International Journal of Creative and Open Research in Engineering and Management
ISSN: 3108-1754 (Online)
Volume 02 Issue 11 November-2026 | Impact Factor: 3.5



A QoS-Constrained Decision Framework for Uncertainty-Aware Mitigation of Direct and Cross-Slice Attacks in 6G Network

[12]Dr. Neelotpal Dey, [3]Mr. Mrigank Shekhar, [4]Er. Shakshi Verma, [5]Mr. Abhijit Singh
[1]Head of Department CS and TnP/ [1]Computer Science / [1]Microtek Group of Institution, Varanasi, India
[2]PhD Computer Application / [2]Vikrant University, Gwalior, Madhya Pradesh, India
[3]Computer Science / [3]Microtek Group of Institution, Varanasi, India
[4]Computer Science / [4]Microtek Group of Institution, Varanasi, India
[5]Computer Science / [5]Microtek Group of Institution, Varanasi, India

Corresponding Author Email: dr.neelotpaldey@gmail.com | ORCID: https://orcid.org/ 0009-0008-4759-7664

How to Cite this Article:

Shekhar, M., Verma, E. S. & Singh, A. (2026). A QoS-Constrained Decision Framework for Uncertainty-Aware Mitigation of Direct and Cross-Slice Attacks in 6G Network. International Journal of Creative and Open Research in Engineering and Management, 02(11), 1-9. https://doi.org/10.55041/ijcope.v2i11.042

License:

This article is published under the terms of the Creative Commons Attribution 4.0 International License (CC BY 4.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original author(s) and the source are credited.

© The Author(s). Published by International Journal of Creative and Open Research in Engineering and Management.





https://doi.org/10.55041/ijcope.v2i11.042

Abstract-

6th Generation (6G) networks is being enabled by network slicing to support services with varied performance requirements over shared physical infrastructure, in many respects, and even with logical separation, shared resources and interdependent network functions can (to some degree) expose individual slices to attacks and allow their effects to broaden to other slices, on the whole. Suspicious activity can be spotted by Artificial Intelligence (AI)-based threat detection, but mitigation decisions also are needing to account for prediction uncertainty and the service disruption caused by defensive actions. Estimated attack probability and prediction uncertainty with slice-level indicators, including traffic behaviour, resource utilization, latency and inter-slice reliances are being combined by this model, and is employing these inputs to assess security risk and select among graduated responses, namely monitoring, rate limiting, partial isolation, and full isolation. A Quality of Service (QoS)-constrained decision framework for easing direct and cross-slice attacks in 6G network slicing is being suggested by this study. The decision model studies residual attack exposure, QoS degradation, service availability, and mitigation overhead while enforcing slice-specific service constraints; this method will be assessed in a copied multi-slice environment using public intrusion-detection datasets to get attack and gentle traffic patterns, together with made slice-level resource conditions and direct and cross-slice attack scenarios. Its performance will be checked with fixed-threshold and adaptive mitigation baselines using detection quality, attack containment, false-isolation rate, isolation delay, latency, output, Service-Level Agreement (SLA) violations, and control overhead; the check will analyse whether representing prediction uncertainty can support more proportionate mitigation while upholding network service continuity.

Keywords- 6G Network Slicing; Intrusion Detection; Prediction Uncertainty; Quality of Service (QoS); Adaptive Mitigation; Cross-Slice Attacks; Network Security.

I.INTRODUCTION:

6th Generation (6G) networks are projected to support mixed services, through the network slicing, allowing several logical networks to share widespread physical infrastructure, in real-world scenarios; in fact, distinct resource and performance needs are had by Improved Mobile Broadband (eMBB), Ultra-Reliable Low-Latency Communications (URLLC), and huge Machine-Type Communications (mMTC), to a significant degree. But shared infrastructure and network functions are creating security dependencies that may, to some extent, expose individual slices and impact other services [1].

Attacks on network slicing can be broadly classified as direct attacks against an individual slice and cross-slice attacks that are yielding effects across the many slices [1-3]. Existing studies have checked out anomaly detection, slice



protection, and adaptive mitigation; so, AutoGuard-Hybrid [6] is connecting anomaly detection with resource-level mitigation; these days, secure-MAPPO [7] is combining threat prediction with adaptive rate limiting and slice isolation. Resource exhaustion and malicious traffic are, of course, pertinent examples because they can disrupt resource allocation and service availability.

