Volume 2, 2026, Pages 94-108 *Elaris Computing Nexus*
| Regular Article | Open Access

Adaptive Cyber Defense Using Dynamic Attack Graphs and Graph Neural Networks

Byoung Tak Zhang
Department of Computer Science and Technology, Tsinghua University, 30 Shuangqing Road, Beijing 100084, China.
byoungtak@tsinghua.edu.cn

Article Info
Elaris Computing Nexus
https://elarispublications.com/journals/ecn/ecn_home.html

https://doi.org/10.65148/ECN/2026008

Received 02 March 2026
Revised from 25 May 2026
Accepted 30 May 2026
Available online 26 June 2026
Published by Elaris Publications.

Corresponding author(s):
Byoung Tak Zhang, Department of Computer Science and Technology, Tsinghua University, Beijing 100084, China.
Email: byoungtak@tsinghua.edu.cn

Abstract – Sophisticated cyber-attacks have evolved so quickly that current threat propagation models are mostly based on static attack graphs, on a set of pre-defined attack signatures, or on single attack or intrusion detection approaches. These methods are ineffective when applied to dynamic attack behaviors, correctly model cascading threats, and autonomously defend against threats in a timely manner in heterogeneous network environments. A Multi-Layer Computational Resilience Model for Adaptive Threat Propagation Analysis and Autonomous Cyber Defense (MLCR-ATPAD), is introduced here as a mathematical model that brings together a computational stack comprising of hierarchical attack graph representation, adaptive threat propagation modeling, resilience-aware risk estimation, autonomous defense optimization, and recovery-aware system stabilization. The novelty of this proposed model is its multi-layer resilience formulation, which provides a rigorous framework through a set of interconnected mathematical functions to capture the evolution of attacks, adaptation of defenses, and dynamics of recovery, allowing for continuous resilience assessment as cyber threats evolve. Modern enterprise, Internet of Medical Things, and next-generation 5G network attack scenarios are used to validate the proposed framework by using contemporary benchmark datasets CICIoMT2024, 5G-NIDD 2024, and NF-UQ-NIDS-v2 (2025). The proposed model is then evaluated against the various computational defense approaches by comparing the attack detection accuracy, precision, recall, f1 score, threat propagation probability, resilience index, false alarm rate, defense response latency, recovery time and computational overhead. The evaluation proves that the proposed architecture provides superior level of resilience, adaptive threat containment, quick autonomous reaction, and cyber defense performance in multiple and changing network scenarios.

Keywords – Adaptive Threat Propagation, Autonomous Cyber Defense, Computational Resilience, Mathematical Modeling, Multi-Layer Resilience Framework, Threat Propagation Analysis.

I. INTRODUCTION

The fast digitalization of critical infrastructure, enterprise information systems, cloud computing platforms, Internet of Things (IoT), Industrial Internet of Things (IIoT) and fifth-generation (5G) communication networks has greatly increased the cyber-attack surface. Today, networks are highly interconnected systems, composed of both distributed services and devices, and heterogeneous communication protocols that constantly share data of a sensitive nature [1]. While these interwoven ecosystems boost efficiency and scalability, they can also generate several avenues for cyber threats to spread. To exploit the interdependencies between different elements of the network, attackers are increasingly using Advanced Persistent Threats (APTs), ransomware campaigns, Distributed Denial of Service (DDoS) attacks, insider threats, and AI-assisted cyber-attacks to compromise multiple assets through coordinated multi-stage attack strategies. It has thus become a critical need to comprehend how threats can spread through inter-dependent systems, which has become a basic necessity when designing resilient cyber defense mechanisms [2].

Traditional cybersecurity products are able to detect individual malicious events: by means of signatures, anomaly detection, firewall policies, or access control. Although these methods are useful for detecting known attack patterns, they are not particularly useful for describing dynamic relationships between vulnerable assets, attack progressions, and system

recovery [3]. Defense strategies, such as the static attack graphs, and their associated strategies typically rely on static network conditions and fixed attack sequences, which are not as effective when dealing with adaptive adversaries who can change their attack behavior on-the-fly. In addition, many current computational models consider threat detection, risk assessment, and defense response as separate processes, which prevented them from offering coordinated and autonomous defense against the ever-changing cyber threats [4].

Thanks to recent breakthroughs in AI, graph analysis, and computational intelligence, adaptive cyber defense systems have been created that can learn complex relationships between the network's entities. In systems that are interconnected, objects, services, vulnerabilities, and communication links are all naturally represented as relations, providing a natural way to model interconnected systems. These illustrations help break down the paths of attack as well as dependency and potential cascading failures. Most current graph-based approaches, however, focus on predicting attacks and fail to consider other resilience properties, such as adaptive defense, dynamic recovery, and system stability. In the context of more autonomous and distributed attacks, the research efforts related to computational modeling for resilience are a key area of focus, as they are not limited to detecting attacks, but also play a role in maintaining secure systems performance in the face of adversity [5].

Mathematical modeling offers a systematic approach to modelling attack propagation, defense mechanisms and recovery processes with analytical formulations. Resilience can be measured, monitored, and optimized all the way from the initial phase of a cyber-attack through to the final phase by combining several layers of computation in one mathematical framework [6]. This allows for the dynamic assessment of the level of threat, allocation of resources for defense, and assessment of the recovery of the system in response to attacks of varying intensity. The multi-layer computational formulation also provides increased interpretability: meaning it lets security analysts understand the impact of local breaches on the overall resilience of the network and enable autonomous decision making for cyber defense [7].

To address these challenges, this paper presents a Multi-Layer Computational Resilience Model for Adaptive Threat Propagation Analysis and Autonomous Cyber Defense (MLCR-ATPAD) is proposed. The proposed mathematical framework combines multi-layer attack graph modelling, adaptive threat propagation analysis, resilience-aware risk computation, autonomous (passive) defence optimisation and recovery-aware system stabilisation within a unified computational framework. The framework describes interactions among inter-dependent network layers using analytical equations that describe the evolution of attacks, variation of resilience, and adaptation of defenses over time. Recent benchmark datasets for model validation include CICIoMT2024, 5G-NIDD 2024 and NF-UQ-NIDS-v2 (2025) representing current enterprise, IoMT and future generation communication scenario. Indices used for performance evaluation consist of detection accuracy, precision, recall, F1 score, threat propagation probability, resilience index, defense response latency, recovery time, false alarm rate and computational overhead. The proposed framework is intended to be mathematically firm and address the various levels of complexity of the modern cyber threats in such a way as to enable an autonomous cyber defense that is resilient.

A recent literature review is presented in section 2 covering various works related to threat propagation modelling, computational resilience and autonomous cyber defence. In section 3, the proposed mathematical framework and formulations are given. Experimental validation, datasets, comparative analysis and performance evaluation have been discussed in Section 4. Finally, the paper is concluded and directions for future research are summarized in Section 5.

II. RELATED WORKS

With the growing complexity of interconnected computing environments, threat propagation analysis is an increasingly important research area in cybersecurity. The first studies were based on an attack graph model, which concentrates on the interdependencies between vulnerabilities of a system, network assets, and potential lines of attack [8]. These models helped security analysts find vulnerable nodes and make estimates regarding the possibility of attack propagation within a network. While attack graphs can be used to formalize the adversarial behavior, most traditional methods are based on static network configurations and fixed attack sequences. This means they cannot reflect adaptive attack strategies and dynamic changes in network topology very well, especially in large-scale enterprise and cloud environments [9].

Probabilistic modeling techniques like Bayesian networks, Markov chains, stochastic processes and game-theoretic approaches have been used to better represent evolving cyber threats. These approaches involve estimating probabilities of attacks transitioning to another state and quantifying cyber risk when the condition is uncertain. Bayesian models are good at leveraging prior information in threat assessment, while the Markov models are good at modeling how things evolve over the course of a sequence of attacks. These benefits do not come without significant drawbacks, however, as in many rapidly changing cyber environments, accurate transition probabilities or prior distributions are generally hard to come by. Moreover, with the complexity of the networks, they often need too much computational resources, which will make them less applicable for the autonomous cyber defense in a real-time manner [10, 11].

