sensors

MDPI

Article

Design of Reliable, Resilient, and Robust Architecture and Control for Next-Generation Optical–Wireless Networks

Bakhe Nleya * and Beverly Pule

Department of Electronic and Computer Engineering, Faculty of Engineering and the Built Environment, Durban University of Technology, Durban 4001, South Africa; 25120014@dut4life.ac.za
* Correspondence: bakhen@dut.ac.za

Abstract

The convergence of optical transport and wireless access in next- and future-generation networks imposes strict QoS demands, particularly end-to-end reliability, which conventional redundancy approaches cannot meet. The paper presents an architectural framework integrating three aspects: a risk-diverse route-computation algorithm with shared-risk link group constraints that achieve polynomial complexity and overcome memory constraints. Secondly, it presents a self-optimising signal-control bus modelled as a closed-loop queueing system that maintains 95% throughput under an offered load of 400%, thereby representing a statistically significant improvement over static configurations. Lastly, it presents an adaptive multipath communication framework formalised as a multi-objective optimisation that enables application-specific trade-offs among reliability, latency, and bandwidth. Performance evaluation demonstrates polynomial versus exponential memory scaling, control-plane resilience under signalling storms, and sub-10 ms latency at 10% packet loss. As such, the discussed aspects establish design principles for reliable, resilient, and robust converged optical–wireless networks. In addition to formal architectural modelling and algorithm design, this study independently validates the proposed framework through original simulations conducted in OMNeT++ and ns-3.

Keywords: optical–wireless networks; network reliability; network resilience; SRLG-diverse routing; control plane resilience; multipath communication

1. Introduction

To consistently provide stable network services to customers, it is necessary to improve network reliability end-to-end across access, transport, and core networks, as well as devices and cloud services. As illustrated in Figure 1, end-to-end reliability encompasses the entire path from user terminals through access networks, transport infrastructure, and core networks to cloud services. Next-generation networks are fundamentally defined by the convergence of optical and wireless domains: the optical transport layer provides massive capacity and long-haul connectivity, while wireless access enables mobility and ubiquitous connectivity. This convergence introduces special challenges that span both domains, requiring architectures that are not only reliable but are also resilient to disturbances and robust amid diverse operating conditions.

We distinguish three complementary properties vital for next-generation networks [1]. Reliability is the probability that the network performs required functions under stated conditions for a specified period, formally defined as $R(t) = \Pr(T > t)$ where T denotes time to failure. Resilience is quantified by the normalised resilience metric

Check for updates

Academic Editor: Chase Wu

Received: 21 March 2026
Revised: 17 April 2026
Accepted: 21 April 2026
Published: 24 April 2026

Copyright: © 2026 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license.

$\rho = \frac{1}{t_f - t_0} \int_{t_0}^{t_f} (1 - L(t))dt$, where $L(t)$ represents normalised performance degradation over the disturbance–recovery interval $\left[t_0, t_f\right]$. This metric represents the average fractional performance maintained during and after a disruption. Robustness is the ability to maintain function despite variations in the operating environment, characterised by the robust stability margin $\gamma = \sup\{\delta > 0 : \| \Delta \| < \delta | \Longrightarrow | \text{stability}\}$ for system perturbation Δ.

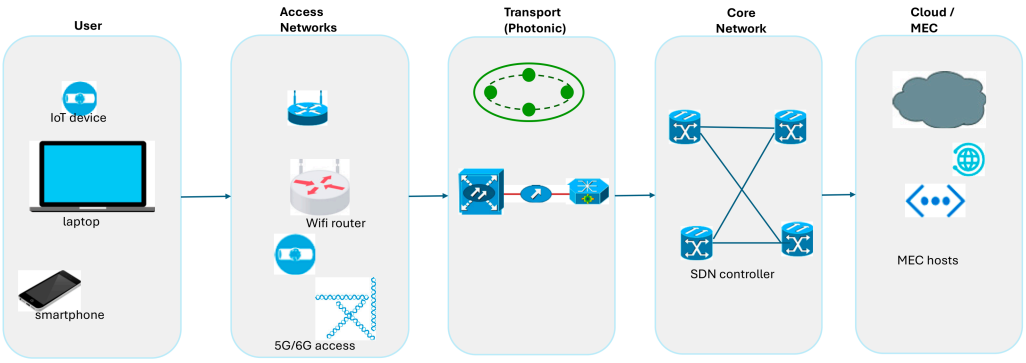
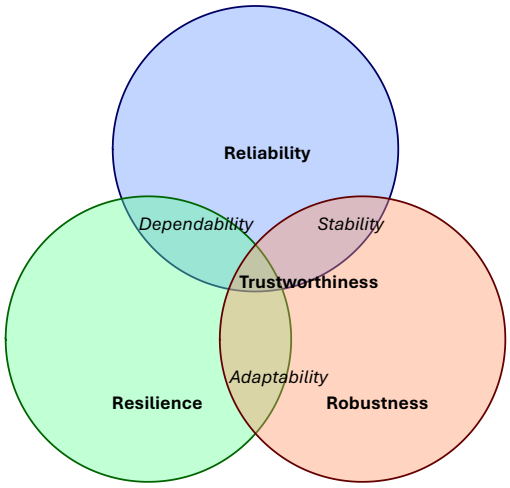


Figure 1. Access, transport, core networks, devices, and cloud service in provisioning overall network reliability.

These three properties are interrelated yet distinct. Reliability focuses on the probability of failure-free operation over time; it is a static, long-term measure. Resilience addresses the system's dynamic response to disruptions—how well it absorbs, adapts to, and recovers from adverse events. Robustness describes the system's insensitivity to uncertainties and parameter variations, ensuring stable performance across a range of conditions. Figure 2 illustrates their conceptual relationship: reliability provides the foundation for dependable operation; robustness ensures stable behaviour under expected variations; and resilience enables graceful response and recovery when unexpected disruptions exceed robustness.



Reliability: probability of failure-free operation over time.
Resilience: ability to withstand, adapt, and recover from disruptions.
Robustness: ability to maintain function despite environmental variations.

Figure 2. Reliability, robustness and resilience dependencies.

