IEEE Open Journal of the Communications Society

Received 13 March 2026; accepted 21 April 2026. Date of publication 27 April 2026; date of current version 14 May 2026.

Digital Object Identifier 10.1109/OJCOMS.2026.3687133

An Overview of Principles, Enablers, Metrics and Emerging Technologies for Resilient Networks

VIJAYA DURGA CHEMALAMARRI, MAHROKH ABDOLLAHI (Member, IEEE), ADAM BRYANT (Member, IEEE), MEHRAN ABOLHASAN (Senior Member, IEEE), AND RAYMOND OWEN (Member, IEEE)

University of Technology Sydney, Sydney, NSW 2007, Australia

CORRESPONDING AUTHOR: V. D. CHEMALAMARRI (vijayadurga.chemalamarri@uts.edu.au)

This work was supported by the Department of Infrastructure, Transport, Regional Development, Communications, Sport and the Arts.

ABSTRACT There are approximately 5.78 billion users relying on mobile networks to access a wide range of digital services. Hence, the resilience of these communication networks is of the highest importance. In this paper, we define network resilience and outline key architectural design principles and their enabling technologies. We further describe relevant metrics for assessing network performance and examine emerging technologies, such as the integration of terrestrial and non-terrestrial networks, artificial intelligence-enabled network management and optimization, as well as innovative concepts like core network disaggregation and non-IP-based architectures. We identify current challenges and highlight critical research directions for the advancement of resilient mobile networks.

INDEX TERMS IP, mobile networks, emergency and network resilience.

I. INTRODUCTION

CAMBRIDGE Dictionary defines resilience as "*the ability of a substance to return to its usual shape after being bent, stretched, or pressed*". In the communications networks, resilience remains loosely defined across both technical and policy domains. It cannot be achieved solely through device-level configurations, network design, over-engineering, or continuous monitoring. For example, hardware redundancy provides secondary communication paths during physical network failures but may be insufficient in the event of security breaches or network wide failures. In the context of communications infrastructure, we define network resilience as "*the ability of a network to anticipate an adverse event, withstand such an event by retaining its core function (operational state), and recover quickly afterwards*". This operational state may range from the delivery of critical services to complete service restoration, depending on the severity and nature of the incident.

The current communication landscape consists of fixed, mobile, device-to-device, aerial, and space networks. As the range of connectivity options expands, so does the number of devices interfacing and communicating across them. This rapid proliferation of connected devices has led to the exponential growth of data produced and consumed. Everyday applications, such as Uber (ride-sharing services), Netflix (streaming services), and Google Search (search engine), generate and consume substantial amounts of data. Many of these applications are distributed, cloud-based, and rely on continuous, high-performance network connectivity. Access to these services, including emergency services, requires reliable network connectivity, which lies exactly within the scope of network resilience.

Distributed applications require infrastructure redundancy, robust device configuration, monitoring, maintenance, and orchestration for continued operation. Any incorrect action can result in widespread service disruption, as evident from the downtime for UniSuper [2]. Google Cloud engineers accidentally applied incorrect configurations to the virtual machines which hosted user accounts, leading to outage that lasted over a week.

Sectors like banking, commerce, and healthcare also rely heavily on fully operational networks and are very sensitive to disruptions. With many banks closing physical branches in sparsely populated and remote areas in favor of online-only operations, there is an increased necessity for resilient, always-on networks to ensure a seamless user experience. The Optus 2023 outage in Australia affected approximately 400,000 small businesses [3], underscoring the dependence on network connectivity in everyday life.

Natural disasters, such as flood and bushfire, and human-initiated threats, like cyberattacks, infrastructure sabotage,

and unplanned events such as large-scale outages, often damage the physical and logical components of communication networks. Such disruptions can impact access networks, transport networks, cloud infrastructure, telecommunications, and the internet, as experienced during the massive power outage across the Iberian Peninsula on April 28, 2025 [4].

Industries such as mining and defense are increasingly using on-site autonomous systems (e.g., drones, mining equipment) for riskier operations. Autonomous systems are managed remotely, thus requiring continuous and adaptive communication for safety and operational efficiency.