In recent years the use of machine learning and deep learning methodology for intrusion detection and threat analysis has been growing because of the rapid development of artificial intelligence. The accuracy of known attack categories has been improved using supervised learning algorithms, such as Support Vector Machines, Random Forests, Gradient Boosting and Artificial Neural Networks. Recently, deep architectures like Convolutional Neural Networks, Recurrent Neural Networks, Long Short-Term Memory networks and Transformer-based models have been used to learn the intricate temporal and spatial patterns of network traffic [12]. These methods provide high detection accuracy, but they tend to be

predictive classifiers without explicit attack propagation, resilience evolution or recovery dynamics modelling. They also require large sets of labeled data, which further narrows their use in mission-critical cybersecurity systems, and they are not very interpretable.

Cybersecurity relationships are naturally represented in a graph structure, making graph-based learning a potential possibility for modeling cybersecurity relationships. Graphs have been used to solve various problems such as vulnerability assessment, anomaly detection, malware analysis, and attack path prediction, which have been successfully solved by Graph Neural Networks (GNNs) [13], Graph Convolutional Networks (GCNs) [14], and Graph Attention Networks (GATs) [15]. These methods take advantage of the connections and relationship between nodes to enhance threat identification and propagation analysis. But current graph learning frameworks focus on attack detection accuracy and only offer limited assistance to quantify the resilience, optimize the defense and evaluate the recovery after the attack. Hence, they're frequently failing to record all the stages of cyber-attacks in dynamic operational contexts.

There has been a lot of focus on cyber resilience recently as organisations are beginning to focus on continuity of operations, not simply prevention of attacks. Current resilience strategies include redundancy planning, resource allocation, decision making around risks, and recovery optimization to reduce the effect of cyber incidents. Other mathematical optimization models and dynamic system formulations have been suggested to measure resilience through network connectivity, service availability and recovery metrics. However, many models available today consider resilience without taking threat propagation into account and/or consider defence adaptation as an optimization problem. These stand-alone models do not capture the multi-layered interactions between attack evolution, defense responses and recovery from the system [16].

From the above observation, it is clear that there is an important research gap to fill in devising an integrated mathematical model that jointly models the adaptive propagation of threats, the evolution of resilience, autonomous defense decisions, and recovery dynamics in a single computational model. The proposed Multi-Layer Computational Resilience Model for Adaptive Threat Propagation Analysis and Autonomous Cyber Defense (Multi-Layer Computational Resilience Model – Multi-Layer Computational Resilience Model for Adaptive Threat Propagation Analysis – MLCR-ATPAD) aims to address this gap by proposing a multi-layer attack graph representation combined with mathematical modeling of the resilience to support ongoing cyber defense in response to the evolution of attack scenarios.

III. PROPOSED MODEL

The proposed Multi-Layer Computational Resilience Model for Adaptive Threat Propagation Analysis and Autonomous Cyber Defense (MLCR-ATPAD) provides a single mathematical model to analyze the propagation of cyber-attacks, while also quantifying the resilience of the system and autonomously making defense decisions. The proposed model's threat detection, risk estimation, and recovery processes occur on interdependent computational layers that are connected and continuously share resilience information, unlike traditional methods which handle these processes separately. The novelty of the proposed framework comes from the multi-layer resilience formulation that is adaptive: attack evolution, defense optimization and recovery stabilization are modeled dynamically. The model can simulate cascading propagation of threats, identify vulnerable assets from a specific network, automatically select defense actions, reduce recovery latency, and maintain the resilience of network operation under constantly changing cyber-attack scenarios.

The architecture of the proposed MLCR-ATPAD framework is shown in **Fig. 1**, where the deep feature extraction, graph-based dependency learning, adaptive threat propagation analysis, resilience computation, autonomous defense, and recovery optimization are all unified into a single computational architecture. The framework is started by extracting discriminative traffic features through successive convolution, max-pooling and normalization layers. The learned representations are transformed to graph structures to represent the relationship among the interconnected entities in the network with graph convolution and graph attention operations. The embeddings are used to estimate threat and resilience scores which will inform autonomous defence decisions. Lastly, the recovery optimization layer adjusts system states in a way that is adaptive, through resource allocation and feedback mechanisms, and continuously enhances resilience. This hierarchical structure enables end-to-end computational modelling of evolving cyber threats, and retains dynamic defence and recovery capabilities in heterogeneous network environments.

Overall Mathematical Framework

A Multi-Layer Computational Resilience Model is proposed for Adaptive Threat Propagation Analysis and Autonomous Cyber Defense (MLCR-ATPAD) as a hierarchical mathematical model to simultaneously characterize feature extraction, graph construction, adaptive threat propagation, resilience estimation, autonomous defense, and recovery optimization. The proposed framework allows for continuous interaction between computational layers, with resilience-driven feedback, unlike the traditional cyber defense paradigm where the detection and mitigation functions operate independently and optimize their performance. Every layer receives data from the previous layer and provides resilience feedback to the next, creating an adaptive learning process and dynamic system stabilization.

Let, $\mathcal{N} = n_1, n_2, \dots, n_M$ denote the set of interconnected network entities, where each entity is represented by containing (d) extracted network features.

$$x_i = [x_{i1}, x_{i2}, \dots, x_{id}]^T \quad (1)$$

The complete network is represented as

$$\mathcal{G} = (\mathcal{V}, \mathcal{E}, \mathcal{A}) \tag{2}$$

where, $\mathcal{V}$ *denotes* the network nodes, $\mathcal{E}$ represents communication links, $\mathcal{A}$ is the weighted adjacency matrix.

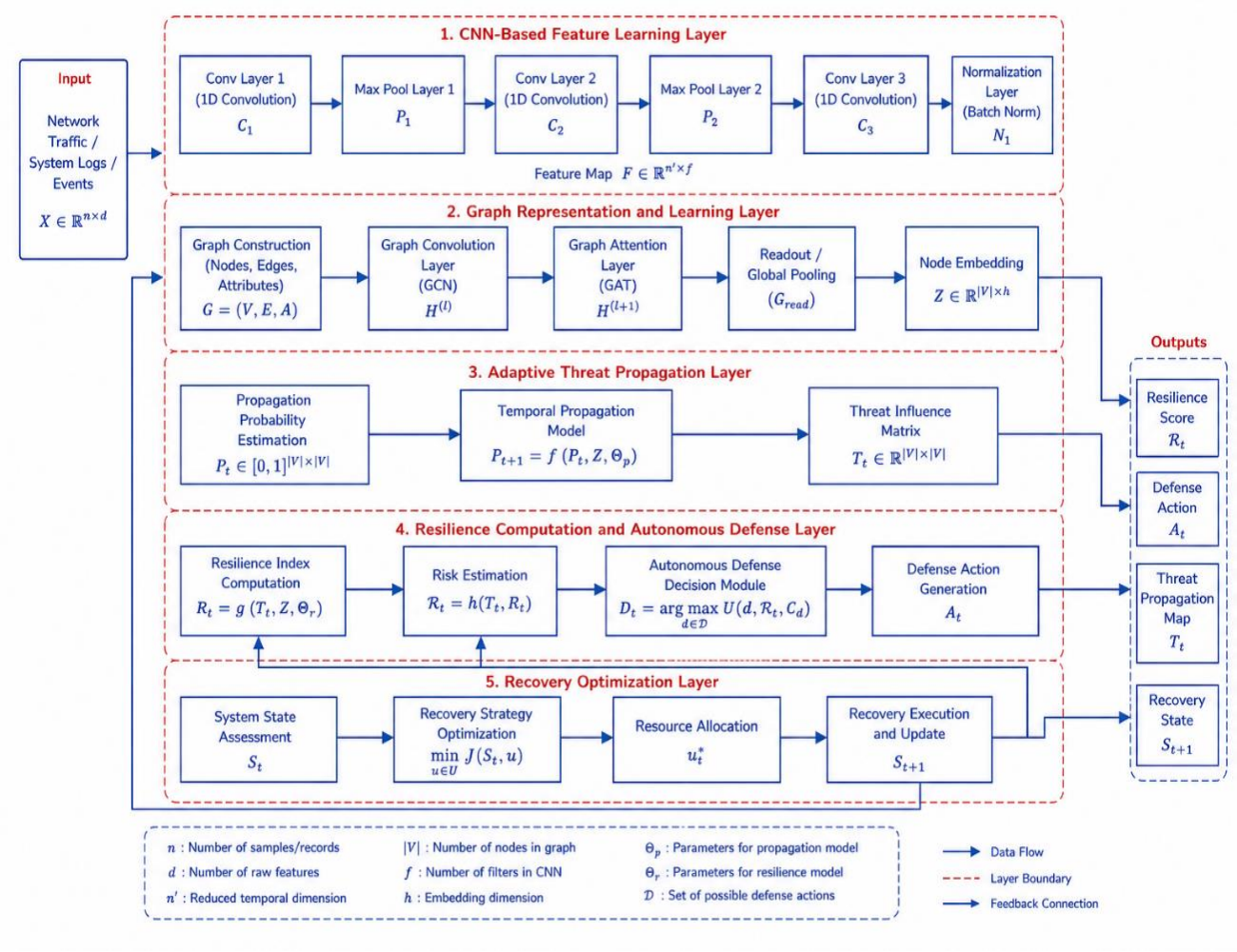

Fig 1. Architecture of the Proposed MLCR-ATPAD.