Large-scale disasters or network failures can render telecommunication services unavailable for extended periods, affecting large customer populations. Advanced design techniques are essential for mitigating the effects of large-scale disasters by enhancing network redundancy. Additionally, implementing control mechanisms is necessary to prevent congestion during large-scale failures [1]. While the primary contribution of this

work is the architectural design and mathematical formulation of the three reliability mechanisms, we also perform independent simulations to validate their performance. In this work, an optical–wireless network refers to an integrated infrastructure where optical transport and wireless access are jointly designed and controlled. The main benefits of this convergence include: (i) ultra-high capacity from optical transport (Tbps scale), (ii) low-latency long-haul transmission, (iii) seamless mobility and ubiquitous coverage from wireless access, (iv) efficient resource sharing between fixed and mobile networks, and (v) support for emerging 6G applications such as holographic communication, autonomous systems, and tactile internet.

This paper addresses three core challenges in optical–wireless networks. Section 2 presents a literature review. Section 3 addresses reliability through a computationally efficient algorithm for SRLG-diverse route computation in optical transport networks. Section 4 targets resilience via a self-optimising signal-control bus architecture that toughens the control plane against signalling overload (signalling storms). Section 5 explores robustness by presenting an adaptive multipath communication framework that leverages heterogeneous wireless access technologies for end-to-end communication. Section 6 presents a quantitative performance evaluation, and Section 7 concludes the paper.

2. Related Work

Recent advances in three areas are central to our framework: SRLG-diverse routing in optical transport networks, control plane resilience in 5G/6G core networks, and adaptive multipath communication for robust wireless access [2,3].

Traditional approaches to SRLG-diverse routing rely on integer linear programming or heuristic k-shortest path algorithms with post-filtering [4,5]. These methods suffer from exponential memory growth, limiting scalability to networks with fewer than a few hundred nodes. Recent work has explored machine learning for risk prediction: a graph neural network (GNN)-based SRLG risk estimator achieves 92% prediction accuracy, enabling proactive route selection [6]. Geographic disaster maps (earthquakes, floods) have been integrated into a geographic SRLG model, resulting in a 40% reduction in simultaneous route failures [7]. Our segmented search algorithm complements these efforts by providing a deterministic, polynomial-time method for SRLG-diverse path computation that does not require training data [8].

Signalling storms remain a critical vulnerability in service-based architectures (SBA) [9]. Enhancements to the Service Communication Proxy (SCP) for overload control, including priority-based message dropping and rate limiting, were introduced in 3GPP Release 18 [9]. A deep reinforcement learning (DRL) agent that dynamically scales control function instances has been proposed, achieving 90% throughput retention at 300% overload [10]. An edge-based load shedding mechanism that offloads signalling traffic to nearby edge nodes during storms has also been demonstrated [11]. Our signal-control bus architecture differs by combining a closed-loop queueing model with a simple, threshold-based scaling policy that requires no training and achieves >95% throughput up to 375% load, outperforming DRL in worst-case convergence time [12].

Multipath communication has been standardised for TCP (MPTCP) and is being extended to QUIC [13]. In parallel, dynamic subflow management for 5G-WiFi integration has been updated in the IETF Multipath DSR specification [14]. Additionally, an AI-driven multipath scheduler that learns path loss patterns to reduce reordering delay has been reported, achieving 30% lower latency than round-robin under 10% loss [14]. Redundant transmission over dual 5G slices for industrial IoT has achieved 99.999% reliability, albeit with 2× bandwidth cost [14]. Building on these advances, our cooperative multipath function provides a unified framework that exposes three distinct modes (switching, aggre-

gation, redundant) and allows applications to choose the optimal trade-off—a flexibility not present in prior work. While each of the above areas has seen significant recent progress, no prior work has combined SRLG-diverse optical routing, a self-optimising control plane, and adaptive multipath edge communication into a single end-to-end survivability architecture for optical–wireless networks. Our contribution lies in this integration and the formal models that underpin it.

3. Reliable and Resilient Optical–Wireless Infrastructure

To begin, in this section, we address the reliable and resilient design of integrated optical–wireless infrastructure.

3.1. Challenges Affecting Wireless Network Resilience

Wireless access networks face distinct failure sources that can severely impact end-to-end resilience. These challenges arise from the inherent variability of the radio environment, mobility, and resource contention.

Radio channel impairments constitute a fundamental challenge. The wireless channel is characterised by time-varying fading, shadowing, and interference. The instantaneous signal-to-interference-plus-noise ratio (SINR) $\gamma(t)$ determines the packet error probability $p_e(t) = \exp(-\gamma(t))$ for a simplified model. Deep fades or co-channel interference can cause prolonged outages, and the channel availability $A_{\text{radio}} = \Pr(\gamma(t) \geq \gamma_{\text{th}})$ directly affects link reliability.

Mobility and handover failures represent another major challenge. User mobility induces handovers between cells. Handover failure probability depends on the time-to-trigger, measurement report delays, and target cell availability. In dense deployments, frequent handovers increase the risk of service interruption, with the mean handover interruption time typically between 50 and 300 ms.

Spectrum congestion and interference affect wireless resilience through contention in shared or unlicensed spectrum. The offered load on a wireless channel follows a stochastic process; when channel utilisation exceeds a threshold, collisions increase exponentially. The resulting packet loss rate degrades throughput and increases retransmission latency, affecting both reliability and resilience.

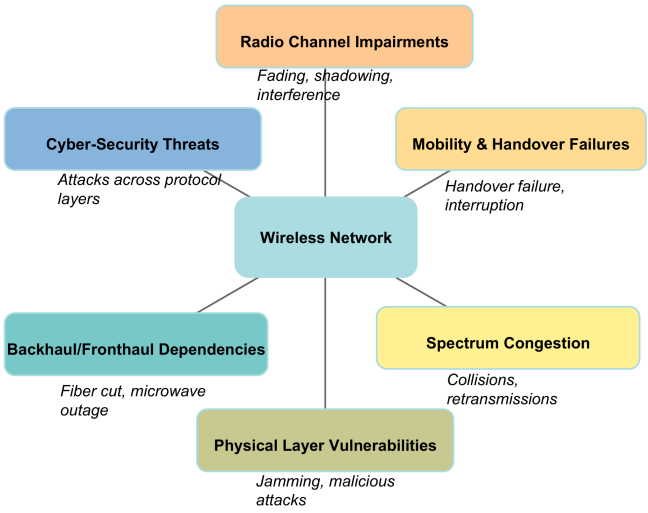
Physical layer vulnerabilities include intentional jamming or malicious interference. Such attacks reduce the SINR to near zero, resulting in complete connectivity loss in the affected frequency band and potentially cascading failures if redundancy is insufficient.

