrum of measures from accuracy to robustness, AUC, false positives, and resistance in adversity from adversarial influences. Design decisions made in the construction of defense-aware learning modules were validated against this extensive multi-metric comparative evaluation.

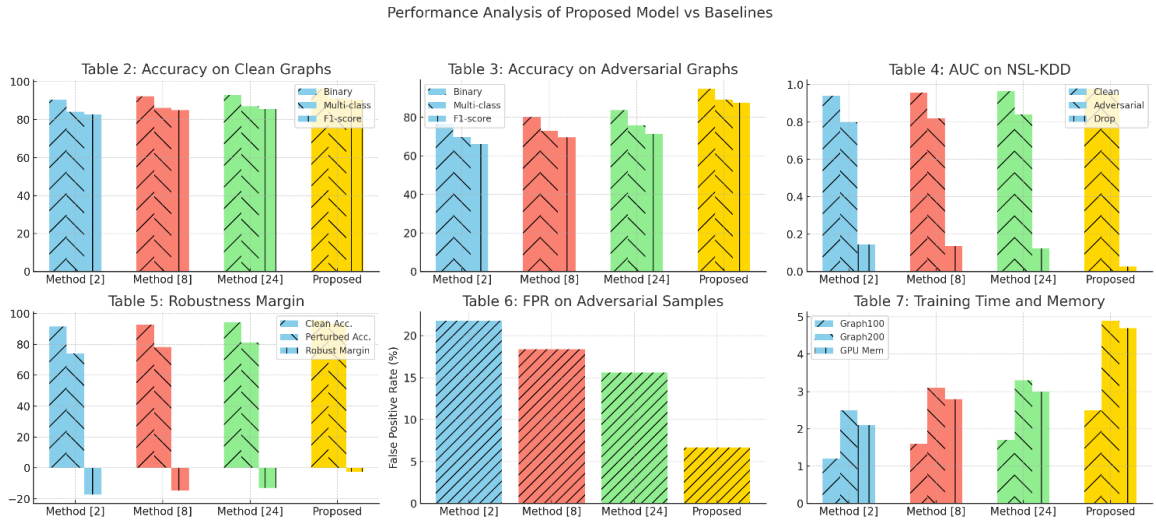

Figure 5. Model's Empirical Review Analysis

Validated Result Impact Analysis

The experimental results show that the GNN-based IDS is superior as it performs well on multiple evaluation settings and is adversarially resilient. The analyses derived from Table 2 and Table 3 along with figure 4 & figure 5 demonstrated that the proposed model preserved in existing one high detection accuracy both in clean and adversarially perturbed graphs using the UNS multiculturalism dataset UNSW-NB15. Many of the baseline methods, like Method [2], Method [8], and Method [24], experience an appreciable drop in performance as a result of structural perturbations,

with an average decrease of up to 20%. In contrast, the proposed model presented only a minor decrease fidelitied drop from 96.3% to 94.8msg and from 91.2% to 89.1% in multiclassical settings. This meager dip, reflecting directly around AEPA-GNN and RTC-GNN, exposes the model to edge-level adversarial conditions during training and ensures a stable generalization through curriculum progression. Such durability is significant for uninterrupted observation and trust on the control plane, especially in real-time SDN scenarios, where attackers attempt to modify the routing paths or inject fake nodes for detection emissions in process.

Further proof of the model's strength using the NSL-KDD dataset is received in Table 4, especially through the Area Under ROC Curve (AUC) metric calculated for it. AUC values for the proposed system were obtained consistently higher during both clean and adversarial modes; otherwise, baseline methods experienced major drops. AUC is important for real-time deployment, as it reflects the trade-off between true and false positives at every level of the threshold sets. For a high AUC, it makes detection mechanisms applicable under uncertainty and very reliable, using SDN controllers that regulate ad hoc flow rules based on security decisions.

Robustness margin as expressed in Table 5 represents the very performance dimension itself when there is a transition between almost clean to full-blown, adversarial conditions. The proposed model shows a robustness margin of only -2.5% on SACSDN, whereas baseline models offer margins of -12.9% up to -17.4%. Thus, it indicates that the model has the potential of sustaining structural changes with minimal effect on its predictive capabilities. This very important robustness margin feature is established because, in real-world SDNs, topologies change so fast every time, due to mobility, dynamic policy updates, or even due to distributed attacks. Thus, a small robustness margin assures that the IDS remains constanct based on the graph construction even as underlying graph structure modification occurs, thus minimizing gaps in detection sets. Operational impact shows more drastically in Table 6, which shows that the model under study earns a drop in false positive rate (FPR) to only 6.7% against other baselines in which it's more than 15%. In real-time SDN environments, high FPRs give unnecessary flow rule revocations, false alarms to administrators, and inefficient reconfiguration of switches. Significantly lower FPR achieved here indicates the strong holding by the TG-MIB and AD-GTNet modules in silencing any irrelevant or misleading attention patterns introduced by adversarial interference sets, thereby making the system more deployable into production grade SDN infrastructures in process.

