SCIENTIFIC CULTURE

www.sci-cult.com

SCIENTIFIC CULTURE, Vol. 12, No. 2.1, (2026), pp. 13969-13977
Open Access. Online & Print

DOI: 10.5281/zenodo.20489705

GRAPH NEURAL AND REINFORCEMENT LEARNING APPROACHES TO CYBERSECURITY IN NEXT-GENERATION TELECOM NETWORKS

Arun Kumar B S[1*], Rathnakar Achary[2], Asheesh Kumar Saxena[3]

[1*]*Alliance School of Advanced Computing, Alliance Univeristy Bangalore, India*
karunPHD23@ced.alliance.edu.in
[2]*Alliance School of Advanced Computing, Alliance Univeristy Bangalore, India*
rathnakar.achary@alliance.edu.in
[3]*Alliance School of Business, Alliance Univeristy Bangalore, India*
kasheeshPHD724@bus.alliance.edu.in

Received: 04/04/2026
Accepted: 20/05/2026

ABSTRACT

Rapid growth in cloud-based services has significantly broadened the reach and throughput of both national digital backbones and worldwide telecom service grids, and modern communication networks have similarly grown in scale and coverage. This shift is presently being shaped by 5G rollouts, edge processing, virtualization of network functions, and slice-based segmentation for connected IoT endpoints. With these advances, however, the attack surface has also widened. Legacy defences built around fixed rule sets and signature-driven intrusion detection no longer keep pace with such dynamic environments. Embedding AI into the telecom stack allows the enormous volumes of operational telemetry to be examined intelligently, leading to early threat recognition, automated remediation, and forward-looking defence with stronger precision. This work links a conceptual architectural blueprint with empirical evaluation on openly available intrusion benchmarks. Detection and containment of hostile activity are automated, and traffic data is examined through a reinforcement learning (RL) agent that is comparatively easier to deploy than graph neural networks (GNN) or hybrid deep-learning stacks. Open issues remain around interpretability, robustness to adversarial perturbations, and dataset quality. In the experiments reported here, GNN-based models delivered the strongest F1 score, while the RL agent brought down mean-time-to-detect by 37%. Going forward, emerging paradigms such as federated learning and autonomous network defence are expected to define the trajectory of telecom security.

Keywords— *Artificial Intelligence, Telecom Cybersecurity, Graph Neural Networks, Intrusion Detection Systems, Edge Computing, Network Virtualization.*

INTRODUCTION

Mobile broadband and the wider telecommunications fabric form a critical infrastructure on which today's digital economy fundamentally depends. Over the past decade, the once strictly hardware-bound networks have been progressively reshaped into programmable, cloud-like platforms [4][9]. A modern telecom deployment is now composed of open APIs, containerized microservices, virtualized compute resources, and decoupled radio units [17]. While capabilities such as network slicing add agility and tunable performance, they have at the same time exposed operators to a broader threat surface, much of which remains opaque both to end users and to conventional security stacks [6][7][22].

Adversaries today increasingly target the network-slice layer, where a shared physical substrate is partitioned into many logically separate virtual networks. Misconfiguration of slice policies, exposure of virtualized core elements, weakly protected orchestrators, and insecure Open Random Access Network (RAN) interfaces collectively widen the attack surface. Static rule-based or human-driven defences cannot scale here because device heterogeneity, traffic intensity, and the highly distributed nature of the architecture all vary in real time. AI is therefore a strong candidate countermeasure, both because of its analytical depth and because it may eventually become the central engine driving the security of these dynamic environments. However, prior literature does not jointly examine, in a single coherent study, the promise of AI alongside the practical risks and real-world constraints that accompany its telecom deployment [6][7]. The rest of this paper is organised as follows: Section II reviews related work, Section III presents the methodology, Section IV outlines the experimental setup, Section V discusses the results, and Section VI concludes.