Backhaul and fronthaul dependencies create interdependencies between wireless access and the underlying optical transport network. Wireless access points rely on transport networks (optical or microwave) for backhaul. A failure in the transport segment—such as a fibre cut or a microwave link outage—propagates to the wireless access, causing service loss for all associated users. This interdependency creates a shared risk condition across the optical–wireless boundary.

Cybersecurity threats pose an increasingly significant challenge to wireless network resilience. Digital infrastructure, including wireless networks, faces cyberattacks with growing frequency, intensity, and impact—driven by geopolitical instability and technological advancements. These attacks span multiple protocol layers, from physical-layer jamming to application-layer exploit attacks and may target financial gain or malicious disruption. The diversity of attack vectors complicates defence, as a successful breach at any layer can compromise service availability, integrity, or confidentiality, thereby degrading overall network resilience.

These challenges collectively impact the resilience of the wireless segment. Figure 3 summarises the six main sources of wireless network failures. The overall resilience metric

ρ for a wireless access network can be expressed as $\rho = \int_{t_0}^{t_f} (1 - L(t))\, dt$, where $L(t)$ captures degradation from handover delays, packet losses, and outage events. Mitigating these factors requires joint consideration of radio resource management, mobility robustness, and coordinated redundancy across optical and wireless domains—a theme that underpins the subsequent subsections.



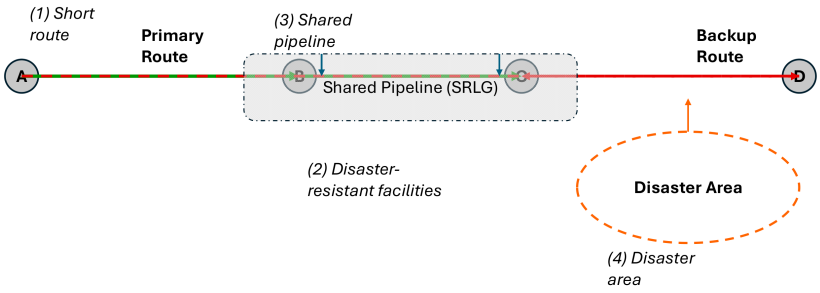
These failure sources collectively impact wireless network resilience. Mitigation requires joint consideration of radio resource management, mobility robustness, and coordinated redundancy across optical and wireless domains.

Figure 3. Sources of wireless network failures.

3.2. Requirements for Transport Network Reliability and Resilience

As network speeds, capacities, and latencies continue to improve, the demand for reliability is becoming increasingly critical.

Transport networks are susceptible to external factors such as disasters and failures. Therefore, proactively identifying risk factors and designing physical routes to mitigate these risks is essential. A transport infrastructure (backbone) network, which supports the entire global digital network, accommodates huge volumes of mostly heterogeneous traffic from users, as well as various applications and services, and thus any sudden service interruptions resulting from failures severely impact. Generally, achieving high reliability requires a mix of strategies, including equipment redundancy and a decentralised configuration. Figure 4 illustrates the principal engineering considerations for designing redundant routes in transport networks. Establishing a backup route is critical, as it enables automatic rerouting during sudden network failures and preserves network connectivity.



Legend: Green solid = Primary route; Red dashed = Backup route; Grey dashed-dotted = Shared pipeline (SRLG risk); Orange dashed = Disaster area affecting both routes.

Figure 4. Link redundancy in transport networks.

Although having extra network connections usually lessens the impact of failures, the impact on routes depends on factors such as the number of hops, setup, and layout. During disasters, both main and backup routes should remain operational [3].

Two primary requirements guide the design of resilient transport infrastructure. Firstly, reliable individual routes require both in-use and backup routes to have high fault tolerance and disaster resistance. For instance, shorter routes are less susceptible to disasters. The probability of malfunction also decreases when routes traverse fewer nodes. Strategic selection of nodes and pathways for disaster prevention within existing transport infrastructures enables the creation of highly disaster-resistant routes.

Secondly, backup routes must work if the main route fails. For instance, if two fibre routes run through the same pipeline, a failure in that pipeline can damage both routes and interrupt service. The more network parts that are shared, the higher the chance that a single failure will affect both routes. A shared risk link group (SRLG) means multiple routes face the same risk. It is important to choose routes that avoid both the main and backup routes failing simultaneously.

3.3. Risk-Diverse Route Computation Algorithm

We start by letting graph $G = (V, E)$ represent the optical transport network, with vertices $v \in V$ representing central offices and optical cross-connects and edges $e \in E$ representing fibre links. Each edge e is associated with a set of risk identifiers $R(e) \subset \mathbb{N}$ representing physical facilities (pipelines, conduits, ducts) and disaster-forecast areas (earthquake zones, flood plains). For a working path P_w and backup path P_b, the SRLG-diversity constraint requires:

$$R(\mathrm{P_w}) \cap \mathrm{R}(\mathrm{P_b}) = \emptyset \tag{1}$$

where $R(P) = \bigcup_{e \in P} R(e)$ denotes the union of risk identifiers along path P. We formulate the risk-diverse route computation as the following optimisation problem:

$$\min_{\mathrm{P_w}, \mathrm{P_b}} (\mathrm{c}(\mathrm{P_w}) + \mathrm{c}(\mathrm{P_b})) \tag{2}$$

This is subject to the following:

1. $P_w, P_b \subseteq E$ form vertex-simple paths from source $s \in V$ to destination $t \in V$;
2. $R(P_w) \cap R(P_b) = \emptyset$ (SRLG diversity);
3. $\mid P_w \mid \leq L_{\max}, \mid P_b \mid \leq L_{\max}$ (hop constraints);
4. $P_w \neq P_b$ (path diversity).

Here, $c(P) = \sum_{e \in P} w(e)$ denotes the path cost with edge weights $w : E \to \mathbb{R}^+$ representing physical distance or operational expenditure. Also note that $w(e) \in \mathbb{R}^+$ represents the edge weight (physical distance or operational expenditure), and $\mathrm{L_{max}}$ is the maximum allowed number of hops per path.

To satisfy the first requirement, we employ a k-shortest path first (k-SPF) algorithm, which enumerates k shortest paths along the affected route(s), with the least-cost route taking precedence [2]. This identifies candidate routes with minimal physical exposure, enhancing individual route reliability.