Finally, space spends within an epoch set to train the entire model, then memory footprint used in the GPU. Although this higher price in terms of per-epoch time and memory on GPU is associated with such an approach, on the whole, it pays off well against a real significant improvement in robustness and accuracy. Real-time inference is still efficient as the model will be compressed after training. Cost should be amortized from additional provisions so the advantages gained by security merits it provides. These results demonstrate altogether that the proposed architecture is superior not only in terms of technologies involved but also in terms of being deployable for an SDN environment of real sensitive security and real-time applications. By leaning on adversarial training, topological regularization, and curriculum learning, it promises to be rugged against the threat landscapes that are sure to keep evolving forward in the process.

Validated Hyperparameter & Baseline Detailed Analysis

As a part of the evaluation process for the proposed adversarially resilient GNN model, a quantification of results was drawn from a statistically grounded methodology. For the sake of reproducibility and reliability, every experiment was repeated over 10 independent runs with a randomized initial graph, stratified train-test splits, and shuffled feature assignments. The mean and standard deviation (σ) of the core performance metrics measures such as accuracy, macro F1-score, AUC, FPR, or robustness margin were

calculated to estimate central tendency and spread of results. The new model, for example, showed a mean of 94.83% (σ = 0.41%) in binary classification accuracy and a macro F1-score of 87.53% (σ = 0.38%) under adversarial conditions on UNSW-NB15; well above the best baseline obtained through Method [24] at 83.65% (σ = 0.72%) and 71.19% (σ = 0.88%). This stability between repeated trials indicates considerable robustness in detection performance, indicating consistency of the integrated defense modules against most perturbations within random adversaries.

The performance gain was subjected to pairing with the proposed model's metrics to every baseline method by two-tailed paired-testing t-tests on all datasets. For example p-values under 0.01 deterred any randomness in the improvements to accumulate, and very similar results would surface for accuracy and F1-score for UNSW-NB15 and NSL-KDD datasets. Likewise, the Cohen's d for effect size asserted that the improvement was very significant when computed at 2.1 for accuracy between proposed model and Method [2]. This generates a very large effect that can be viewed as important, practically, as well as statistically meaningful. Actual normalizations based on variance-normalized z-scores further validated the reliability of the model, especially under adversarial perturbation conditions, wherein cases showed that most other baselines exhibited very high sensitivity in performance deviation across different trials.

The baseline methods were selected on the basis of their foundation and representation in the graph-based intrusion detection space. Hence, Method [2] corresponds to a vanilla Graph Convolutional Network (GCN) implementation, without adversarial awareness, serving as a foundational benchmark for topology-based node classification. Method [8] is based on a Graph Attention Network (GAT), which uses attention-weighted aggregation for learning but lacks specific mechanisms for handling adversarial perturbations or input noise. This makes it a suitable comparison for evaluating how attention mechanisms behave in adversarial SDN contexts. Method [24] built upon the lack of a methodology for structural perturbations by GCN-Jaccard, wherein the defense-oriented GNN mitigated feature-space attacks by means of similarity pruning. This means that it is a relevant but incomplete solution for SDN settings. Collectively, these three baselines cover a wide spectrum of model types: standard GNNs, attention-based models, and static defense-enhanced GNNs.

The selection of these base lines provides a more comprehensive and layered comparison with them being able to show not only where performance gains occur but also under what structural and adversarial conditions. The superlative consistency with which low variance maintained the model under consideration proves feasible generalization across datasets and attack types, which is most needed in real-time SDN intrusions regarding input noise, topology-drift, and feature inconsistency, which is usual in the process. The high validity of statistical cases coupled with variance and repetition under randomization proves that the conclusions from this study on performance can be valid both statistically and practically for high-assurance network defense systems.