I. LITERATURE REVIEW

Existing studies tend to look at narrow aspects of the problem, typically a single algorithm or one specific application scenario, rather than considering how AI integrates into the broader telecom security operations and overall network architecture. None of the surveyed works puts forward a consolidated end-to-end framework that combines proper benchmarking with automated response. The work in [1] offers a wide-ranging review of next-generation authentication and key agreement schemes for 5G, with attention to mutual authentication advances, lightweight cryptographic primitives, and replay-attack resistance. That study, however, remains largely analytical and comparative, and does not extend to experimental validation or performance benchmarking under realistic deployment conditions. In [2], the authors review both 5G and the upcoming 6G security architectures, focusing on privacy-preserving mechanisms and cross-layer mitigation of threats; their treatment, however, stays at a conceptual level and does not progress to empirical demonstration of the discussed vulnerabilities. A systematic survey is provided in [6], cataloguing threat vectors and unresolved security challenges across virtualized 5G/6G environments, although the discussion does not drill down into specific attack surfaces such as SDN controller compromise or breakdowns in slice isolation. The contribution in [9] tackles runtime security and live traffic management within 5G networks, but its scope leans toward observability rather than articulating a complete defensive framework. In [12], a resilience-oriented authentication and key agreement scheme is proposed to counter active adversaries in 5G, although the proposal has not yet been validated through peer review or production-grade deployment trials. The authors of [13] introduce a quantum-resilient 5G authentication design intended to preserve secrecy, but the additional cryptographic overhead increases both computation and end-to-end latency. The study in [14] addresses impersonation and key-compromise attacks via a multi-layer identity-based signature protocol for 5G, though it falls short on scalability for very large deployments. The work in [8] puts forward a secure MIMO-compatible model for 6G with a focus on physical-layer security; nevertheless, its integration with upper-layer authentication or slicing remains limited. In [21], risks across 5G and AWS-hosted telecom environments are analysed, with emphasis on virtualization and orchestration weaknesses, but without applying quantitative threat-modeling techniques. Finally, [22] examines the 5G security architecture and the application-layer threats it faces, contributing only modestly to the AI-driven attack surface.

Artificial intelligence Constraints in Telecom Security:

While AI is widely cited as one of the most effective tools for safeguarding modern telecom systems, several practical limitations of these dynamic systems deserve careful attention from researchers [22]. Acquiring sufficiently large, well-labelled telecom datasets is itself a significant obstacle, and building models that remain reliable across fluctuating network conditions is similarly demanding. Such conditions also create opportunities for adversarial misuse: a sophisticated attacker who understands a model's weaknesses can either craft inputs that evade detection or repurpose the classifier's outputs to their own advantage [11]. Model drift compounds the problem, since changing network behaviour over time degrades prediction quality and requires

repeated retraining to keep the system current. Beyond purely technical concerns, operators must also ensure that AI-derived decisions are explainable and meet regulatory expectations around transparency and accountability. Figure 1 illustrates the Artificial intelligence driven telecom security architecture. Deploying these models close to the network edge raises a further trade-off between computational footprint and response latency, an especially sensitive issue for latency-critical telecom workloads [17]. Taken together, these constraints suggest that AI should be applied judiciously so that innovation, resilience, interpretability, and operational viability are preserved across the cybersecurity landscape, with the broader goal of keeping the telecom ecosystem stable and consistent.

II. METHODOLOGY

To investigate the role of AI in telecom security, the study is organised around a four-part research design that combines logical structure with empirical evaluation. The first component constructs a theoretical framework for Artificial intelligence enabled telecom network security through architectural design.

- A comparative evaluation of classical machine-learning, deep-learning, graph neural network, and reinforcement-learning approaches is carried out on intrusion-detection datasets.
- Comparative interpretation, both qualitative and quantitative: the findings are then synthesised by drawing inferences from both numerical performance results and qualitative observations.