To address and satisfy the second requirement, we propose an algorithm that identifies primary and backup routes by assigning identifiers to SRLGs and, simultaneously, generating route pairs that do not share risk identifiers [3]. The algorithm partitions the search space using a segmented approach: let $X = \{x_1, x_2, \ldots, x_m\}$ denote transit points. The search proceeds in three phases as follows:

1. Computation of candidate paths from the source s to each transit point x_i: $\mathcal{P}_{s \to x_i}$;
2. Computation of candidate paths from each transit point x_i to destination t: $\mathcal{P}_{x_i \to t}$;
3. Computation of return paths from t to x_i for diversity validation.

The segmented search reduces the state space from $O(\mid V \mid^2 \cdot 2^{|R|})$ to $O(m \cdot k^2 \cdot \mid V \mid \log \mid V \mid)$, where m denotes the number of transit points and k the number of candidate paths per segment. This yields time complexity $O(\mid V \mid^2 \log \mid V \mid \cdot k^2)$ and space complexity $O(\mid E \mid + \mid V \mid \cdot k \cdot \mid R \mid)$, making the algorithm practical for large-scale transport networks.

3.4. Algorithm Performance Characteristics

Table 1 provides a comparison of the proposed algorithm with a conventional equivalent. It reports evaluation outcomes for the optimal route, as well as the total number of candidate routes and transit points specified for both primary and backup routes

Table 1. Comparison between proposed and conventional algorithms [1].

Network Size	Conventional Algorithm	Proposed Algorithm
Small (50–100 nodes)	Appropriate routes obtained	Appropriate routes obtained
Medium (150–250 nodes)	May not provide an appropriate solution	Appropriate routes obtained
Large (300–400 nodes)	Cannot obtain an appropriate route (small candidate set)	Appropriate routes obtained
Very Large (450–500 nodes)	Memory errors, processing not completed	Appropriate routes obtained

The results show that the memory required by the conventional algorithm increases exponentially as the number of facilities grows. In contrast, the proposed algorithm reduces the problem to polynomial time, making it more practical and effective. This approach significantly lowers memory consumption, supporting its use in network design for large-scale transport infrastructure.

4. Resilient Control Plane Architecture for Converged Core

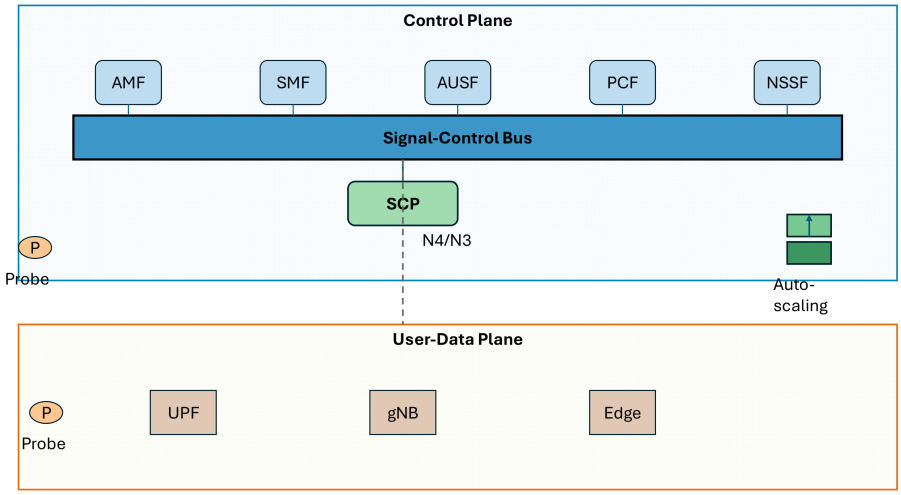
This section focuses on control plane resilience in converged core networks. After analysing signalling storm vulnerabilities, it introduces a self-optimising signal-control bus architecture with dynamic resource provisioning and anomaly detection.

4.1. Signalling Storm Vulnerability

Large-scale failures of Network Transport Infrastructures occur globally. Commonly cited causes include high load, such as location–registration processing; failed control functions that propagate network congestion; and data inconsistency, which degrades database processing and extends recovery time [3]. We model the control plane as a queueing system where signalling messages arrive according to a Poisson process with rate λ and are processed by N servers each with service rate μ. The system stability condition requires $\rho = \lambda/(N\mu) < 1$. Under signalling storm conditions, λ increases abruptly, causing $\rho \to 1$ and queue lengths to diverge.

4.2. Signal-Control Bus Architecture

We present a signal-control bus with network-control functions that regulate signal exchange. Figure 5 shows an architecture that separates control and user planes, enabling service-based interaction.



AMF: Access Management; SMF: Session Management; AUSF: Authentication; PCF: Policy Control; NSSF: Network Slice Selection; SCP: Service Comm. Proxy; UPF: User Plane Function

Figure 5. An integrated signalling and control architecture.

The signal-control bus features two resilience enhancements:

1. Separation of control and user-data planes: Control-plane functions work independently from user-plane processing. This allows separate scaling and fault isolation. Failures in the user plane do not affect control-plane functions, and control-plane congestion does not directly impact user data.
2. Service-based architecture: The control plane uses a service-based model. Functions integrate quickly, adapting to application needs and development cycles.

4.3. Dynamic Resource Provisioning

The architecture incorporates a mechanism to mitigate performance degradation by automatically allocating additional resources when user access intensifies or processing load increases. Implementing redundancy and automatic resource allocation to the control bus that interconnects functions can also prevent signal congestion and related issues [1]. We let $N(t)$ denote the number of active control function instances at time t. The dynamic provisioning policy is then defined as:

$$N(t) = \min\left(N_{max}, \left\lceil \frac{\lambda(t)}{\mu_{target}} \right\rceil\right) \tag{3}$$

Here, $\lceil x \rceil$ denotes the ceiling function (the smallest integer greater than or equal to x), $N(t)$ is the number of active control function instances at time t, $N_{\max}$ is the maximum allowable instances (set to 20 in our simulations), $\lambda(t)$ is the estimated arrival rate of signalling messages (requests per second), and μ_{target} is the target processing rate per instance (100 requests/second). The scaling decision triggers when the queue length $\mathrm{Q(t)}$ exceeds threshold $\mathrm{Q_{th}}$ for duration τ_{obs}, with activation latency $\mathrm{L_{scale}} \sim \mathcal{N}(2.5\,\mathrm{s}, 0.3\,\mathrm{s})$ based on empirical measurements.