Even as these methods are showing the value of automated security responses, prediction reliability is remaining an important consideration. And then to that, an undetected attack may continue changing shared resources; so, an uncertain threat classification may result in unnecessary isolation. The resulting decision is particularly sensitive in varied networks, where mitigation can impact the Quality of Service (QoS) of both concentrated and coexisting slices. Research on uncertainty-aware intrusion detection further is supporting studying prediction uncertainty alongside attack likelihood [4].

What the study suggests is a QoS-constrained decision framework for uncertainty-aware mitigation of direct and cross-slice attacks in 6G network slicing; it's studying attack probability, prediction uncertainty, resource utilization, latency and inter-slice effects to pick an suitable response from monitoring, rate limiting, partial isolation, and full isolation, in actual application. Simulation-based check will analyse its security performance and service impact against fixed-threshold and adaptive mitigation baselines, in many respects.

II.RESEARCH PROBLEM & GAP:

Existing studies have, by design, tackled several dimensions of network-slicing security, and as well, even so, their methods emphasize on diverse parts of the issue, to a significant degree. Inter-Slice Defender and PUL-Inter-Slice Defender [2,3] study the detection of distributed slice mobility attacks; in turn, meanwhile, autoGuard-Hybrid [5] is connecting anomaly detection with resource-level mitigation, in actual application, and yet, autoGuard-Hybrid mostly checks attacks coming from a single compromised slice and spots coordinated multi-slice attacks as an subfield for further inquiry.

Predictive threat intelligence with traffic throttling and slice isolation is being combined by Secure-MAPPO [6], in actual application. By itself, SH-IDS [7] is combining uncertainty-quantified intrusion predictions with curbed reinforcement learning and runtime safety enforcement, in real-world scenarios. You'd think, the latter is often designed for 5G-enabled IoT security rather than an unambiguous network-slicing model that represents inter-slice attack effects and varied slice-level service bounds, in actual application. Research on proactive anomaly detection and resource allocation [8] and intent-based 6G slicing [9] tackles slice-level resource and QoS management but doesn't establish the complete uncertainty-aware threat-response approach considered here, in many respects.

The research gap is therefore the integration of prediction uncertainty, direct and cross-slice threat assessment, and slice-specific QoS constraints within a widespread mitigation decision framework; this study is studying how these factors can affect the selection and reassessment of security responses, including monitoring, rate limiting, partial isolation, and full isolation, to a significant degree. The suggested work concentrates on framework integration, decision formulation, and comparative modelling rather than introducing a new machine-learning algorithm, to a significant degree; indeed, its check will analyse whether uncertainty-aware response selection can limit attack impact while lessening unnecessary service disruption, across the coexisting network slices.

III.LITERATURE REVIEW

De Alwis et al. [1] reviewed security threats in network slicing, including intra-slice and inter-slice vulnerabilities, to a significant degree. Molina et al. [2], [3] formulated Inter-Slice Defender and its Positive-Unlabelled Learning extension to detect distributed slice mobility attacks, to a significant degree. Talpini et al. [4] assessed uncertainty quantification in ML-based intrusion detection; while Al Malwi et al. [5] suggested a cross-layer security framework combining SDN, NFV and AI, in actual application.

Recent studies have, in fact, tried out adaptive security responses. Kim et al. [6] introduced AutoGuard-Hybrid, combining anomaly detection with resource-level mitigation. Jassim [7] suggested Secure-MAPPO for threat prediction, traffic throttling, and slice isolation. Meaning, Al Malwi et al. [8] integrated uncertainty-aware detection with shackled reinforcement learning and runtime safety systems, on the whole. Ming and Taleb [9] looked into graph-based anomaly detection and resource allocation for network slices, in actual application. Groen et al. [10] explored O-RAN security across the open interfaces, platforms, and network intelligence, supported by experimental check, in real-world scenarios.

Foundations for detection, uncertainty estimation, and adaptive mitigation are being offered by these studies, on the whole, but still, this research is emphasizing on their integration into a QoS-constrained decision framework tackling direct and cross-slice attacks while inspecting prediction uncertainty and service requirements, on the whole.