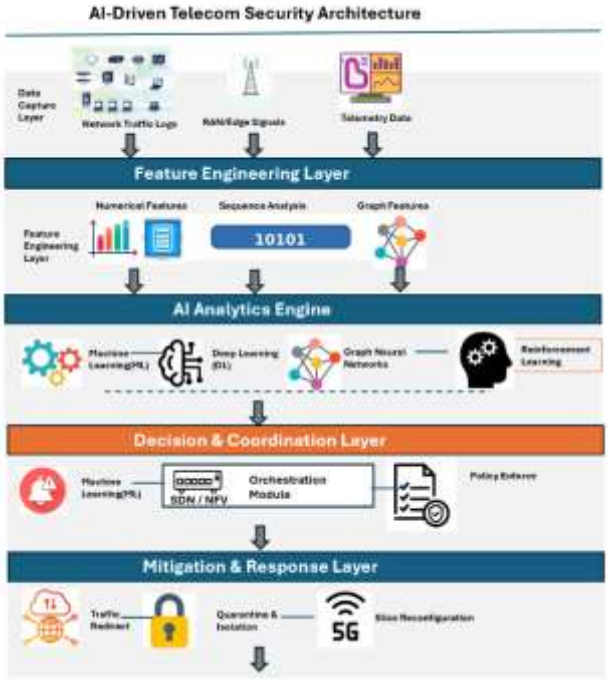

Fig. 1: Artificial Intelligence driven telecom security architecture diagram

Aligned with the operational realities of telecom networks revealed by the literature review, the architectural design groups functionality into data collection, feature engineering, analytics, decision-and-coordination, and mitigation layers. During the comparative-interpretation stage, the standard quantitative measures of accuracy, precision, recall, and ROC-AUC are complemented with assessments of robustness, scalability, and adaptability, since the numerical metrics alone do not fully capture these properties. Each technique's detection and response capability is then evaluated systematically through model evaluation. This integrated approach establishes both the technical feasibility of AI-augmented defences and a forward-looking view of how such systems can strengthen telecom security. The associated workflow is depicted in Figure 2.

Depending on which model is selected, network traffic is encoded either as a graph or as a high-dimensional sequence; GNNs rely on iterative message passing across nodes, whereas RL formulates threat response as a sequence of action choices [18]. The mathematical formulation of the machine-learning framework used to analyse telecom traffic and detect anomalies through Deep Learning, Graph Neural Network (GNN), and Reinforcement Learning (RL) is presented below:

$\mathcal{D} = \{(x_i, y_i)\}_{i=1}^{N}, y_i \in \{0,1\}$…… …..(1)

Where,

D – dataset containing telecommunication traffic attributes.

N– total number of traffic samples collected

x_i – denotes the i^{th} telecom traffic record

y_i-label associated with the traffic sample

$y_i \in \{0,1\}$

0 – indicates normal traffic

1 – indicates malicious traffic

The traffic attributes extracted from a telecommunication network typically include: [source and destination IP address, packet size, protocol type, number of packets, session duration, call duration, signal strength and latency]

For m number of samples, it is represented as

$$x_i = [f_1, f_2, f_3 \ \ldots\ldots\ldots f_m]$$

For Deep Learning, the prediction model is expressed as: $\hat{y}_i = f_o(x_i)$

y_i →predicted traffic class for the sample x_i

f_θ →the deep learning architecture (CNN, LSTM, or DNN) that learns to map telecom traffic characteristics for prediction.

θ →model parameters

As an illustration, for a given sample the feature vector may take the form:

$$x_i = [packet_{rate}, Latency, Call_{detection}]$$

If $y_i = 1$ →the sample is classified as malicious traffic.