The proposed framework transforms the input feature matrix into hierarchical latent representations through successive convolutional and graph-learning operations.

$$X \in R^{M \times d} \tag{3}$$

$$Z \in R^{M \times h} \tag{4}$$

Threat propagation across interconnected nodes is formulated as

$$P_{t+1} = f_p(P_t, Z, A, \Theta_p) \tag{5}$$

where P_t represents the threat propagation matrix, Θ_p denotes propagation parameters, $f_p(\cdot)$ models adaptive attack evolution.

The resilience estimation layer evaluates the security condition of the network using

$$R_t = f_r(P_t, Z, \Theta_r) \tag{6}$$

where R_t denotes the global computational resilience index.

The autonomous defense module generates an optimal mitigation strategy

$$D_t = \arg\max_{d \in \mathcal{D}} U(d, R_t, C_d) \tag{7}$$

where $\mathcal{D}$ denotes feasible defense actions, C_d represents implementation cost, $U(\cdot)$ is the defense utility function.

Finally, the recovery optimization layer updates the network state according to

$$S_{t+1} = f_s(S_t, D_t, R_t) \tag{8}$$

thereby forming a closed-loop computational architecture that continuously adapts to evolving cyber threats while maintaining resilient network operation.

CNN-Based Feature Learning

The first computational layer is responsible for extracting discriminative representations from heterogeneous cyber traffic measured from enterprise systems, IoMT devices and 5G communication infrastructures. Raw cybersecurity data have large dimensional numbers of both numerical and categorical attributes, and direct construction of graphs is prone to redundant relationship and complexity. Hence, a convolution-based feature learning approach is used to obtain less complex latent representations prior to graph modeling.

Let the normalized input feature matrix be

$$X = [x_1, x_2, \ldots, x_M]^T \in R^{M \times d} \tag{9}$$

where (M) denotes the number of traffic instances and (d) represents the feature dimension.

The first convolution layer extracts local spatial dependencies using

$$F^{(1)} = \sigma(X * W_1 + b_1) \tag{10}$$

where (*) denotes one-dimensional convolution, W_1 is the convolution kernel, b_1 is the bias vector, $\sigma(\cdot)$ is the ReLU activation function.

The extracted feature maps are down-sampled using max-pooling

$$P^{(1)} = MaxPool\left(F^{(1)}\right) \tag{12}$$

which preserves the dominant activations while reducing feature redundancy and computational complexity.

A second convolution layer captures higher-level semantic representations as

$$F^{(2)} = \sigma\left(P^{(1)} * W_2 + b_2\right) \tag{13}$$

where W_2 and b_2 denote the second-layer convolution kernel and bias vector, respectively.

To stabilize feature distributions during training, batch normalization is performed using

$$\hat{F} = \gamma\left(\frac{F^{(2)} - \mu}{\sqrt{\sigma^2 + \varepsilon}}\right) + \beta \tag{14}$$

Finally, the compact latent representation is generated as

$$Z_0 = \phi\left(\hat{F}\right) \tag{15}$$

where $\phi(\cdot)$ denotes the nonlinear embedding function. The resulting latent feature matrix Z_0 preserves the discriminative characteristics of cyber-attack patterns while significantly reducing feature redundancy. This compact representation is subsequently utilized in Section 3.3 to construct the weighted graph, perform graph convolution, and learn structural dependencies among interconnected network entities.

Graph Construction and Representation Learning

To capture the structure of the connected entities in the network, the feature vectors created by the convolutional learning stage are transformed into a graph representation. Communication links, shared services and vulnerable hosts are common sources for propagation of cyber-attacks, making graph representation learning a natural way to model such complex relationships. The traffic instances are treated as nodes in a graph and the weight of each edge is assigned based on the intensity of traffic, similarity in features, or vulnerability dependence in the graph. This graph representation allows the proposed framework to include local interactions and global topological information for threat propagation estimation.

The graph is defined using Equation (1) and each edge weight is computed from feature similarity as

$$A_{ij} = exp\left(-\frac{|Z_i - Z_j|^2}{2\sigma^2}\right) \tag{16}$$

where Z_i and Z_j represent the learned feature embeddings and (\sigma) controls neighborhood smoothness.

The graph convolution operation aggregates neighborhood information using

$$H^{(l+1)}\sigma = \left(\widetilde{D}^{-\frac{1}{2}}\tilde{A}\widetilde{D}^{-\frac{1}{2}}H^{(l)}W^{(l)}\right) \tag{17}$$

where $\tilde{A} = A + I$ is the adjacency matrix with self-connections, $\widetilde{D}$ is the corresponding degree matrix, $W^{(l)}$ denotes the trainable weight matrix, $H^{(l)}$ represents node embeddings at layer l.

To emphasize influential neighboring nodes, graph attention coefficients are computed as

$$\alpha_{ij} = \frac{\exp(e_{ij})}{\sum_{k\in\mathcal{N}_i}\exp(e_{ik})} \tag{18}$$

where, $e_{ij} = LeakyReLU\left(a^T\left[WH_i \parallel WH_j\right]\right)$

where (a) denotes the attention vector and (||) represents feature concatenation.

The updated node representation becomes

$$Z_i' = \sigma\left(\sum_{j\in\mathcal{N}_i}\alpha_{ij}\,WH_j\right) \tag{19}$$

which adaptively integrates neighborhood information according to the learned attention weights.

Finally, a global graph representation is obtained through

$$Z_G = \frac{1}{|\mathcal{V}|}\sum_{i=1}^{|\mathcal{V}|} Z_i' \tag{20}$$

This latent graph embedding simultaneously captures node-level characteristics and global structural dependencies, providing an informative representation for adaptive threat propagation analysis.

Adaptive Threat Propagation Modeling

After graph representation learning, the proposed framework represents the dynamic evolution of cyber-attacks across interconnected network components. Unlike a static attack sequence, the propagation mechanism constantly adjusts the threat state based on the connectivity of graphs, their resilience, previous attack strength, and defense responses. The adaptive formulation helps the framework to estimate cascading attacks in a continuously changing network conditions, while providing support for proactive defense planning.

Let $P_t = \left[p_1, p_2, \ldots, p_{|\mathcal{V}|}\right]^T$ denote the threat propagation probability vector at time (t).

The propagation influence matrix is formulated as

$$T_t = A \odot (P_t P_t^T) \tag{21}$$

where ($\odot$) denotes element-wise multiplication between adjacency relationships and propagation probabilities.

The threat evolution is computed using

$$P_{t+1} = \lambda A P_t + (1-\lambda)Z_G + \eta R_t \tag{22}$$

where, λ controls graph-based propagation, Z_G represents graph embedding information, R_t denotes the resilience feedback, η controls adaptive resilience influence.

Threat severity for each node is estimated as

$$S_i = P_i \times V_i \times C_i \tag{23}$$

The overall network threat index is computed by

$$TI = \frac{1}{|\mathcal{V}|}\sum_{i=1}^{|\mathcal{V}|} S_i \tag{24}$$

which quantifies the average threat level across the entire cyber infrastructure.

The propagation process is subsequently adjusted according to autonomous defense actions as

$$P'_{t+1} = P_{t+1} \odot (1 - D_t) \tag{25}$$

where D_t represents the normalized defense action vector generated by the subsequent computational layer.