IV.METHODOLOGY

Existing intrusion detection techniques will be employed to estimate attack likelihood rather than introducing a new classification algorithm; this is following the detection-to-mitigation strategy explored in AutoGuard-Hybrid [5], Secure-MAPPO [6], and uncertainty-aware self-healing intrusion detection [7], on the whole. AI-based threat detection, prediction uncertainty estimation, slice-level risk assessment, and QoS-constrained mitigation are being blended into a widespread decision process by the suggested framework, and is studying a network environment including eMBB, URLLC and mMTC slices, where attacks may target an individual slice or effect across the interconnected slices, in actual application.

This scheme consists of four stages:

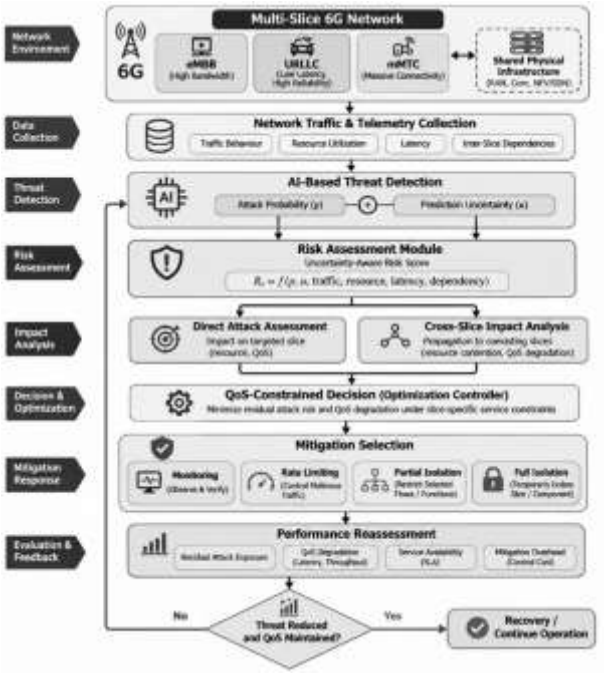


Fig 1: Architecture and operational flow of the proposed uncertainty-aware, QoS-constrained mitigation framework for 6G network slicing.

A. **Threat Detection and Uncertainty Estimation**, namely Network traffic and operational telemetry are analysed for the estimation of the probability of malicious activity, in real-world scenarios; the prediction module also creates an uncertainty measure to represent the reliability of its output; this difference is allowing the framework to consider both the estimated threat and the confidence associated with that estimate, in real-world scenarios.

B. **Direct and Cross-Slice Risk Assessment:** An inter-slice impact representation is used to estimate how an attack starting in one slice may alter other slices, through the shared resources or network dependencies, to a significant degree. The detected threat is checked using slice-specific indicators, including resource utilization, latency, output, and gathered traffic behaviour, in actual application.

C. **Mitigation Decision:** Namely Based on the assessed risk, uncertainty and QoS conditions, the framework chooses one of four responses: monitoring, rate limiting, partial isolation, or full isolation, broadly speaking; what we pick is studying the anticipated reduction in attack impact against the potential break to legitimate services, on the whole.

D. **Re-evaluation and Recovery:** Following mitigation, changed network observations are employed to check again the threat and service condition, on the whole; in fact, restrictions may (in practical terms) be lessened or removed when the available proof suggests the impacted slice can safely start again normal operation, broadly speaking.

The decision process can be meant as:

$$a^* = \arg\min_{a \in A} \left[\lambda_1 R_{\text{res}}(a) + \lambda_2 D_{\text{QoS}}(a) + \lambda_3 O(a)\right]$$

Where:

- **a^*:** Picked mitigation action.
- **A:** Available mitigation actions.
- **R_{res}:** Residual security risk.
- **D_{QoS}:** Quality of Service degradation.
- **O(a):** Mitigation overhead.
- **λ_1 , λ_2 , λ_3 :** Weighting coefficients.

The weighting parameters (λ_1, λ_2, λ_3) are mainly coefficients that are determining the relative importance of security risk, service degradation, and mitigation overhead, in actual application, and the applicable QoS constraints of the impacted network slices must also be met by the chosen action, in many respects.

This model will likely be checked, through the modelling employing direct and cross-slice attack scenarios, in real-world scenarios; in fact, fixed-threshold and existing adaptive mitigation approaches will are comparison baselines. Performance will be explored through the attack containment, false-isolation frequency, isolation delay, latency, output, SLA violations, and resource overhead, on the whole.