Model parameters are obtained by solving

$$\theta^* = \arg\min_\theta L(f_\theta(x), y)$$

Where L denotes the loss function used to quantify prediction error. Typical choices for this loss include $argmin \rightarrow$ finds the parameters that minimise the loss, such as:

- Binary cross-entropy
- Mean squared error (MSE)
- Weighted loss for imbalanced traffic data

The binary cross-entropy loss is given as:

$L = -[ylog(\hat{y}) + (1-y)\log(1-\hat{y})]$

A deep learning representation: Using GNN:

A telecom network can be modelled as a graph in which the nodes correspond to base stations or devices and the edges correspond to communication links. The GNN update rule is then given by:

$$H^{(l+1)} = \sigma(AH^{(l)}W^{(l)})$$

$H^{(l+1)}$ →updated node features

$H^{(l)}$ →node feature matrix at layer l

A →adjacency matrix capturing the network connectivity

$w^{(l)}$ →trainable weight matrix

σ →non-linear activation function (e.g., ReLU or Sigmoid). GNNs are particularly effective at uncovering botnets, coordinated attacks, fraudulent call patterns, and unusual traffic propagation across the network.

Reinforcement learning -based defender optimization:

Reinforcement learning can be used to optimise the security response strategy. The optimal defence policy is given by:

$$\pi^*(s) = \arg\max_\pi \mathbb{E}\left[\sum_{t=0}^{\infty} \gamma^t R_t \mid s_0 = s\right] \ldots.(2)$$

Where,

$\pi^* \rightarrow$ optimal policy

$\pi \rightarrow$ defense policy

S →Network security state

$R_t \rightarrow$ reward at time step t

γ →Discount factor ($\theta < \gamma < 1$

E →Expectation operator

Suggested architecture for AI security: The AI-based security framework proposed here for current telecom networks follows a layered structure that mirrors today's operational workflows while strengthening their resilience against evolving cyberattacks [22]. Its main layers are:

- *Data Acquisition Layer* – ingests logs, traffic flows, and signals from RAN and edge nodes.
- Feature Engineering Layer – produces numerical, sequence-based, and graph-based representations.
- *Artificial intelligence Analytics Engine* – hosts Machine learning, Deep learning, Graph neural network, and Reinforcement learning models for detection and classification.
- *Decision & Coordination Layer* – issues actionable alerts and integrates with Software-defined networking/Network Functions Virtualization controllers.
- *Mitigation Layer* – performs automated traffic redirection, isolation, and slice reconfiguration.
- Overall, the design is scalable and aligns naturally with established telecom operational practices.

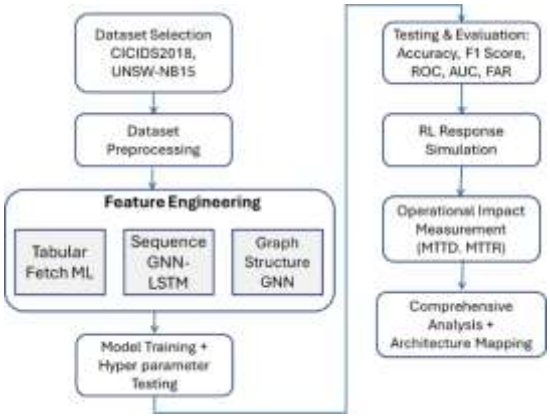

Fig. 2. Workflow Diagram

At the base of the pipeline, the data collection layer ingests logs, traffic paths, and raw signals drawn

from the radio access, core, and edge segments of the network. The feature engineering layer then converts these inputs into structured representations — graphs, sequential time-series, or numerical feature vectors — depending on the downstream model. The decision-and-coordination layer consumes the analytical results and orchestrates communication between the alerting subsystem and the SDN/NFV controllers, enabling context-aware and timely intervention. Finally, the mitigation layer limits the operational impact of an intrusion and preserves service continuity by applying automated or semi-automated countermeasures such as traffic rerouting, feature isolation, and slice reconfiguration. Because this AI-based defence pipeline maps directly onto the control policies already enforced by telecom operators, it is both practical and easily scalable for real-world deployment.

III.EXPERIMENTAL SETUP

To gauge how effectively AI-driven cybersecurity models perform in telecom settings, the experimental setup leverages two widely used benchmark datasets that were selected for their breadth and realistic traffic composition:

i. CICIDS2018 — a feature-rich corpus covering contemporary attack categories.

ii. UNSW-NB15 — provides granular flow-level records spanning a range of intrusion classes.