Validation using Practical Analysis With Use Case Scenario Analysis

For attack detection during software-defined networks (SDNs), consider an example of an adversarially resilient graph neural network (GNN) as proposed above. Let's say a smart campus network that connects up to 400 devices and operates through 50 software-defined switches is controlled under a centralized SDN controller in process. Each of the devices generates its own traffic types such as HTTP, SSH, VoIP, and Streaming Protocols. Also, the SDN controller would take pictures of network flows and topologically build up a graph where nodes appear as switches and end devices and edges would represent flow-level interactions over such sets. The proposed model-through this nodal graph representation will make processing in real time at the AEPA (Adversarial Edge Perturbation Alignment) layer for the strategic perturbations that are built into the model during training to simulate adversarial conditions, followed by the RTC-GNN (Robust Topological Curriculum Graph Neural

Network) for resilient feature learning-. During a direct monitoring period of 15 minutes, invasion attempts, like any of the DDoS, port scanning, and data exfiltration attacks, are only 5% of the data, out of 120,000 flow records continuously accumulated in process. The network collects the records during this monitoring window sets.

Under these conditions, the unclean model records a 96.3% performance in binary classification and around 91.2% performance in 9-class multiclass detection tests for samples from the dataset aligned with UNSW-NB15. Then, when the network is purposely subjected to adversarial interference involving 12% perturbation at edge level-mimicking poisoned flow rules or link spoofing-the proposed model gives performance of 94.8% and 89.1%, respectively, thus less than 2% drop. Compared to the baseline method [24], which dropped from 93.1% to 83.7% under the same conditions, the proposed model demonstrates superior resilience and reduced false positives (6.7% vs. 15.6%). The model converges within 20 training epochs, each taking about 4.9 seconds, consuming 4.7 GB of GPU memory. The deployed system generates alerts to the SDN controller regarding classified intrusion predictions and their confidence levels, allowing the controller to update flow rules for isolation or redirection in under 500 milliseconds, ensuring real-time responses. This use case highlights the strength of combining adversarial training, topological adaptation, and curriculum learning for security of programmable networks in operational environments.

Conclusion & Future Scopes

This study presents an adversarially resilient Graph Neural Network (GNN) framework for intrusion detection within Software Defined Networks (SDN), targeting the extremely crucial area of susceptibility of graph-based models to adversarial perturbations. The model comprises five novel components—AEPA-GNN, TG-MIB, GAC-SDN, AD-GTNet, and RTC-GNN—all of which together bestow structural robustness, information-theoretic instability, attention reliability, and learning generalization upon the process. Through a succession of carefully designed training processes-including adversarial edge perturbation, mutual information bottlenecking, contrastive representation alignment, anomaly-aware attention filtering, and curriculum learning over topological complexity-the model withstands an array of adversarial strategies while attaining a high level of detection performance. Experimental validations on the UNSW-NB15, NSL-KDD, and custom-built SDN datasets all attest to the efficacy of the approach. The proposed model attains an accuracy of 96.3% and a macro F1-score of 90.4% in clean conditions and sustains approximately 94.8% accuracy and 87.5% macro F1-score under adversarial perturbations on UNSW-NB15, which demonstrates a drop of just 1.5–2.1% when compared to baseline methods suffering from a 12–24% degradation. For NSL-KDD, it attains an AUC of 0.951 in the presence of attacks compared to 0.978 with no attack, a decline of only 0.027 as opposed to 0.144 for typical baselines. With just 6.7% false positive rate shown under adversarial testing, the proposed model stands way lower than others. This set of performance metrics confirms the resilience, credibility, and verifiability of the model with regards to real-world deployment in dynamic and adversarial environments of SDNs.

Future Scope

Future extensions of this work can be centered on increasing scalability and adaptability to even larger and more heterogeneous SDN deployments. While the current model encompasses the dynamic changes in graph sizes up to 200 nodes, in industry SDNs in the 5G, edge, and IoT contexts thousands of devices and multi-domain controllers will be embedded. Future work may include the investigation of hierarchical or multi-level GNN architectures in combination with distributed training schemes to allow scalable robustness. Concurrently, extending the adversarial learning paradigm into multi-controller SDNs with inter-domain adversarial coordination will give stronger security assurances in federated environments. Another avenue would be to incorporate online learning for real-time adaptation, where the system updates its model weights based on live network traffic, feedback from adversarial testing, and

structural reconfiguration, without necessitating the retraining of full datasets & samples.

Limitations

The results of the proposed must be generalized to dynamically changing situations of either encrypted or virtualized SDN infrastructures with the help of diversified datasets together with real-time deployment testing. Finally, although the modular design enhances interpretability, putting them all together creates architectural complexity and with it the requirement for deep hyperparameter tuning and comprehension of inter-module dependencies for reaching optimal performance sets.