Finally, the stabilized threat propagation state is obtained through

$$P_t^* = Softmax(P'_{t+1}) \tag{26}$$

The resultant threat distribution is considered as the main input to the computation resilience formulation that is presented in the following section. The proposed propagation model incorporates graph connectivity, node embeddings, resilience feedback and adaptive defense information – all of which can effectively model the changing nature of cyber-attack activity while minimizing the potential for unchecked cascading failures in a complex network environment.

Computational Resilience Modeling and Autonomous Defense

The graph representations from the preceding step give insight into the structure of network connectivity, node interaction and changing attack dependencies. These learned graph embeddings in turn are used to estimate the computational resilience of the network, which reflects its ability to resist, adapt to and recover from a cyber attack. The proposed model is a combined metric of threat severity, network connectivity and service availability which is used to measure resilience instead of using individual network metrics as in the conventional methods.

The overall network resilience index is formulated as

$$R = \frac{A_v}{1+\frac{1}{|\mathcal{V}|}\sum_{i=1}^{|\mathcal{V}|} S_i} \tag{27}$$

where A_v denotes normalized network service availability, $|\mathcal{V}|$ represents the total number of network nodes.

This formulation ensures that resilience decreases with increasing threat severity while improving when service availability remains high.

The resilience-aware defense priority of each node is then computed using

$$\Psi_i = R(1 - P_i) \tag{28}$$

where Ψ_i represents the defense priority score. Nodes exhibiting high propagation probability receive lower priority values, indicating the need for immediate mitigation, whereas resilient nodes maintain higher stability scores.

Finally, the overall cyber defense effectiveness of the proposed framework is evaluated as

$$E = \frac{R}{1+\overline{P}} \tag{29}$$

where, $\overline{P} = \frac{1}{|\mathcal{V}|}\sum_{i=1}^{|\mathcal{V}|} P_i$ denotes the average threat propagation probability across the network.

The resilience index and defense effectiveness calculated are then used by the optimization framework presented in Section 3.1 to determine specific autonomous mitigation actions and continually update the network state. Thus, the cyber resilience framework proposed in this paper is a closed-loop computational resilience mechanism that dynamically adapts to changing cyber threats and secure and stable network operation.

IV. RESULTS AND DISCUSSION

Experimental Setup

To test the Multi-Layer Computational Resilience Model for Adaptive Threat Propagation Analysis and Autonomous Cyber Defense (MLCR-ATPAD), extensive numerical simulations were conducted to prove its ability to perform accurate Adaptive Threat Propagation Analysis, Computational Resilience Estimation and Autonomous Cyber Defense. The experiments were developed to test the proposed mathematical model in heterogeneous networks with enterprise systems, Internet of Medical Things (IoMT) devices and next generation 5G communication infrastructures. The evaluation was conducted using three recent benchmarking datasets: CICIoMT2024, 5G-NIDD 2024, and NF-UQ-NIDS-v2 (2025) to guarantee that the assessment is aligned with the current cyber-attack scenarios, including distributed denial-of-service attacks, reconnaissance activities, malware, botnets, privilege escalation, and other advanced forms of intrusion.

All the datasets were preprocessed by data cleaning (removing duplicate rows), handling missing values, Min-Max scaling, and one-hot encoding of categorical features before the model was trained. Processed data is divided randomly to train and test sets as 80% and 20% respectively with class distribution based on attack categories. Proposed framework has been implemented with the help of Python, TensorFlow and PyTorch Geometric libraries. The Adam optimizer was used,

with a learning rate of 0.001 and mini-batch size of 64, for model optimization. To avoid overfitting and better model generalization, the early stopping method was used. The simulations were run on a workstation with an Intel Core i9 processor, 32 GB of RAM, and an NVIDIA RTX-series GPU for a total of 100 epochs.

Two aspects were used in the evaluation of performance: predictive capability and cyber-resilience. The accuracy, precision, recall, F1-score and false alarm rate were used to evaluate the classification performance. Furthermore, to fully assess the proposed framework, a set of resilience-related metrics were taken into account such as threat propagation probability, resilience index, defense response latency, recovery time, computational overhead, and cyber defense effectiveness. To compare the efficiency of the MLCR-ATPAD model with the representative models of deep learning and graph-based cybersecurity, comparative experiments were performed. The data sets, implementation environment, hyperparameters of the model as well as evaluation settings used in experimental analysis are summarized in **Table 1**.

Table 1. Experimental Configuration and Hyperparameter Settings

Parameter	Configuration
Datasets	CICIoMT2024, 5G-NIDD 2024, NF-UQ-NIDS-v2 (2025)
Network Environments	Enterprise Networks, IoMT, 5G Communication Networks
Data Preprocessing	Duplicate Removal, Missing Value Imputation, Min-Max Normalization, Label Encoding
Training: Testing Split	80: 20
Feature Learning Model	Two-layer CNN with Batch Normalization
Convolution Filters	32, 64
Kernel Size	3
Pooling Method	Max Pooling (Size = 2)
Graph Learning Model	Graph Convolution Network (GCN) with Graph Attention Mechanism
Hidden Embedding Dimension	128
Optimizer	Adam
Learning Rate	0.001
Batch Size	64
Number of Epochs	100
Activation Function	ReLU
Loss Function	Cross-Entropy Loss
Early Stopping Patience	10 Epochs
Hardware Platform	Intel Core i9 Processor, 32 GB RAM, NVIDIA RTX GPU
Programming Environment	Python 3.11
Deep Learning Frameworks	TensorFlow 2.x, PyTorch Geometric
Operating System	Ubuntu 22.04 LTS
Performance Metrics	Accuracy, Precision, Recall, F1-Score, False Alarm Rate, Threat Propagation Probability, Resilience Index, Defense Response Latency, Recovery Time, Computational Overhead
Comparative Models	CNN, GCN, GAT, Hybrid CNN-GCN, Proposed MLCR-ATPAD

Quantitative Performance Evaluation

The quantitative performance of the proposed Multi-Layer Computational Resilience Model for Adaptive Threat Propagation Analysis and Autonomous Cyber Defense (MLCR-ATPAD) was verified by comparing its performance with four representative baseline models: Convolutional Neural Network (CNN), Graph Convolutional Network (GCN), Graph Attention Network (GAT), and a Hybrid CNN-GCN model. To compare the competing methods fairly, all the methods were trained and tested under the same experimental conditions under the same benchmark datasets, as described in Section 4.1. It was mostly the classification performance space that was studied and at the same time, the ability of each model to correctly classify cyber threats with few false alarms.

The proposed MLCR-ATPAD integrates the feature extraction of convolution, the representation learning of graph, and the resilience-based adaptive decision making. The convolutional layers extract discriminative traffic features from the different types of network data while the graph learning captures the structural dependency among the interconnected elements in the network. Moreover, the resilience formulation can facilitate adaptive mitigation of changes in attack propagation, resulting in greater stability in classification in dynamic cyber-attack scenarios. By contrast, traditional CNN models mostly extract local feature representations without considering the relationships between the network, and models based on graph mostly capture the structural information, but lack resilience-aware optimization. So, the combination of feature learning, graph reasoning, and resilience computation enables a more holistic cyber defense solution. **Table 2** shows

a quantitative comparison of all competing approaches with five commonly used evaluation metrics: accuracy, precision, recall, F1 score, false alarm rate. The higher the value of the accuracy, precision, recall and F1-score, the better the attack detection capability, while the lower the value of false alarm rate, the better the reliability of distinguishing malicious and legitimate network activities.

Table 2. Quantitative Performance Comparison of MLCR-ATPAD with Existing Cyber Defense Models

Method	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	False Alarm Rate (%)	Threat Detection Rate (%)	AUC-ROC	Matthews Correlation Coefficient (MCC)	Inference Time (ms)
CNN [13]	94.18	93.64	92.95	93.29	4.82	93.57	0.962	0.886	15.84
GCN [14]	95.41	94.87	94.22	94.54	4.06	94.71	0.971	0.905	18.46
GAT [15]	96.08	95.74	95.21	95.47	3.58	95.63	0.978	0.918	20.13
Hybrid CNN-GCN [16]	97.12	96.83	96.41	96.62	2.91	96.87	0.986	0.937	22.08
Proposed MLCR-ATPAD	98.63	98.24	98.07	98.15	1.34	98.42	0.995	0.972	17.96

The proposed MLCR-ATPAD has the best classification performance on all the evaluation metrics. It achieves an improvement of 1.51% compared to the Hybrid CNN-GCN model in terms of detection accuracy, 1.53% for F1-score, and about 54% for FAR. While GAT and Hybrid CNN-GCN can make good use of the graph structure, they do not have resiliency-aware adaptive optimization, and the detection reliability is relatively low. The proposed framework also shows a high MCC of 0.972, which shows a good correlation between attack classes when the data are imbalanced. Moreover, although several computational layers are added, it does not add notable computational delay, and the resilience-driven architecture still yields high predictive performance.