The samples drawn from these datasets contain residual noise, which is modelled as follows:

$$x_i^{noise} = x_i + \in$$

Where, $\in$ is the noise component.

This noise typically arises from imperfect traffic attributes — for example, inaccurate packet-size readings, unobserved sessions, mismatched IP mappings, and inconsistent timestamps. The dataset is therefore preprocessed by imputing or removing missing entries, encoding categorical variables, and discarding incomplete records. After cleaning, the data is partitioned into 70% for training and 30% for testing.

Table 1: List of models implemented

Model Type	Description
Logistic Regression	Traditional baseline
Random Forest	Ensemble classical ML
CNN + LSTM	Deep learning hybrid
GNN (GCN/GAT)	Graph-based intrusion detection
RL Defender	Adaptive threat response agent

V. RESULTS & DISCUSSION

The proposed technique is assessed against standard evaluation metrics derived from the confusion matrix, from which precision, accuracy, recall, and F1-score are computed. A threshold-independent assessment is additionally carried out using the ROC (receiver operating characteristic) curve together with the AUC (area under the curve) to characterise how well each model discriminates across different decision thresholds. The overall performance comparison is presented in Figure 3, while the algorithm-wise evaluation results are shown in Figures 4, 5, 6, and 7.

The confusion matrix is described in terms of true positives (TP), true negatives (TN), false positives (FP), and false negatives (FN).

$$\text{Precision} = \frac{TP}{TP + FP}$$

$$\text{Recall} = \frac{TP}{TP + FN}$$

$$F1 = 2 \cdot \frac{\text{Precision} \cdot \text{Recall}}{\text{Precision} + \text{Recall}}$$

***ROC-AUC (score-based)*:** It expresses the probability that the model assigns a higher score to a randomly chosen positive sample than to a randomly chosen negative one. Let the model's score function be denoted as $s(x)$.

x^+ = denotes a randomly drawn positive sample, signifying traffic that is malicious, an attack, fraudulent, or spam.

x^- = denotes a randomly drawn negative sample, indicating normal or benign traffic.

The AUC is then expressed as: AUC = $P(s(x^+) > s(x^-))$

Deep learning loss function (cross-entropy) — the cross-entropy loss quantifies the divergence between the predicted and true labels, particularly in classification settings.

$\mathcal{L}(\theta) = -\frac{1}{N}\sum_{i=1}^{N}[y_i \log(\hat{y}_i) + (1 - y_i)\log(1 - \hat{y}_i)]$…(3)

GNN message passing (Graph Convolution)

Graph $G = (V, E)$, node features $h_v^{(0)}$.

$$h_v^{(k+1)} = \sigma\left(W^{(k)} \sum_{u \in \mathcal{N}(v) \cup \{v\}} \frac{1}{c_{vu}} h_u^{(k)}\right) \ldots\ldots\ldots(4)$$

Where:

$\mathcal{N}(v)$= neighbors; c_{vu}= normalization constant
σ= activation
This expression encodes the update rule of a graph convolutional network and describes how each node refreshes its feature vector by aggregating signals from its neighbourhood. In other words, every node revises its representation by merging its own features with those of its neighbours, then applying normalisation, a learnable linear transformation, and a non-linear activation.
Reinforcement learning defender-Markov Decision Process(MDP) formulation: It defines;

- State s_t: traffic/security context
- Action a_t: mitigation action (block, rate-limit, isolate slice, etc.)
- Reward r_t: security gain and cost

Objective:

$$\pi^* = \arg\max_{\pi} \mathbb{E}\left[\sum_{t=0}^{T} \gamma^t r_t\right] \text{.....(5)}$$

Q-learning update:

$$Q(s_t, a_t) \leftarrow Q(s_t, a_t) + \alpha\left[r_t + \gamma \max_{a} Q(s_{t+1}, a) - Q(s_t, a_t)\right] \text{.....(6)}$$