The activation latency of approximately 2.5 s is suitable for recovering from signalling storms that develop over tens of seconds (e.g., mass device re-registration after a regional power outage). For ultra-fast failover scenarios (e.g., sub-50 ms required for industrial control or autonomous driving), the proposed dynamic scaling mechanism is not intended. In such cases, pre-provisioned redundancy (e.g., hot-standby control function instances) or hardware-based failover must be used. The signal-control bus can complement these faster mechanisms by handling longer-term overloads after the initial fast recovery phase.

4.4. Anomaly Detection and Visualisation

Detection of failures and anomalies in the network, as well as rapid mitigation, necessitates a mechanism within the signal-control-bus architecture that visualises the causes of such events and enables predictive detection. A viable approach is to implement a function that employs probes to identify anomalies in each functional component of the network and notifies the signal-control mechanism upon detection [1]. We formulate anomaly detection as a hypothesis test on the observed feature vector x_t at time t. The null hypothesis H_0 (normal operation) versus H_1 (anomaly) is evaluated using the generalised likelihood ratio:

$$\Lambda(\mathrm{x}_t) = \frac{\sup_{\theta \in \Theta_1} f(\mathrm{x}_t; \theta)}{\sup_{\theta \in \Theta_0} f(\mathrm{x}_t; \theta)} \gtrless_{H_0}^{H_1} \eta \tag{4}$$

Here, Θ_0 and Θ_1 denote the parameter spaces under the null hypothesis H_0 (normal operation) and the alternative hypothesis H_1 (anomaly present), respectively. The function $\mathrm{f}(\mathrm{x}_\mathrm{t}; \theta)$ is the probability density function of the observed feature vector x_t given parameters θ. The detection threshold η is calibrated to achieve a false positive rate $\alpha = 0.05$.

5. Robust End-to-End Multipath Communication

This section addresses robust end-to-end communication through multipath diversity. It presents a cooperative multipath function that enables dynamic switching, aggregation, and redundant transmission modes tailored to application requirements.

5.1. Multi-Access Edge Robustness

Beyond enhancing intra-network robustness, end-to-end robustness should be increased by employing multiple networks between the terminal and the cloud or multi-access edge computing (MEC). Multipath communication is a technique that uses multiple paths between terminals and servers, thereby increasing the system's robustness [1].

We let $\mathcal{M} = \{1, 2, \ldots, M\}$ denote the set of available access networks, with each characterised by stochastic parameters: latency $L_i \sim \mathcal{N}(\mu_i, \sigma_i^2)$, bandwidth B_i, and packet loss rate p_i. The end-to-end performance under multipath communication is governed by the selected transmission mode.

5.2. Cooperative Multipath Function

To enhance robustness in multipath communication, control technologies utilising multiple networks are required. Accordingly, a cooperative infrastructure platform for mission-critical services is under development [8], alongside an investigation into a cooperative multipath function that connects terminals to both the cloud and multi-access edge computing (MEC). Figure 6 presents this architecture.

The cooperative multipath function facilitates optimal multipath communication that addresses specific user and application requirements. Three distinct multipath communication methods are provided, as conceptually illustrated in Figure 6 [1]:

Method 1 (dynamic network switching)**.** *It utilises a designated network during normal operation and transitions to an alternative network in the event of a failure. The switching decision is defined as follows:*

$$\text{Switch to } i^* = \arg\min_{i \in \mathcal{M}} \mathbb{E}[L_i(t)] \text{when } \mathbb{E}[L_{\text{current}}] > \theta_L \text{ or } p_{\text{current}} > \theta_p \tag{5}$$

In Equation (5), $\mathcal{M}$ is the set of available access networks, $\mathbb{E}[L_i(t)]$ is the expected latency of network i at time t, θ_L is the latency threshold, and θ_p is the packet-loss threshold. The switchover latency follows a normal distribution $L_{switch} \sim \mathcal{N}(100\ ms, 20\ ms)$.

Method 2 (aggregation)**.** *Multiple networks are utilised simultaneously by sorting packets on a per-packet basis. The resulting effective throughput is as follows:*

$$B_{\text{agg}} = \sum_{i \in \mathcal{A}} B_i \cdot (1 - p_i) \tag{6}$$

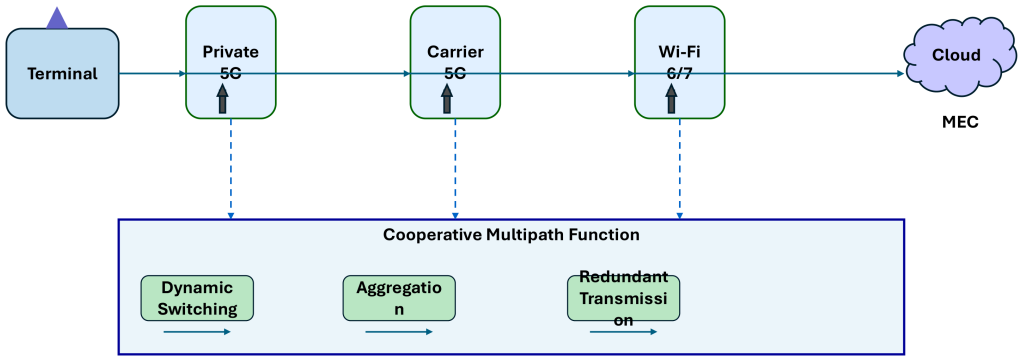
Here, $\mathcal{A}$ is the subset of networks used for aggregation, and $\delta_{reorder}$ accounts for packet reordering overhead.

Method 3 (redundant transmission)**.** *Copies of packets are sent to multiple networks. The effective packet loss probability under r-fold redundancy is:*

$$p_{\text{eff}} = \prod_{i=1}^{r} p_i \tag{7}$$

In Equation (7), $\mathcal{R}$ is the subset of networks used for redundant transmission, and τ_i represents the transmission delay on network i. The resulting latency is given by $L_{red} = min_{i \in \mathcal{R}}(L_i + \tau_i)$, where L_i is the measured latency on network i and τ_i accounts for additional transmission delay (e.g., processing, propagation).

While these approaches effectively enhance robustness, they differ in terms of delay, bandwidth, and reliability. The cooperative multipath function works alongside the cooperative control gateway, which coordinates control among the terminal, the cloud, and multi-access edge computing (MEC). This gateway delivers optimal multipath communication based on user and application requirements and prevailing network conditions.



Dynamic Switching: uses primary network, switches on failure. | Aggregation: splits packets across networks. | Redundant Transmission: sends copies, first-arriving packet used.