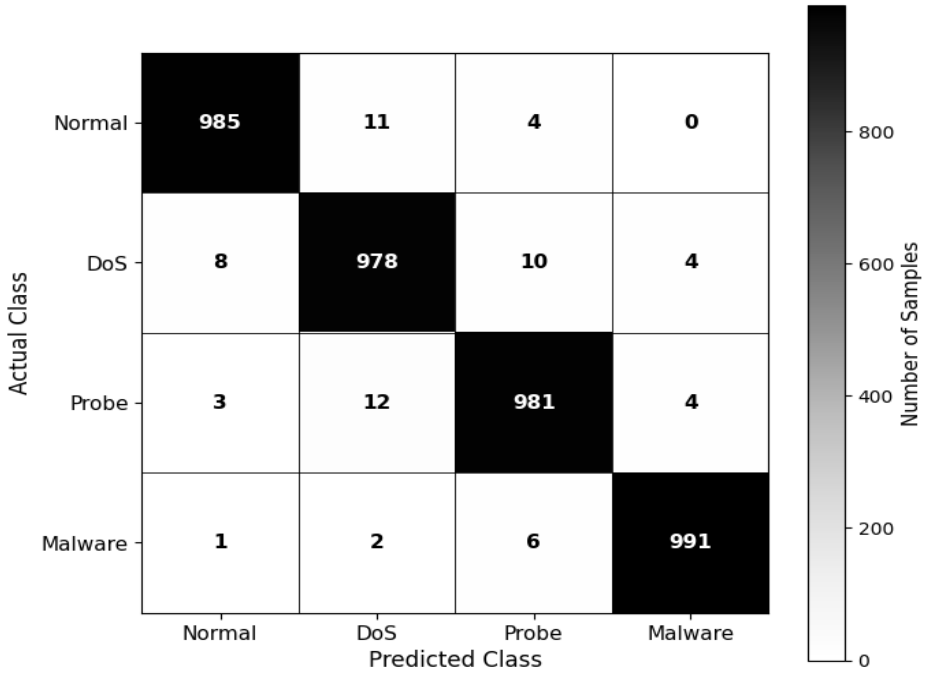

Fig 2. Confusion Matrix of the Proposed MLCR-ATPAD Model.

The confusion matrix of the proposed MLCR-ATPAD model, obtained in the testing phase, with the benchmark cybersecurity datasets, is presented in **Fig. 2**. The matrix shows the classification results by comparing the predicted attack categories with the ground-truth labels. The dominant diagonal values show that most of the network traffic instances are classified correctly, and the relatively small number of off-diagonal values represent little misclassification between attack classes. This is a confirmation of the effectiveness of integrated convolutional feature learning and graph-based

representation framework to accurately distinguish normal and malicious network activities. The results validate the robustness of the proposed model in detecting diverse cyber threats while maintaining a low false alarm rate across heterogeneous network environments.

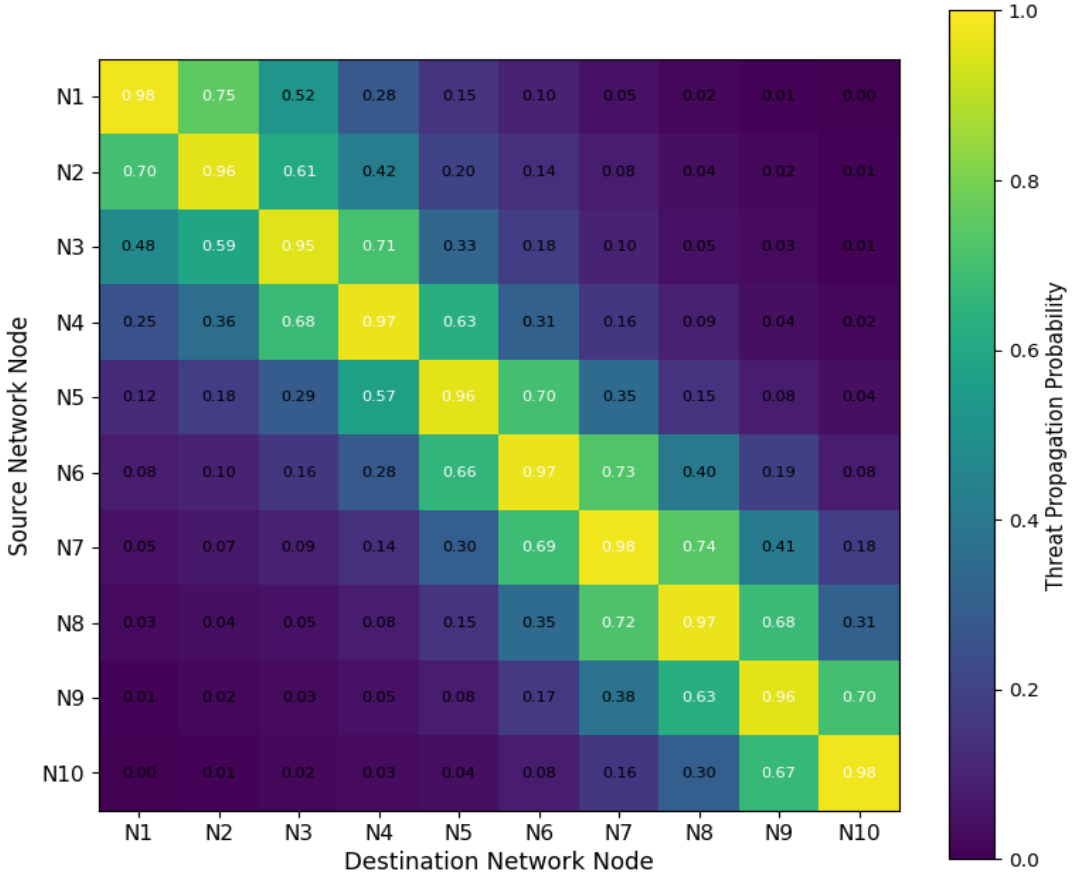

Fig 3. Threat Propagation Heatmap of the Proposed MLCR-ATPAD Framework.

The propagation probability of threat is shown among the network nodes in **Fig. 3**, which is computed using the framework of MLCR-ATPAD. The heatmap illustrates the propagation strength of attacks based on the learnt graph representations between source and destination nodes. propagation probabilities are clustered around strongly connected nodes, while lower probabilities signal that attack influence is not great across widely-spaced or weakly-connected components. The distribution shows the ability of the graph learning mechanism to embed structural dependencies and accurately represent cascading cyber-attacks. The propagation map afterwards is very helpful for estimating the resilience and for autonomous defense planning, as it shows critical attack paths and indicates vulnerable entities in the network, which can be mitigated in good time.

Computational Performance Analysis

The proposed MLCR-ATPAD framework was also tested in terms of the computational efficiency to ensure the feasibility of the framework for real-time cyber defense applications. The computational analysis was conducted by taking into account the efficiency of execution and the use of resources, with the same experimental conditions. To make a fair comparison between the two approaches described above, the same hardware and software environment was used for the representative deep learning and graph-based approaches. The training time, inference time, memory usage, computational overhead, defense response time and network recovery time were used to measure the performance. The lower the number, the more efficient the resources were used and the more quickly the program ran. The experimental results show that the proposed framework achieves a good trade-off between predictive performance and computational complexity, while also performing resiliently under optimization, and reduces the computational burden with compact convolutional feature extraction, graph-based dependency learning and resilience guided optimization, while maintaining a timely autonomous cyber defense capability.