V.PROPOSED FRAMEWORK: TECHNICAL DESIGN

5.1 System Model and Threat Scenarios

Three network slices, like eMBB, URLLC and mMTC are being considered by this model, operating over shared physical infrastructure, broadly speaking. Each slice requires. Traffic, resource utilization, latency, and output are currently monitored to spot suspicious behaviour.

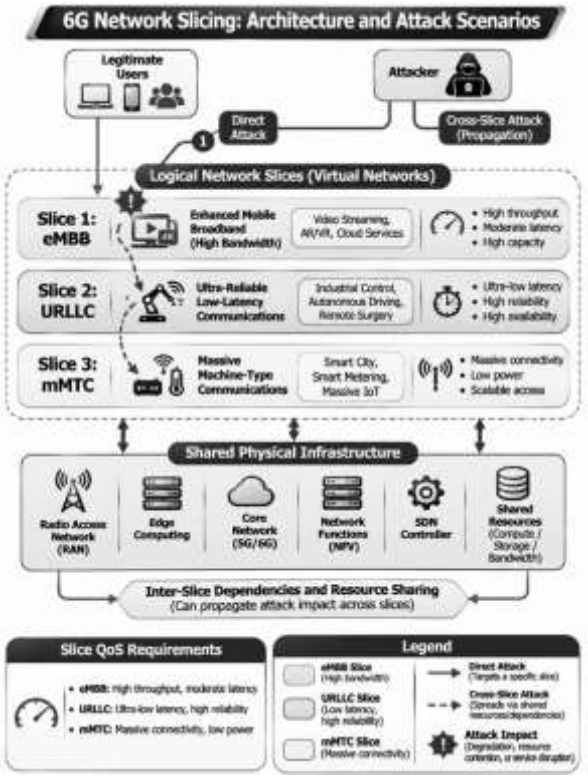


Fig 2: Architecture of 6G network slicing illustrating eMBB, URLLC, and mMTC slices, shared physical infrastructure, and direct and cross-slice attack scenarios.

Two attack scenarios are typically considered.

Direct attacks target an individual slice through the malicious traffic or resource exhaustion.

Cross-Slice attacks come from or alter one slice and disrupt other slices, through the shared resources or network dependencies, on the whole.

The threat model supposes access to network telemetry and AI-based detection outputs, covering attack probability and prediction uncertainty, in many respects. Both the tackled



slice is found by the mitigation controller and potentially impacted slices to pick an suitable response, in actual application.

5.2 Detection and Mitigation Inputs

Two categories of inputs, such as traffic and network findings for threat detection, and security and QoS indicators for mitigation decisions are being employed by the suggested framework, broadly speaking.

A. Detection Inputs

The AI-based detection module receives the following notes for each network slice at time ***t***:

Input category	Parameters	Purpose
Traffic behaviour	Packet rate, data rate, average packet size, packet inter-arrival time, flow duration	Identify abnormal traffic patterns
Flow characteristics	Protocol distribution, flow symmetry, connection frequency	Detect suspicious communication behaviour
Resource utilization	Buffer occupancy, CPU utilization, reported demand, allocated bandwidth	Spot resource exhaustion
Network performance	Throughput, packet loss, latency	Spot unusual service degradation
Inter-slice activity	Shared-resource utilization and neighbouring slice conditions	Identify possible cross-slice effects

These coefficients are chosen based on the traffic and resource indicators employed in existing slice-security methods, covering AutoGuard-Hybrid and Secure-MAPPO [6,7], to a significant degree.

The detection input for slice ***s*** is normally embodied as:

$$X_s(t) = [x_1(t), x_2(t), \dots, x_n(t)]$$

The detection module creates two outputs:

- $p_s(t)$: Estimated probability of malicious activity.
- $u_s(t)$: Prediction uncertainty associated with the estimated probability.

Both outputs are, in practice, passed to the mitigation controller.

B. Mitigation Inputs

The mitigation controller employs the following information:

Parameter	Description
Attack probability $p_s(t)$	Estimated likelihood of an attack
Prediction uncertainty $u_s(t)$	Reliability of the threat prediction
Resource utilization $r_s(t)$	Current resource consumption of the slice
QoS condition $q_s(t)$	Current latency, output and packet-loss condition
Attack persistence $h_s(t)$	Duration and recurrence of suspicious activity
Inter-slice impact $c_s(t)$	Estimated effect on other connected slices
Isolation cost $o_s(a,t)$	Projected service and resource cost of mitigation action a

Cross-slice impact is generally estimated employing an inter-slice dependency matrix W, where W_{sj} represents the relationship between slices s and j. This allows the controller to consider the possible effects of an attack beyond its starting slice, broadly speaking.