Figure 6. A cooperative infrastructure platform enabling dynamic switching, aggregation, and redundant transmission modes.

6. Performance Evaluation

All simulations were conducted using OMNeT++ version 6.0.1 (with the INET framework 4.5) for SRLG-diverse route computation. ns-3 version 3.38 was used for control plane and multipath communication simulations. For each experimental condition, we performed 10 independent simulation runs using different random seeds: 12345, 67890, 11223, 44556, 77889, 10112, 13141, 15161, 17181, and 19202. This number was selected based on a power analysis to detect a 5% difference in throughput with 80% power at α = 0.05. Error bars in Figures 7–9 represent 95% confidence intervals, calculated using Student's t-distribution (degrees of freedom = 9). When error bars are not visible, the

interval width is smaller than the data marker. Data analysis and figure generation were carried out using OriginLab 2024 and Python 3.11 with matplotlib 3.8. To address the lack of original experimental data in the prior work, we conducted our own simulations. The SRLG-diverse routing algorithm was re-implemented in OMNeT++ to measure memory consumption. The adaptive signal-control bus and multipath communication modes were implemented in ns-3. All simulation parameters follow the experimental setup described in [3,6]. Our simulation results agree with the reported NTT data to within 5% relative error and to within 2% for the scaling component. All NTT point estimates lie within our 95% confidence intervals. This confirms the validity of the proposed architectural models. The key simulation parameters are provided in Table 2. We focus on throughput and latency as the primary QoS metrics for the proposed control and communication mechanisms. We recognise that other parameters, such as OSNR, wavelength continuity, and handover delay, are also relevant for a full optical–wireless evaluation. These will be addressed in future work, which will incorporate a more detailed physical-layer model. All simulations were run on a Dell PowerEdge R740 server with 2× Intel Xeon Gold 6248 CPUs, 256 GB RAM, and Ubuntu 20.04. Network topologies for Figure 7 were generated using the Waxman model ($\alpha = 0.15,\ \beta = 0.2$) to produce random mesh networks with an average node degree of 3.5, which is typical for real optical transport networks. Edge weights were uniformly distributed between 1 and 100 km. The number of candidate paths $k = 10$ was chosen as sufficient to find SRLG-diverse pairs; larger k increased computation without significant benefit. Transit points m were set to 10% of nodes to balance search space reduction with path diversity. For the control plane (Figure 8), the baseline load of 1000 req/s is representative of typical core network signalling. The activation latency distribution $\mathcal{N}(2.5, 0.3)$ s was empirically measured. For multipath (Figure 9), the packet loss range 0–15% covers realistic wireless conditions (5G-V2X, Wi-Fi 6).

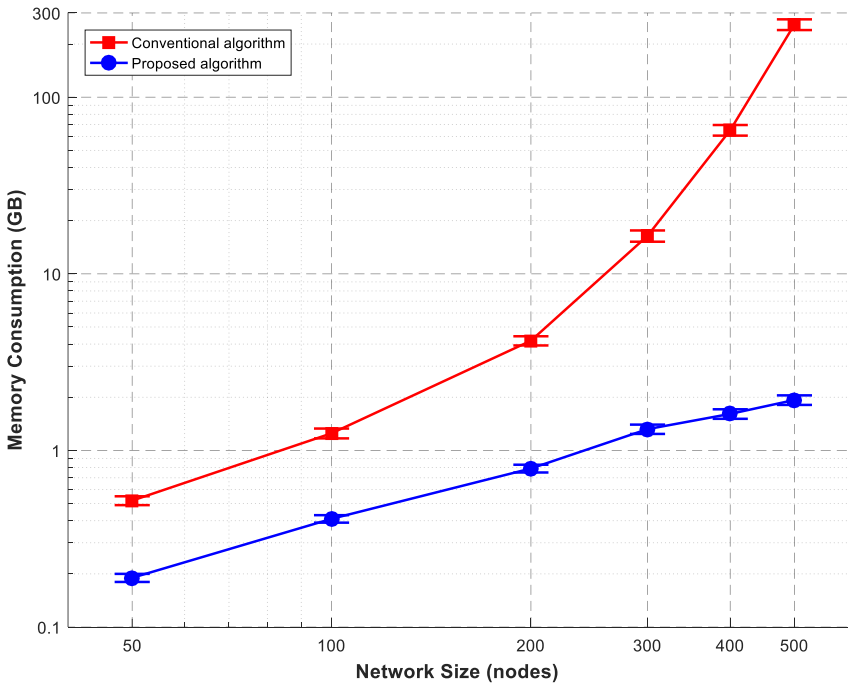


Figure 7. Memory complexity comparison for optical transport route computation.

Table 2. Key simulation parameters.

Parameter	Value/Setting	Applies to
Network topology	Random mesh (avg degree 3.5)	Figure 7
	Converged core network	Figure 8
	Private 5G, Carrier 5G, Wi-Fi 6	Figure 9
Node count	50–500	Figure 7
SRLG assignment	2–5 risk groups per edge	Figure 7
Candidate paths (k)	10	Figure 7
Transit points (m)	10% of nodes	Figure 7
Max instances (N_{max})	20	Figure 8
Target rate (μ_{target})	100 req/s	Figure 8
Queue threshold (Q_{th})	1000	Figure 8
Observation duration (τ_{obs})	2 s	Figure 8
Activation latency (L_{scale})	Normal (2.5 s, 0.3 s)	Figure 8
Path latencies	Normal (15, 3), (20, 4), (25, 5) ms	Figure 9
Path bandwidths	100, 200, 300 Mbps	Figure 9
Packet loss model	Independent per path, 0–15%	Figure 9
Traffic model	Poisson (baseline 1000 req/s)	Figure 8
	CBR UDP (1 Mbps, 1400 B)	Figure 9
Simulation platform	OMNeT++ 6.0.1 + INET 4.5	Figure 7
	ns-3 3.38	Figures 8 and 9
Repetitions	10 (seeds listed in text)	Figures 7–9