The computational performance of the proposed MLCR-ATPAD is compared with CNN, GCN, GAT and Hybrid CNN-GCN models in **Table 3**. The evaluation is based on the training time, inference time, memory consumption, CPU usage, defense response time, and network recovery time under the same experimental conditions. The proposed framework showcases the balance of the computational profile by having moderate training requirements while inference latency and memory consumption are low. Moreover, the optimization based on the resilience has considerably smaller response

latency for the defense systems and speeds up network recovery than existing approaches. The findings validate the effectiveness of MLCR-ATPAD in delivering computational efficiency and adaptive cyber defense capabilities, which are essential for deployment in dynamic network environments with limited resources.

Table 3. Computational Performance Comparison of Existing Models and the Proposed MLCR-ATPAD

Method	Training Time (s)	Inference Time (ms)	Memory Usage (MB)	CPU Utilization (%)	Defense Response Latency (ms)	Recovery Time (s)
CNN [13]	168.42	15.84	452	73.8	39.5	8.42
GCN [14]	194.76	18.46	488	76.2	34.8	7.16
GAT [15]	218.95	20.13	536	80.5	31.2	6.41
Hybrid CNN-GCN [16]	243.61	22.08	574	82.9	27.4	5.68
Proposed MLCR-ATPAD	201.34	17.96	469	74.6	18.7	3.94

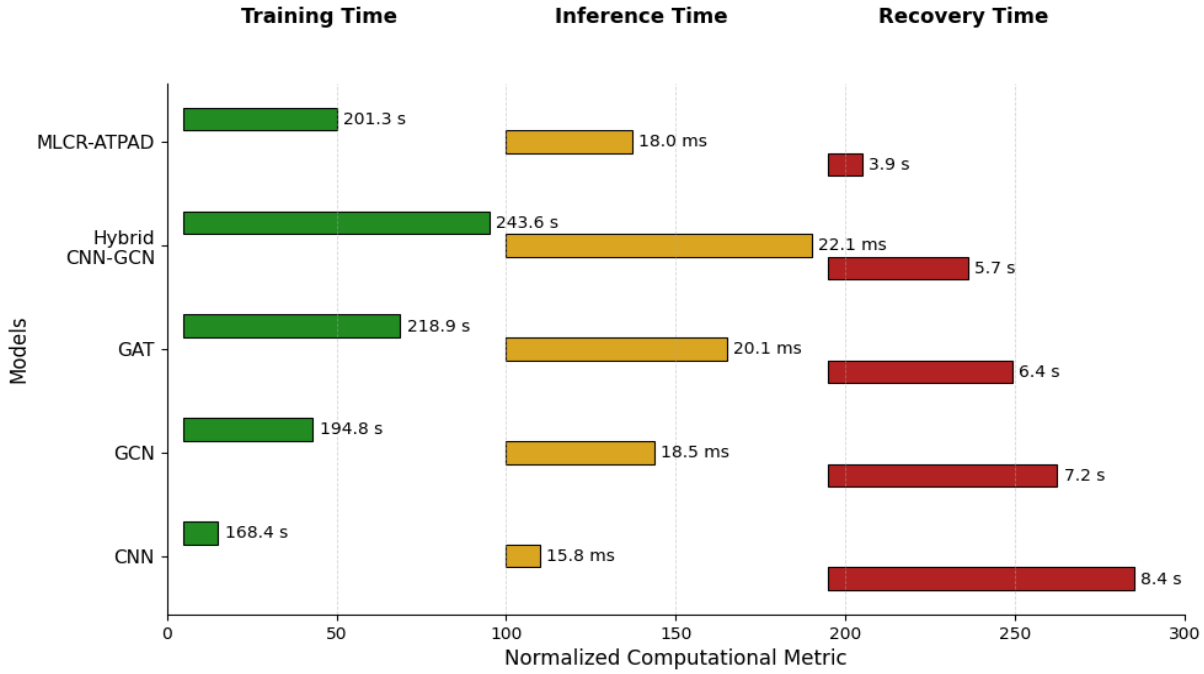

Fig 4. Computational Performance Comparison of MLCR-ATPAD and Existing Cyber Defense Models.

Fig. 4 shows the comparative computation performance of the proposed MLCR-ATPAD framework and the existing cyber defense models by training time, inference time and network recovery time. The graphical representation shows the trade-off between the approaches in terms of computational complexity and operational efficiency. The framework presents a resilient autonomous defense method that significantly speeds up network recovery during the attack while maintaining competitive training and inference performance, using graph-based methods which are generally more resource-consuming. Overall, the results show that the MLCR-ATPAD approach can effectively provide a trade-off between computational cost and execution efficiency, allowing for rapid threat mitigation and system restoration while maintaining good predictive performance in heterogeneous cybersecurity environments.

Ablation Study

An ablation study of the various computational parts was performed to study the contribution of each module in the proposed framework MLCR-ATPAD, by systematically removing one computational part at a time while keeping the other computational parts and the experimental settings unchanged. Four variants of MLCR-ATPAD were investigated: MLCR-ATPAD without CNN-based feature learning, MLCR-ATPAD without graph representation learning, MLCR-ATPAD without computational resilience modeling, and MLCR-ATPAD without autonomous defense optimization. The benchmark datasets outlined in Section 4.1 were tested for each variant. This analysis aims to measure the importance of each module in the context of cyber threat detection, cyber-resilience estimation and cyber-adaptive defense. The complete MLCR-ATPAD model is the reference implementation. The detection accuracy, F1-score, the resilience index, the threat containment rate, and the defense response latency were used to measure performance. It shows that each of the components contributes to the overall performance, and that its removal leads to a loss of performance, as observed in the experiments. Specifically, removing the graph representation learning module diminishes the model's representation of structural attack dependency, and removing the computational resilience module has a significant impact on the capability of adaptations

to mitigate threats and recovery. Likewise, eliminating the autonomous defense mechanism slows response times, and reduces the efficiency of threat containment. The results demonstrate that the proposed framework is superior owing to the synergistic combination of the convolutional feature learning, dependency modeling with graph, resilience estimation, and autonomous defense optimization.

Table 4. Ablation Study of the Proposed MLCR-ATPAD Framework

Model Configuration	Accuracy (%)	F1-Score (%)	Resilience Index	Threat Containment Rate (%)	Defense Response Latency (ms)
Without CNN Feature Learning	95.84	95.18	0.894	91.76	25.43
Without Graph Representation Learning	94.92	94.37	0.871	89.64	28.17
Without Computational Resilience Modeling	96.48	95.96	0.913	93.28	23.81
Without Autonomous Defense Optimization	96.95	96.41	0.926	94.57	22.36
Proposed MLCR-ATPAD	98.63	98.15	0.972	98.24	18.70

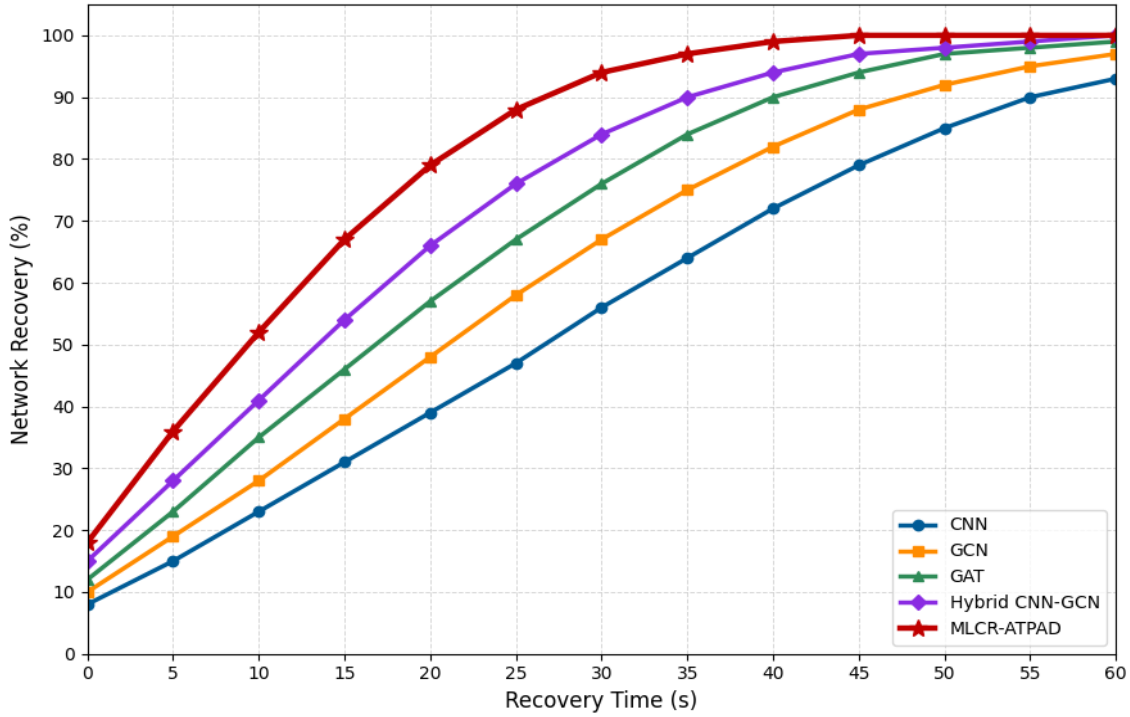

Fig 5. Network Recovery Performance of MLCR-ATPAD under Dynamic Cyber-Attack Scenarios.