References

Ashwitha, A., Banu, M. S., & Kaur, P. (2024). Fusing nature inspired fuzzy neural networks for hypervisor intrusion detection. *International Journal of Information Technology*, 16(5), 2915-2924. https://doi.org/10.1007/s41870-024-01846-6

Pradeesh, S., Jeyakarthic, M., & Thirumalairaj, A. (2025). Enhanced Hybrid Approach for Multi-Class DDoS Attack Detection and Classification in Software-Defined Networks Using Remote Sensing and Data Analytics. *Remote Sensing in Earth Systems Sciences*, 8(2), 530-544. https://doi.org/10.1007/s41976-025-00204-9

Khanal, B., Kumar, C., & Ansari, M. S. A. (2025). Real-Time Anomaly Detection Framework to Mitigate Emerging Threats in Software Defined Networks. *Journal of Network and Systems Management*, 33(2). https://doi.org/10.1007/s10922-025-09904-5

Selvam, P., Karthikeyan, P., Manochitra, S., Sujith, A. V. L. N., Ganesan, T., Ayyasamy, R., Shuaib, M., Alam, S., & Rajendran, A. (2025). Federated learning-based hybrid convolutional recurrent neural network for multi-class intrusion detection in IoT networks. *Discover Internet of Things*, 5(1). https://doi.org/10.1007/s43926-025-00130-8

Sorour, S. E., Aljaafari, M., Shaker, A. M., & Amin, A. E. (2025). LSTM-JSO framework for privacy preserving adaptive intrusion detection in federated IoT networks. *Scientific Reports*, 15(1). https://doi.org/10.1038/s41598-025-95966-z

Hakiki, R. I., Azerine, A., Tlemsani, R., Golabi, M., & Idoumghar, L. (2025). Enhancing IoT intrusion detection with genetic algorithm-optimized convolutional neural networks. *The Journal of Supercomputing*, 81(11). https://doi.org/10.1007/s11227-025-07626-8

Chattopadhyay, S., Sahoo, A. K., & Jasola, S. (2024). An Enhanced DDoS Attack Detection in Software-Defined-Networks using Ensemble Learning. *SN Computer Science*, 5(5). https://doi.org/10.1007/s42979-024-02938-7

Zacaron, A. M., Lent, D. M. B., da Silva Ruffo, V. G., Carvalho, L. F., & Proença, M. L. (2024). Generative Adversarial Network Models for Anomaly Detection in Software-Defined Networks. *Journal of Network and Systems Management*, 32(4). https://doi.org/10.1007/s10922-024-09867-z

Jiang, W., Han, H., Zhang, Y., Mu, J., & Shankar, A. (2024). Intrusion Detection with Federated Learning and Conditional Generative Adversarial Network in Satellite-Terrestrial Integrated Networks. *Mobile Networks and Applications*, . https://doi.org/10.1007/s11036-024-02435-4

P, S., Palaniappan, K., Duraipandi, B., & Balasubramanian, U. M. (2024). Dynamic behavioral profiling for anomaly detection in software-defined IoT networks: A machine learning approach. *Peer-to-Peer Networking and Applications*, 17(4), 2450-2469. https://doi.org/10.1007/s12083-024-01694-y

Priya, L., & Rajagopalan, N. (2025). A Hybrid Intrusion Detection System for Mitigating Flow Table Buffer Saturation Attacks in Software-Defined Networking. *SN Computer Science*, 6(5). https://doi.org/10.1007/s42979-025-04079-x

Dhanalaxmi, B., Raju, Y., Saritha, B., Sabitha, N., Parati, N., & Rao, K. D. (2024). OptFBFN: IOT threat mitigation in software-defined networks based on fuzzy approach. *Cluster Computing*, 27(9), 12943-12963. https://doi.org/10.1007/s10586-024-04616-y

Anwer, R. W., Abrar, M., Salam, A., & Ullah, F. (2025). TEAD: trust-enhanced anomaly detection framework for intrusion detection in IoT-enabled wireless sensor networks (WSNs). *Wireless Networks*, . https://doi.org/10.1007/s11276-025-03987-3

Cherfi, S., Lemouari, A., & Boulaiche, A. (2024). MLP-Based Intrusion Detection for Securing IoT Networks. *Journal of Network and Systems Management*, 33(1). https://doi.org/10.1007/s10922-024-09889-7