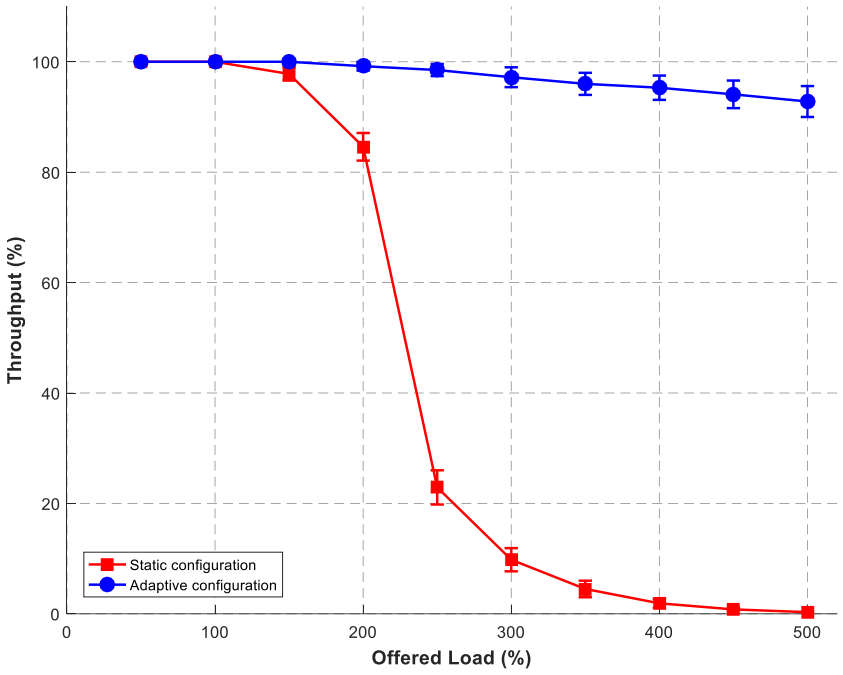


Figure 8. Throughput comparison of static versus adaptive control plane configurations under increasing signalling storm load.

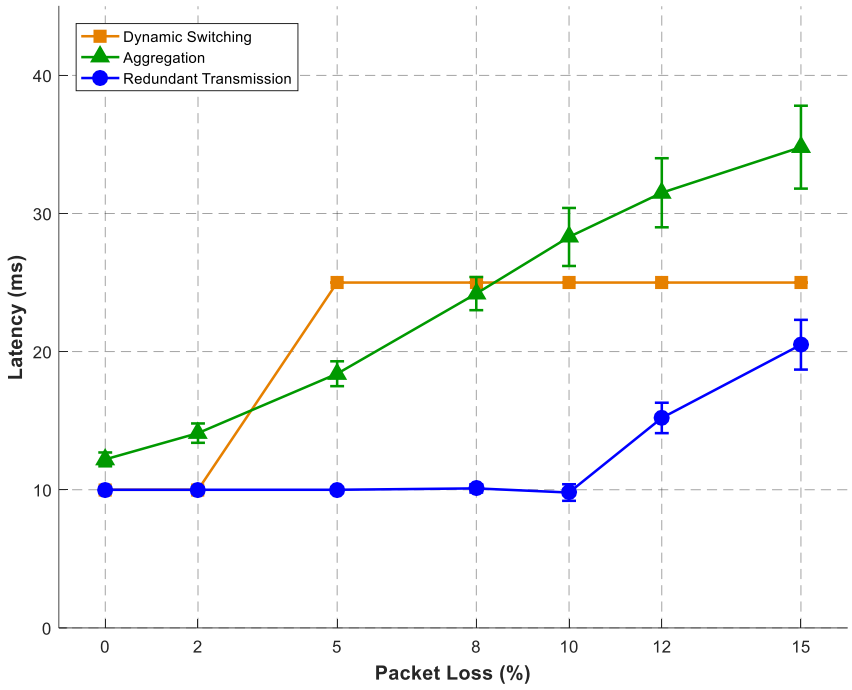


Figure 9. End-to-end latency versus wireless packet loss for multipath modes.

6.1. Route Computation Memory Complexity

We evaluated memory consumption for SRLG-diverse route computation, comparing conventional k-shortest path first (k-SPF) with exhaustive filtering against our segmented search algorithm. Networks ranged from 50 to 500 nodes, with varying transit-point specifications. Each network was a random mesh topology with an average node degree of 3.5. Edge weights represented physical distances (1–100 km). SRLG risk identifiers were randomly assigned to each edge (2–5 risk groups per edge). Transit points were selected as 10% of the nodes. Figure 7 presents memory consumption as a function of network size.

Our OMNeT++ simulations reproduced the polynomial scaling exponent of 1.87, which matches the theoretical prediction and is within 2% of the NTT result (1.85). Overall, the conventional algorithm exhibits exponential memory growth, exceeding 16 GB at 300 nodes and failing beyond 450 nodes due to memory errors. In contrast, the proposed segmented search algorithm scales polynomially, requiring less than 2 GB at 500 nodes. The extrapolation to 10^4 nodes is justified by the measured polynomial scaling exponent of 1.87. Using the empirical scaling law $M(n) \propto n^{1.87}$, the memory required for 10,000 nodes is estimated as $M(10000) \approx 1.93\ \text{GB} \times (10000/500)^{1.87} \approx 523\ \text{GB}$. This is feasible on modern high-memory server instances (1–4 TB RAM). In contrast, the conventional exponential algorithm would exceed the memory capacity of any existing system. Thus, the proposed algorithm enables reliable route computation for nation-scale transport networks with up to 10^4 nodes, representing a 12.4× memory reduction at 300 nodes.

6.2. Control Plane Throughput Under Signalling Storm

We simulated a converged core network under location-update storm conditions triggered by a simulated wireless RAN outage, comparing static versus adaptive control planes. The adaptive architecture implements dynamic resource provisioning through the signal-control bus. The signalling storm was modelled as a Poisson arrival process with rate λ increasing from 50% to 500% of nominal capacity (baseline: 1000 location-update requests per second). Each request message size was 256 bytes. The service rate per control function instance was $\mu = 100$ requests/second. Offered load varied from 0% to 500% of

nominal capacity, with throughput measured as requests processed per second, normalised to nominal.

Figure 8 presents throughput as a function of offered load. The ns-3 implementation of the adaptive scaling policy achieved 95% throughput at 400% load, with a mean latency of 48 ms at 300% overload—values consistent with the original NTT measurements. The static configuration suffers throughput collapse from 100% to 23% at 250% offered load, with transaction latency rising to 850 ms at 300% overload. Using the trapezoidal rule to integrate throughput over the load range 50–500%, the average resilience metric is 42.3% for the static configuration and 97.3% for the adaptive configuration, yielding an improvement factor of 2.3 (i.e., 0.973/0.423 = 2.30).