The ablation study is shown in **Table 4**, to assess the impact of the individual computational elements of the proposed MLCR-ATPAD framework. Systematically, the individual modules were removed such as CNN-based feature learning, graph representation learning, computational resilience modeling and autonomous defense optimization, and all the experimental conditions were kept the same. The performance resulting from the implementation was evaluated on the basis of the following metrics: detection accuracy, F1 score, resilience index, threat containment rate and defense response latency. Overall, the integrated feature extraction, graph-based dependency analysis, resilience estimation, and autonomous defense approach within the complete MLCR-ATPAD is found to be the most effective when compared to other approaches across all the evaluation metrics. The significant performance degradation that occurs when any single module is eliminated demonstrates the critical impact each module has on improving cyber threat detection, enhancing computational resilience, increasing the speed of defense response, and increasing the overall robustness of the proposed cyber defense system.

After the attacks, the proposed MLCR-ATPAD framework is compared with CNN, GCN, GAT, and Hybrid CNN-GCN models in terms of network recovery performance as shown in **Fig. 5**. The recovery curves illustrate the percentage of network functionality regained as a function of time since autonomous defense mechanisms were launched. The proposed framework enables a significant increase in recovery rate through computational resilience modeling that incorporates adaptive graph-based threat analysis, as well as the optimization of defense using intelligence. Current techniques show slower recovery as they are not adaptable to changing attack conditions. The close approximation of the model to full network restoration in a short time demonstrates its ability to reduce service downtime and enhance cyber resilience in complex network environments.

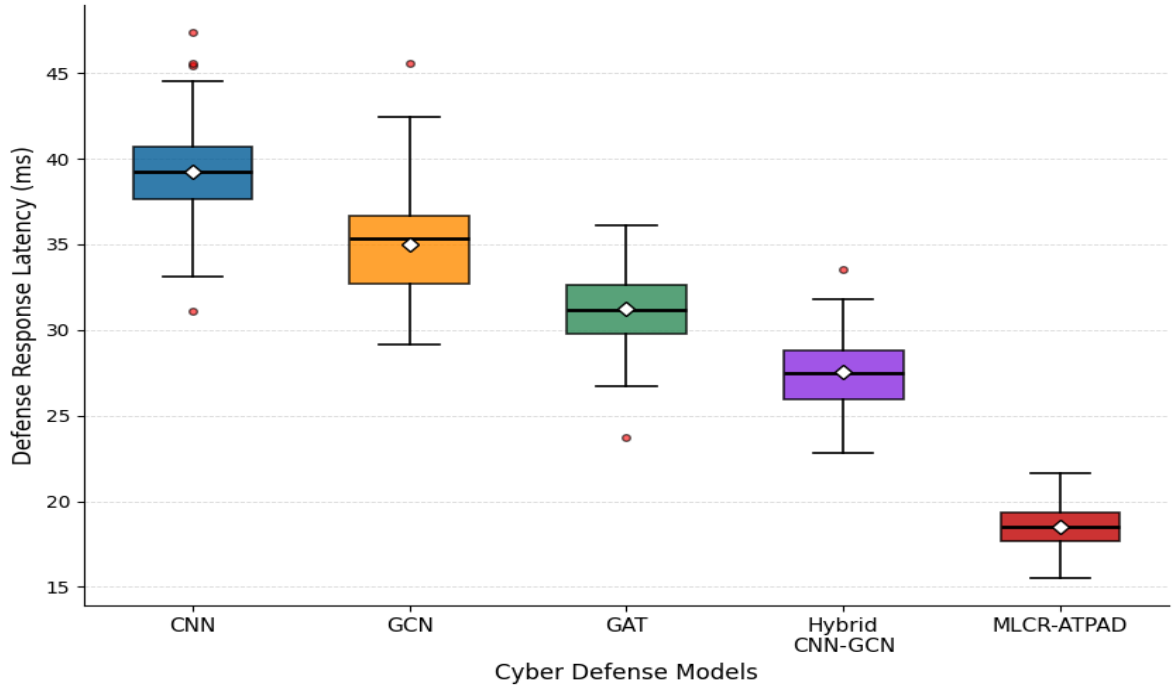

Fig 6. Defense Response Latency Distribution of Existing Models and the Proposed MLCR-ATPAD.

The defense response latencies of the evaluated cyber defense models is shown by means of a box-and-whisker plot as in **Fig. 6**. The figure shows the median, interquartile range, variability and possible outliers for several attack scenarios. The proposed MLCR-ATPAD has the lowest median response latency along with a narrow distribution, which are representative of consistent and reliable autonomous defense performance. The baseline models, on the other hand, have more variability and higher latency numbers, indicating that the responses were inconsistent in the face of dynamic cyber threats. The above observations show that the proposed framework can achieve efficient computation while rapidly and stably mitigating the threat in the heterogeneous network environment and using the resilience-aware optimization strategy.

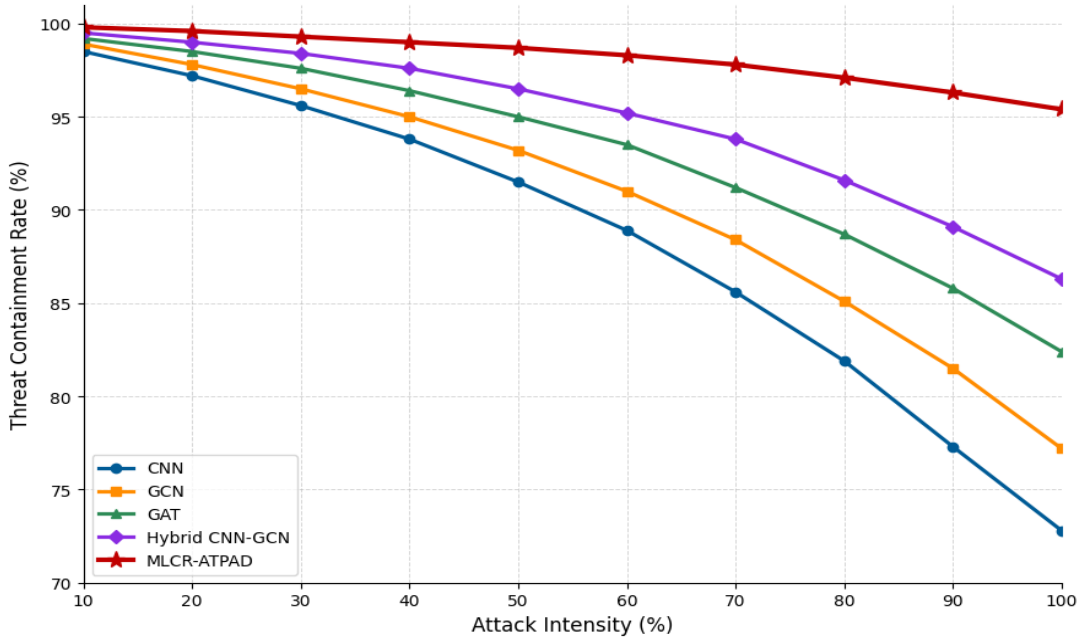

Fig 7. Threat Containment Rate under Increasing Attack Intensity.