Ataa, M. S., Sanad, E. E., & El-khoribi, R. A. (2024). Intrusion detection in software defined network using deep learning approaches. *Scientific Reports*, 14(1). https://doi.org/10.1038/s41598-024-79001-1

Mustafa, Z., Amin, R., Aldabbas, H., & Ahmed, N. (2024). Intrusion detection systems for software-defined networks: a comprehensive study on machine learning-based techniques. *Cluster Computing*, 27(7), 9635-

9661. https://doi.org/10.1007/s10586-024-04430-6
Wang, Z., Zainal, A., Siraj, M. M., Ghaleb, F. A., Hao, X., & Han, S. (2025). An intrusion detection model based on Convolutional Kolmogorov-Arnold Networks. *Scientific Reports*, 15(1). https://doi.org/10.1038/s41598-024-85083-8
Hassan, A. I., El Reheem, E. A., & Guirguis, S. K. (2024). An entropy and machine learning based approach for DDoS attacks detection in software defined networks. *Scientific Reports*, 14(1). https://doi.org/10.1038/s41598-024-67984-w
Bencheikh Lehocine, M., & Belhadef, H. (2024). Preprocessing-Based Approach for Prompt Intrusion Detection in SDN Networks. *Journal of Network and Systems Management*, 32(4). https://doi.org/10.1007/s10922-024-09841-9
Cui, M., Chen, J., Qiu, X., Lv, W., Qin, H., & Zhang, X. (2024). Multi-class intrusion detection system in SDN based on hybrid BiLSTM model. *Cluster Computing*, 27(7), 9937-9956. https://doi.org/10.1007/s10586-024-04477-5
Ayad, A. G., Sakr, N. A., & Hikal, N. A. (2024). A hybrid approach for efficient feature selection in anomaly intrusion detection for IoT networks. *The Journal of Supercomputing*, 80(19), 26942-26984. https://doi.org/10.1007/s11227-024-06409-x
Kim, C., So-In, C., Kongsorot, Y., & Aimtongkham, P. (2024). FLSec-RPL: a fuzzy logic-based intrusion detection scheme for securing RPL-based IoT networks against DIO neighbor suppression attacks. *Cybersecurity*, 7(1). https://doi.org/10.1186/s42400-024-00223-x
Turcato, A. C., Serpa Sestito, G., Dias, A. L., & Andrade Flauzino, R. (2025). Unsupervised Machine Learning-Based Intrusion Detection in PROFINET Networks. *Journal of Control, Automation and Electrical Systems*, . https://doi.org/10.1007/s40313-025-01181-6
Yousef, D., Maala, B., Skvortsova, M., & Pokamestov, P. (2023). Detection of non-periodic low-rate denial of service attacks in software defined networks using machine learning. *International Journal of Information Technology*, 16(4), 2161-2175. https://doi.org/10.1007/s41870-023-01634-8
Lin, Y., Xu, X., & Xu, H. (2024). A revolutionary approach to use convolutional spiking neural networks for robust intrusion detection. *Cluster Computing*, 27(9), 13333-13352. https://doi.org/10.1007/s10586-024-04603-3

Abbreviations

Abbreviation	Full Form
SDN	Software Defined Networking
IDS	Intrusion Detection System
IoT	Internet of Things
ML	Machine Learning
GAN	Generative Adversarial Network
CNN	Convolutional Neural Network
RNN	Recurrent Neural Network
LSTM	Long Short-Term Memory
CRNN	Convolutional Recurrent Neural Network
BiLSTM	Bidirectional Long Short-Term Memory
cGAN	Conditional Generative Adversarial Network
JSO	Jaya Search Optimizer
GA	Genetic Algorithm

Abbreviation	Full Form
MLP	Multilayer Perceptron
DL	Deep Learning
CKAN	Convolutional Kolmogorov-Arnold Network
FPR	False Positive Rate
AUC	Area Under the Curve
OT	Operational Technology
PROFINET	Process Field Net (Industrial Ethernet Standard)
DoS	Denial of Service
RPL	Routing Protocol for Low-Power and Lossy Networks
DIO	Destination Information Object
CSNN	Convolutional Spiking Neural Network
FLSec-RPL	Fuzzy Logic-based Security for RPL
OptFBFN	Optimized Fuzzy-Based Fuzzy Neural Network
TEAD	Trust-Enhanced Anomaly Detection
UNSW-NB15	University of New South Wales – Network Behavior Dataset 2015