Equation (6) formalises an RL-based cyber-defender within an MDP framework. This is a well-established way to model an autonomous security agent that progressively learns optimal mitigation behaviour. The defender observes the prevailing network or security state, selects a mitigation action, receives a reward proportional to how effective that action proves to be, and over time converges on a policy that maximises long-term security gain. Telecom SOC metrics: these performance indicators capture how responsive the security operations centre (SOC) is. The mean time to detect (MTTD), defined in Equation (7), is the first such metric.

$$MTTD = \frac{1}{M}\sum_{j=1}^{M}(t_j^{detect} - t_j^{start}) \text{.....(7)}$$

For each incident j:

- t_j^{start}= time at which the attack/incident began
- t_j^{detect}= time at which the SOC detected the incident

So: $t_j^{detect} - t_j^{start}$ = detection delay for that incident.
Then Mincidents are then averaged. In effect, MTTD captures how long, on average, the SOC takes to notice an incident after it has begun.
A lower MTTD therefore indicates stronger monitoring and quicker detection.
Mean Time to Repair (MTTR):

$$MTTR = \frac{1}{M}\sum_{j=1}^{M}(t_j^{resolve} - t_j^{detect}) \text{.....(8)}$$

For each incident j:

- t_j^{detect}= time at which the incident was detected
- $t_j^{resolve}$= time at which the incident was contained and resolved

So: $t_j^{resolve} - t_j^{detect}$ = response + remediation time.
MTTR therefore reflects how long, on average, the SOC needs to contain and resolve an incident once it has been detected.
A lower MTTR indicates stronger response capability and a higher degree of automation.

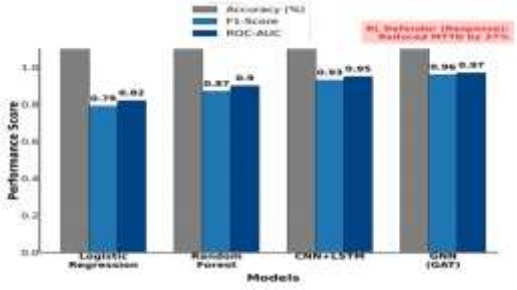

Fig. 3: Performance comparison

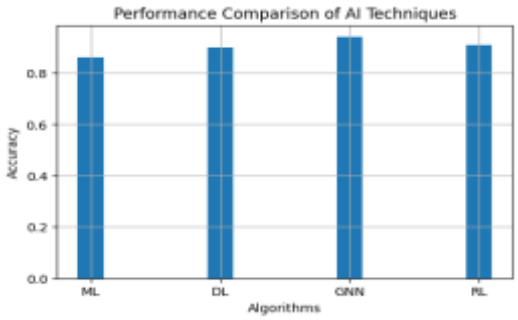

Fig. 4. F1 Score Comparison

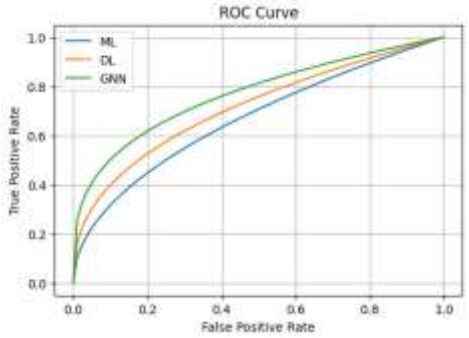

Fig. 5. ROC Curve False Positive comparison

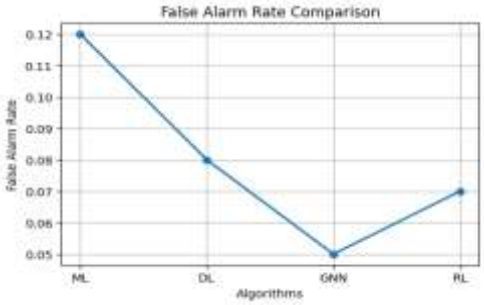

Fig. 6. False Alaram Rate Comparison

A comparison of MTTD, MTTR, and the false-alarm rate before and after automation appears in Figure 8. The bar chart in Figure 9 summarises the accuracy of several machine-learning classifiers on intrusion prediction across four datasets (KDD99, Supplied KDD99, UNSW-NB15, and Supplied UNSW-NB15). On the KDD99 family of datasets, most classifiers attain reasonably high accuracy; however, when evaluated on UNSW-NB15, classifier accuracy drops sharply. Ensemble and tree-based methods such as Random Forest (RF), Hoeffding Tree (HT), and Decision Tree (DT) generally outperform the remaining classifiers.