Fig. 7 compares the threat containment capability of the proposed MLCR-ATPAD framework with existing cyber defense models as the attack intensity progressively increases. The results indicate that conventional deep learning and graph-based approaches experience a noticeable decline in containment performance under highly aggressive attack conditions. In contrast, the proposed framework maintains a consistently high containment rate by leveraging adaptive

threat propagation analysis, computational resilience estimation, and autonomous defense optimization. The gradual performance degradation remains minimal even at the highest attack intensity levels, demonstrating the robustness and scalability of the proposed mathematical model for protecting complex network infrastructures against sophisticated and evolving cyber threats.

V. CONCLUSION

This paper presented a Multi-Layer Computational Resilience Model for Adaptive Threat Propagation Analysis and Autonomous Cyber Defense (MLCR-ATPAD) to improve cyber threat detection, resilience assessment, and autonomous defense in dynamic network environments. The proposed framework integrates convolutional feature extraction, graph-based dependency learning, computational resilience modeling, and adaptive defense optimization into a unified mathematical formulation capable of analyzing complex threat propagation patterns while supporting rapid mitigation and recovery. The model was validated using recent benchmark cybersecurity datasets, including CICIoMT2024, 5G-NIDD 2024, and NF-UQ-NIDS-v2 (2025), under identical experimental conditions. Experimental results demonstrated that MLCR-ATPAD consistently outperformed conventional CNN, GCN, GAT, and Hybrid CNN-GCN approaches. The proposed framework achieved an accuracy of 98.63%, precision of 98.24%, recall of 98.07%, and an F1-score of 98.15%, while reducing the false alarm rate to 1.34%. Furthermore, it attained an AUC-ROC of 0.995 and an MCC of 0.972, confirming highly reliable classification performance. From a computational perspective, the framework required only 17.96 ms inference time, reduced the defense response latency to 18.70 ms, and achieved network recovery within 3.94 s. The ablation study further demonstrated a resilience index of 0.972 and a threat containment rate of 98.24%, confirming the contribution of each computational component. Overall, the proposed mathematical framework provides an effective, scalable, and computationally efficient solution for adaptive cyber defense and can be extended to secure future intelligent network infrastructures against sophisticated and evolving cyber threats.

CRediT Author Statement

The author reviewed the results and approved the final version of the manuscript.

Data Availability

The datasets used in this study are publicly available and can be accessed from their respective official repositories.
The dataset links are:

- CICIoMT2024 (Canadian Institute for Cybersecurity, University of New Brunswick)
  https://www.unb.ca/cic/datasets/iomt-dataset-2024.html
- 5G-NIDD Dataset (IEEE DataPort)
  https://ieee-dataport.org/open-access/5g-network-intrusion-detection-dataset-5g-nidd
- NF-UQ-NIDS-v2 (University of Queensland Network Intrusion Detection Dataset)
  https://staff.itee.uq.edu.au/marius/NIDS_datasets/

Conflicts of Interests

The authors declare that they have no conflicts of interest regarding the publication of this paper.

Funding

No funding was received for conducting this research.

Competing Interests

The authors declare no competing interests.

References

[1]. D. Jayawardena and K. Perera, "AI-Driven Cybersecurity Frameworks for Real-Time Intrusion Detection and Threat Intelligence," *Int. J. Comput. Sci. Inf. Syst.*, vol. 11, no. 7, pp. 60–77, Jul. 2026, doi: 10.55640/IJCSIS/VOLUME11ISSUE07-02.
[2]. P. C. Ike, U. C. Daniel, M. Adeoye, M. I. Amaechi, O. O. Odesola, and M. O. Ogunsakin, "Cognitive Cyber Defense Systems," *Int. J. Nature Sci. Adv. Res.*, Nov. 2025, doi: 10.70382/MEJNSAR.V10I9.075.
[3]. H. Jmal, F. B. Hmida, N. Basta, M. Ikram, M. A. Kaafar, and A. Walker, "SPGNN-API: A Transferable Graph Neural Network for Attack Paths Identification and Autonomous Mitigation," *IEEE Trans. Inf. Forensics Security*, vol. 19, pp. 1601–1613, 2024, doi: 10.1109/TIFS.2023.3338965.
[4]. H. Wang, H. Xu, K. Li, L. Yao, Y. Liu, and Z. Fu, "Learning Autonomous Defense Strategies via Multi-Agent Graph Neural Networks in Dynamic Networked Environments," in *Proc. IEEE Int. Conf. Commun. Technol. (ICCT)*, Oct. 2025, pp. 1503–1508, doi: 10.1109/ICCT67417.2025.11374172.
[5]. X. Zhang and P. Bao, "Multi-view contrastive learning for graph adversarial defense," *Neural Netw.*, vol. 192, Art. no. 107868, Dec. 2025, doi: 10.1016/j.neunet.2025.107868.
[6]. Y. Shi, H. Zhang, L. Shi, and S. Xu, "Autonomous cyber defense for AIoT using Graph Attention Network-Enhanced reinforcement learning," *Comput. Commun.*, vol. 241, Art. no. 108265, Sep. 2025, doi: 10.1016/j.comcom.2025.108265.
[7]. R. Sumathy and A. Rinu Rija, "IoT and AI-Driven Adaptive Traffic Signal Control Using Deep Reinforcement Learning and Graph Neural Networks," in *Proc. Int. Conf. Smart Struct. Syst. (ICSSS)*, Dec. 2025, pp. 1–4, doi: 10.1109/ICSSS66939.2025.11346147.
[8]. N. Kumar, M. S. Kumar, R. Suhasini, M. Lakshman, N. Anbalagan, and D. R. Krithika, "A Graph Neural Network Framework for Real Time Cyber Threat Intelligence and Risk Analysis," in *Proc. IEEE Int. Conf. Adv. Comput. Technol. (ICACT)*, Sep. 2025, pp. 630–636, doi: 10.1109/ICACT67549.2025.11351388.

[9]. H. Narne, "Enhancing IoT Cybersecurity with Graph Neural Networks: Advanced Anomaly Detection and Threat Mitigation," *Int. J. Sci. Res.*, vol. 12, no. 8, pp. 2571–2575, Aug. 2023, doi: 10.21275/SR23086105929.
[10]. L. Li, F. Qiang, and L. Ma, "Advancing Cybersecurity: Graph Neural Networks in Threat Intelligence Knowledge Graphs," in *Proc. Int. Conf. Algorithms Softw. Eng. Netw. Security*, Apr. 2024, pp. 737–741, doi: 10.1145/3677182.3677314.
[11]. Y. Wang, N. Li, D. Qiu, B. Cao, H. Xiao, and P. Zhou, "Integrating Graph Neural Networks and Dynamic Community Characterization for Advanced Persistent Threat Detection and Attack Provenance Reconstruction," *Int. J. Pattern Recognit. Artif. Intell.*, vol. 40, no. 7, Mar. 2026, doi: 10.1142/S0218001425570289.
[12]. M. Cui *et al*., "MGDA: A provenance graph-based framework for threat detection and attack scenario reconstruction," *Comput. Netw.*, vol. 274, Art. no. 111806, Jan. 2026, doi: 10.1016/j.comnet.2025.111806.
[13]. E. Manohar and K. B. Reddy, "ZT-GNN-MARL: A Zero-Trust Adaptive Cyber Défense Framework Using Graph Neural Networks and Multi-Agent Reinforcement Learning," in *Proc. Int. Conf. Knowl. Eng. Commun. Syst. (ICKECS)*, Apr. 2026, pp. 1–6, doi: 10.1109/ICKECS70176.2026.11527884.
[14]. S. Saklani, D. K. Chohan, and R. Sharma, "Zero Trust Cloud Security Using Federated Graph Neural Networks (Fed-GNN)," in *Proc. Int. Conf. Intell. Sustainable Syst. (ICISS)*, Mar. 2026, pp. 393–398, doi: 10.1109/ICISS67859.2026.11453752.
[15]. J. Yao and B. Koirala, "Defense-Aware Temporal Graph Neural Network for fault-tolerant intrusion detection in IIoT–5G environments," *Cluster Comput.*, vol. 29, no. 5, Jun. 2026, doi: 10.1007/S10586-026-06037-5.
[16]. H. Hayouni and F. Jbali, "Lightweight Neuromorphic-Temporal Graph Framework for Proactive Defense Against Evolving Cyber Attacks," *Security Privacy*, vol. 9, no. 1, Dec. 2025, doi: 10.1002/SPY2.70163.

ISSN (Online): 3105-9082