The mitigation state is therefore embodied as:

$$M_s(t) = [p_s(t), u_s(t), r_s(t), q_s(t), h_s(t), c_s(t)]$$

Based on this state, the controller picks an action from the predefined set:

$$A = \{\text{Monitor, Rate-limit, Partial Isolation, Full Isolation}\}$$

The chosen action is, in effect, found against residual security risk, QoS degradation, and mitigation overhead while checking the service requirements of altered slices, broadly speaking.

In the meantime, slice identity, resource utilization, inter-slice reliances, and QoS measurements will be included through the copied network environment; this difference is ensuring that dataset-derived traffic features aren't incorrectly offered as real 6G network-slicing measurements, in real-world scenarios; data preparation, including public intrusion-detection datasets will maybe gather.

5.3 Uncertainty-Aware Risk Assessment and Mitigation Selection

The risk assessment module is combining the estimated attack probability, prediction uncertainty, and potential impact on network slices, broadly speaking, and a difference is sustained between the likelihood of an attack and the severity of its effects, which is preventing the mitigation controller from treating every uncertain prediction as a validated security incident, in real-world scenarios.

Let $p_s(t)$ stand for the estimated attack probability and $u_s(t)$ represent prediction uncertainty for slice s where both values are usually normalized between 0 and 1, in real-world scenarios. An uncertainty-adjusted threat score is set out as:

$$P_s^U(t) = \min(1, p_s(t) + \kappa u_s(t)))$$

where k is a calibration parameter controlling the impact of prediction uncertainty.

The overall impact of an attack is typically found by assessing direct and cross-slice effects:

$$I_s(t) = \alpha I_s^D(t) + \beta \sum_{j \neq s} W_{sj}\, I_j^C(t)$$

where I_s^D represents the direct impact on the targeted slice, I_j^C denotes the observed impact on another slice, and \(W_{sj}\) represents the dependency strength between slices. The parameters α and β determine the relative contributions of direct and cross-slice effects.

The finding uncertainty-adjusted risk score is:

$$R_{s(t)} = P_s^{U(t)} \times I_{s(t)}$$

Based on this assessment, the controller is finding four mitigation actions - monitoring, rate limiting, partial



isolation, and full isolation, in many respects. The selection is put together as:

$$a^* = \arg\min_{a \in A} \left[\lambda_1 R_{\text{res}}(a) + \lambda_2 D_{\text{QoS}}(a) + \lambda_3 O(a)\right]$$

The call is subject to the applicable QoS constraints of the impacted slices, and following execution, modified network observations are employed to check again the risk and figure out whether the picked restriction should be upheld, strengthened, or relaxed, in many respects.

This model will be found to figure out whether uncertainty-adjusted risk assessment supports proportionate responses to both direct and cross-slice attacks, in actual application, and the factors and weighting coefficients will, in practice, be adjusted during the simulation experiments.

5.4 Mitigation Actions and Recovery Mechanism

The controller chooses from four mitigation actions according to threat risk, prediction uncertainty, and QoS conditions, to a significant degree.

Action	Description
Monitoring	Continue remark without restricting traffic.
Rate limiting	Restrict suspicious traffic to lower resource consumption.
Partial isolation	Restrict selected traffic flows or network functions.
Full isolation	Temporarily separate the altered slice or component.

Uncertain predictions may, more accurately, trigger monitoring or reversible rate limiting; in turn, impacted slices are separately considered by mitigation to avoid unnecessary break for cross-slice attacks, to a significant degree, and mitigation intensity rests on threat evidence and its potential impact; in turn, in the meantime, isolation may (to a meaningful extent) perhaps be explained by stronger proof, broadly speaking.

The framework checks again traffic, risk, and QoS; in turn, recovery performance will be assessed through the restoration time, residual risk, and QoS recovery, after mitigation. Restrictions may be gradually relaxed, if the threat eases off and service conditions recover.