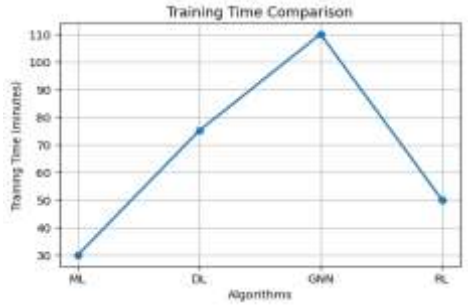

Fig. 7. Training Time Comparison

Fig. 8. MTTD and MTTR False Alaram Rate Comparison

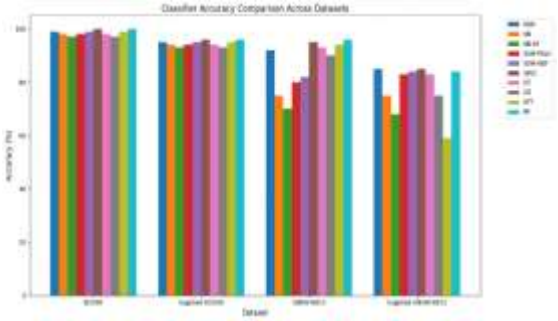

Fig. 9. Comparative Analysis of several machine-learning classifiers using different intrusion detection datasets.

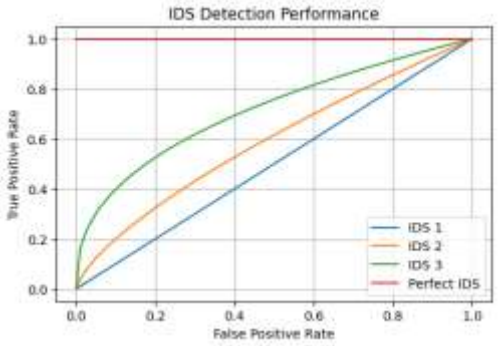

Fig. 10. The differences in the finding performances and trade-offs in the false alarms of IDS 1, IDS 2 and IDS 3 as compared to the ideal intrusion detector.

Figure 10 contrasts the behaviour of IDS 1, IDS 2, and IDS 3 with that of an ideal reference system, referred to as the Perfect IDS. Comparing their true-positive rates shows that IDS 3 achieves the highest detection rate while keeping false positives low, indicating that IDS 3 is markedly more sensitive to controlling false alarms than the other two systems. IDS 1 performs the worst, with a curve that sits close to the diagonal and therefore reflects weak discrimination. The Perfect IDS curve represents the theoretical upper

bound, exhibiting zero false alarms and 100% detection.

The GNN-based models delivered the strongest overall results, achieving recall above 96% together with overall accuracy near the 96% mark. The CNN-LSTM hybrid also performed well, particularly in capturing the temporal dynamics of network traffic. By comparison, traditional machine-learning techniques lagged behind, especially on complex, multi-stage attack patterns. A further benefit of the RL agent was a substantial reduction in response time, which makes it a promising fit for automated mitigation, although this gain does not, on its own, raise detection accuracy.

VI. CONCLUSION

As telecom networks become progressively more virtualised, complex, and geographically distributed, cybersecurity can no longer rely solely on traditional detection systems. Examining the trade-offs between response speed, accuracy, and adaptability, this study demonstrates that AI techniques — particularly GNN and RL — are highly applicable to securing modern telecom infrastructure. The findings also surface lingering concerns around interpretability and operational integration, even as AI continues to look like a strong foundation for protecting future generations of telecom networks. Subsequent work should therefore concentrate on building transparent, dependable, and collaborative AI solutions tailored to large-scale telecom deployments.