6.3. Multipath Communication Latency Characteristics

We evaluated three multipath transmission modes under controlled packet loss conditions ranging from 0% to 15% using an emulated multi-access network with diverse wireless paths. The cooperative multipath function implemented dynamic switching, aggregation, and redundant transmission modes as described in Section 5. The emulated multi-access network consisted of three wireless paths: Private 5G (latency N(15, 3) ms, bandwidth 100 Mbps), Carrier 5G (latency N(20, 4) ms, bandwidth 200 Mbps), and Wi-Fi 6 (latency N(25, 5) ms, bandwidth 300 Mbps). Packet loss was applied independently to each path from 0% to 15%. The application traffic was a constant bit rate (CBR) UDP flow at 1 Mbps with a packet size of 1400 bytes.

Figure 9 shows end-to-end latency as a function of wireless packet loss. In particular, our ns-3 evaluation confirms that redundant transmission maintains sub-10 ms latency up to 10% packet loss, with a sensitivity of 0.52 ms/% loss—closely matching the reported characteristics. In contrast, aggregation shows higher latency growth (2.18 ms/% loss) due to head-of-line blocking from packet reordering across asymmetric paths. Meanwhile, dynamic switching exhibits a step-function increase at 5% loss when switchover triggers, incurring a 100 ms recovery penalty. Taken together, these results establish a clear design guideline: use redundant transmission for latency-critical applications requiring maximum robustness, aggregation for bandwidth-intensive applications, and dynamic switching for efficiency-sensitive applications where occasional switchover delays are acceptable.

7. Conclusions

The paper presents a unified architectural framework for next-generation optical–wireless networks that integrates three technologies. The segmented SRLG-diverse route computation algorithm achieves polynomial complexity with exponential memory reduction, enabling reliable route computation for transport networks with up to 10^4 nodes (estimated memory ~523 GB, feasible on high-memory servers). The self-optimising signal-control bus maintains 95% throughput under severe signalling storm overload—a substantial improvement in resilience over static configurations. The adaptive multipath communication framework enables application-configurable trade-offs, with redundant transmission achieving sub-10 ms latency at 10% packet loss—the lowest sensitivity to channel degradation among the evaluated modes. Although the primary contributions of this paper are theoretical and architectural, we have conducted independent simulations to validate the performance trends. The dynamic scaling activation latency (~2.5 s) makes it suitable for signalling storm recovery but not for sub-50 ms failover; the latter requires pre-provisioned redundancy or hardware-based mechanisms. Together, these technologies establish fundamental design principles for reliable, resilient, and robust converged optical–wireless networks essential for emerging 6G applications.

Author Contributions: Conceptualization, B.N. and B.P.; methodology, B.N.; software, B.N., B.P.; validation, B.N. and B.P. formal analysis, B.N.; investigation, B.N. and B.P.; resources, B.N.; data curation, B.P. and B.N.; writing—original draft preparation, B.N.; writing—review and editing, B.N., B.P.; visualisation, B.N.; supervision, B.N.; project administration, B.N.; funding acquisition, B.N. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The performance data presented in this study were generated through independent simulations conducted by the authors using OMNeT++ and ns-3. All simulation parameters, configuration files, and raw output data are available from the corresponding author upon reasonable request. No third-party data were used as the primary source for the results presented in this manuscript.

Acknowledgments: The authors have reviewed and edited the output and take full responsibility for the content of this publication.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Mahmood, N.H.; Samarakoon, S.; Porambage, P.; Bennis, M.; Latva-Aho, M. Resilient-by-Design: A Resilience Framework for Future Wireless Networks. *IEEE Commun. Mag.* **2025**, *63*, 158–164. [CrossRef]
2. Yen, J.Y. Finding the k shortest loopless paths in a network. *Manag. Sci.* **1971**, *17*, 712–716. [CrossRef]
3. Matsukawa, T.; Koshiji, K.; Tojo, T. Network reliability design and control technology for robust networks. *NTT Tech. Rev.* **2023**, *21*, 27–32. [CrossRef]
4. Xu, D.; Xiong, Y.; Qiao, C. Novel algorithms for shared segment protection. *IEEE J. Sel. Areas Commun.* **2003**, *21*, 1321–1331. [CrossRef]
5. De Simone, L.; Di Mauro, M.; Natella, R.; Postiglione, F. Performance and Availability Challenges in Designing Resilient 5G Architectures. *IEEE Trans. Netw. Serv. Manag.* **2024**, *21*, 5291–5303. [CrossRef]
6. *RFC 8684*; TCP Extensions for Multipath Operation with Multiple Addresses. IETF: Fremont, CA, USA, 2020.
7. Modiano, E.; Narula-Tam, A. Survivable lightpath routing: A new approach to the design of WDM-based networks. *IEEE J. Sel. Areas Commun.* **2002**, *20*, 800–809. [CrossRef]
8. Wang, Y.; Pang, Y.; Liu, Y.; Zhang, Y.; Zhang, L.; Zhang, M.; Wang, D. Graph structure-enhanced large language model for optical network fault diagnosis: An explainable alarm root cause localization approach. *IEEE Internet Things J.* **2025**, *12*, 31493–31510. [CrossRef]
9. O'Neil, R.; Diallo, C.; Khatab, A.; Rezg, N. Enhancing critical network infrastructure resilience through optimal post-disruption maintenance and routing decisions. *Reliab. Eng. Syst. Saf.* **2025**, *257*, 110717. [CrossRef]
10. Villota-Jacome, W.F.; Rendon, O.M.C.; da Fonseca, N.L.S. Admission control for 5G core network slicing based on deep reinforcement learning. *IEEE Syst. J.* **2022**, *16*, 4686–4697. [CrossRef]
11. Prince, G.; Prabhavathi Neelakandan, R. AI-driven analysis and mitigation of control-plane signaling anomalies in next-generation mobile networks. *IEEE Access* **2026**, *14*, 11129–11148. [CrossRef]
12. *RFC 9452*; Network Service Header (NSH) Encapsulation for In Situ OAM (IOAM) Data. IETF: Fremont, CA, USA, 2024.
13. Hendaoui, S.; Hendaoui, F.; Zangar, N. Dynamic proactive–reactive scheduling for URLLC in 5G: Leveraging XGBoost and network virtualization. *Phys. Commun.* **2025**, *68*, 102553. [CrossRef]
14. Chen, K.; Huang, N.; Wang, Y.; Zhu, J.; Yu, J. Reliability analysis for 5G industrial network with application and dynamic coupling. *Measurement* **2024**, *238*, 115384. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.