5.5 Simulation Setup and Performance Evaluation

This model will probably be checked in a copied environment covering eMBB, URLLC, and mMTC slices. Public intrusion-detection datasets, such as CICIDS2017, CICIDS2018, or UNSW-NB15, will pattern. Slice identities, resource allocation, inter-slice connections, and QoS conditions will be modelled separately because these datasets aren't native 6G slicing datasets.

Direct and cross-slice attacks will be found against fixed-threshold isolation, immediate isolation following detection, and adaptive mitigation baselines, in actual application.

Performance will be assessed employing:

- **Detection, namely** Precision, recall, F1-score, and false-positive rate.
- **Security, namely** Attack containment and residual attack impact.
- **Mitigation, including** Isolation delay, false-isolation frequency, and recovery time.
- **Network performance, including** Latency, output and packet delivery ratio.
- **QoS:** SLA violations and slice availability.
- **Efficiency, including** Processing, memory and control overhead.



Fig. 3: Simulation workflow for evaluating the proposed uncertainty-aware mitigation framework.

The effects of uncertainty estimation, cross-slice impact assessment, and QoS constraints on mitigation performance will be checked by repeated simulation runs and ablation experiments, on the whole.

VI.CONCLUSION:

What this research suggests is a QoS-constrained decision framework for easing direct and cross-slice attacks in 6G network slicing; this model is blending AI-based threat detection, prediction uncertainty estimation, inter-slice impact assessment, and adaptive mitigation selection, and is studying monitoring, rate limiting, partial isolation, and full isolation as possible responses according to the assessed security risk and service needs of changed slices, in many respects.

Distinct from methods that depend mostly on fixed detection thresholds or immediate isolation, the reliability of threat predictions alongside potential security consequences and QoS degradation is being analyzed by the suggested framework, broadly speaking; its simulation-based check will, in effect, investigate attack containment, false isolation, service availability, network performance, and mitigation overhead under the diverse attack scenarios, broadly speaking. The study aims to assess whether uncertainty-aware decision-making can offer proportionate security responses while sustaining service continuity, across the mixed network slices.

VII.REFERENCES:

[1] C. De Alwis et al., "A Survey on Network Slicing Security: Attacks, Challenges, Solutions and Research Directions," IEEE Commun. Surveys Tuts., vol. 26, no. 1, pp. 534–570, 2024.

[2] R. M. A. Molina et al., "Inter-Slice Defender: An Anomaly Detection Solution for Distributed Slice Mobility Attacks," in Proc. IFIP Networking Conf., pp. 432–440, 2024.

[3] R. M. A. Molina et al., "PUL-Inter-Slice Defender: An Anomaly Detection Solution for Distributed Slice Mobility



Attacks," IEEE Trans. Inf. Forensics Security, vol. 20, pp. 12887–12902, 2025.

[4] J. Talpini et al., "Enhancing Trustworthiness in ML-Based Network Intrusion Detection with Uncertainty Quantification," J. Reliable Intell. Environ., vol. 10, pp. 501–520, 2024.

[5] Z. Allaw et al., "Cross-Layer Security for 5G/6G Network Slices: An SDN, NFV, and AI-Based Hybrid Framework," Sensors, vol. 25, no. 11, Art. no. 3335, 2025.

[6] J.-E. Kim et al., "An Unsupervised Detection-to-Mitigation Framework for Resource Exhaustion Attacks in 5G/6G Network Slicing," Sensors, vol. 26, no. 12, Art. no. 3777, 2026.

[7] E. K. Jassim, "A Secure Multi-Agent DRL-Based Framework for Intelligent Cross-Layer Routing and Slice Isolation in 6G SAGIN," Int. J. Intell. Eng. Syst., vol. 19, no. 7, pp. 630–646, 2026.

[8] W. A. Malwi et al., "Safety-Aware Reinforcement Learning for Self-Healing Intrusion Detection in 5G-Enabled IoT Networks," Comput. Mater. Continua, vol. 87, no. 2, Art. no. 88, 2026.

[9] Z. Ming and T. Taleb, "Proactive Anomaly Detection and Resource Allocation for Service Provision in Network Slices," IEEE Trans. Cogn. Commun. Netw., vol. 12, pp. 9851–9866, 2026.

[10] J. Groen et al., "Implementing and Evaluating Security in O-RAN: Interfaces, Intelligence, and Platforms," IEEE Netw., vol. 39, no. 1, pp. 227–234, 2025.