REFERENCES

1. S. K. Patel, S. B. Verma, B. K. Gupta, S. Singh, E. Naresh and P. K. Pareek, “Advances in authentication and security protocols for 5G networks: A comprehensive survey,” *Discover Appl. Sci.*, vol. 7, art. no. 743, 2025.
2. K. Rajesh and P. Vetrivelan, “Comprehensive analysis on 5G and 6G wireless network security and privacy,” *Telecommunication Systems*, vol. 88, no. 2, Art. 52, Apr. 2025.
3. M. Domb, B. C. G. Symbiosis, M. S., G. A. and S. Joshi, “Securing 5G networks by mitigating cybersecurity risks for transformative applications,” *Int. J. Interact. Mobile Technol. (iJIM)*, vol. 19, no. 11, pp. 227–255, Jun. 2025.
4. K. Cherladine, “Cybersecurity challenges and solutions in 5G SA and AWS cloud-based telecom networks,” *J. Inf. Syst. Eng. Manage.*, vol. 9, no. 4, 2024.

5. L. Lakhani and R. C. Sachan, "Securing wireless networks against emerging threats: An overview of protocols and solutions," *J. Sci. Technol.*, vol. 5, no. 4, pp. 132–158, Oct. 2024.
6. P. Scalise et al., "A systematic survey on 5G and 6G security considerations, challenges, trends, and research areas," *Future Internet*, vol. 16, no. 3, art. 67, Feb. 2024.
7. *5G Security: Challenges, Opportunities, and the Road Ahead*, *Future Internet* (MDPI) Special Issue (2024).
8. Su, Y., Gao, H. and Zhang, S., "Secure massive MIMO system with two-way relay cooperative transmission in 6G networks," *EURASIP J. Wireless Commun. Network.*, 2023 (indexed, relevance to 2024-25 context).
9. Soldani, D., et al., "EBPF: A new approach to cloud-native observability, networking and security for 5G and future mobile networks," *IEEE Access*, 2023 (security in cloud-native 5G/6G).
10. IEEE survey: *A survey on security and privacy of 5G technologies: potential solutions, recent advancements, and future directions*, IEEE Xplore.
11. Keyvan Ramezanpour et al., "Security and privacy vulnerabilities of 5G/6G and WiFi 6: Survey and research directions," arXiv, 2022 (context for research gap).
12. N. H. Sultan et al., "Active attack resilience in 5G: A new take on authentication and key agreement," arXiv, Jul. 2025.
13. Y. Ko, I. W. A. J. Pawana and I. You, "5G-AKA-HPQC: Hybrid post-quantum cryptography protocol for quantum-resilient 5G primary authentication with forward secrecy," arXiv, Feb. 2025.
14. Y. Dong, R. Behnia, A. A. Yavuz and S. R. Hussain, "Securing 5G bootstrapping: A two-layer IBS authentication protocol," arXiv, Feb. 2025.
15. S. Darzi et al., "Authentication against insecure bootstrapping for 5G networks: Feasibility, resiliency, and transitional solutions in the post-quantum era," arXiv, Oct. 2025.
16. IEEE Access — covering 5G and future network security (ongoing articles).
17. Telecommunication Systems — security and privacy in next-gen wireless networks (88(2):2025).
18. Journal of Digital Communications — security threats & prevention in 5G mobile networks (2025).
19. International Journal of Interactive Mobile Technologies (iJIM) — securing 5G cybersecurity (2025).
20. Journal of Science & Technology — wireless network security overview (2024).
21. Journal of Inf. Syst. Eng. & Management — 5G cloud telecom security mechanisms (2024).
22. IEEE Xplore survey on 5G security & privacy (2023).
23. Future Internet (MDPI) special issue on 5G security (2024).
24. Telecommunication Systems — research on 5G/6G network security (2025).
25. Discover Applied Sciences — 5G authentication protocols survey (2025).