Recognizing the growing role of networks in everyday life and other critical industries, various organizations and countries have initiated projects to enhance network resilience. For example, network resilience is a primary use case for enabling hyper-connected, robust infrastructures in European projects such as Hexa-X [5] and Hexa-X-II [6]. PHOENI2X [7] is another such project aimed at delivering a cyber resilience framework that provides intelligent orchestration, automation, and response capabilities to support business continuity and recovery for Operators of Essential Services (OES).

A. RELATED WORK

5G and beyond networks services such as ultra-reliable and low latency communication(URLLC), ubiquitous connectivity(eMBB), and large-scale device communication(mMTC) require a resilient network [8]. There is thus a growing interest in development of robust resilience taxonomies, strategies and examining resilience from diverse viewpoints [9], [10], [11], [12], [13].

Batista and Santos [10] introduce a taxonomy for resilience in information sharing networks based on malicious threats, network disruptions, and performance issues. They note that redundancy techniques such as data aggregation, clustering, and multi-path routing along with monitoring techniques like fault detection, delay estimation, trust, and other statistical models, are key enablers for network resilience.

Vlacheas et al. [14] discuss principal network resilience concepts and propose an ontology to capture the interactions among threats and threat agents, properties, means, and domain.

Tipper et al. [9] attribute next-generation network failures to hardware failures resulting from the adoption of commodity hardware, the integration of edge computing, the maximization of User Equipment (UE) and other environmental failures. They propose resilience strategies for backhaul infrastructure in three deployment scenarios involving one or more operator. The three deployment scenarios are (i) single-operator networks, (ii) collaborative multi-operator environments, and (iii) overlay networks.

Massimo et al. [11] examine network resilience in the context of weather-induced disruptions, for both wired and wireless networks. Grigorjew et al. [13] survey resilience in Time Sensitive Networks (TSN) [15] and identify critical dependencies such as priority handling, redundancy, and synchronization for provisioning TSN. Other mitigation strategies include hot standby configurations, rigorous configuration validation, and system tolerance mechanisms for resilience in TSNs. Failure of these dependencies might lead to lost packets, inaccurate delay measurements, and queue buildups.

Owen et al. [12] introduce the concept of Sovereign Functions, a set of critical IP functions including routing, addressing, and time synchronization, that underpin both mobile and fixed-line connectivity that may affect network resiliency. They attribute most of the recent network failures to misconfiguration of these sovereign functions.

Table 1 compares the existing survey literature with the scope and focus of this paper. As shown in the table, prior surveys typically focus on specific contexts or narrower aspects of resilience, such as information-sharing networks, end-to-end resilience frameworks, NextG backhaul, weather-related disruptions, TSN mechanisms, or sovereign/supporting functions. In contrast, our work provides a broader capability-driven survey that integrates resilience frameworks and lifecycle phases with architectural enablers, including monitoring, redundancy, isolation, security, configuration consistency, and traffic engineering, together with resilience metrics and emerging approaches such as TN-NTN integration, AI/ML-enabled resilience, and mobile core innovation.

B. OUR CONTRIBUTIONS

The focus of this paper is to provide a comprehensive survey of resilience architectures and enabling technologies for building resilient networks. The paper establishes a relationship between the resilience curve and key architectural components, such as redundancy and diversity, isolation, configuration, and layered security, that influence network resilience. These components directly affect network availability, recovery capability, and service continuity.

The study thus assumes that a robust governance framework defining organizational goals, objectives, and direction for a resilient network is already in place. The authors further assume that such goals are sustained through ongoing technical and procedural audits [16]. Thus, based on this assumption and observations made by [9], [11], and [12] on the impact of configuration, hardware, and environmental issues on network resiliency, this study adopts an event-agnostic perspective of network resilience and perceives it as an emergent property, arising from the coordinated interaction of architecture, operational practices, and adaptive responses to disruptions.

Furthermore, the study investigates different metrics for evaluating network performance, outlines emerging approaches to enhancing resilience, and discusses implementation challenges of these approaches.

Section II reviews definitions and examines frameworks for network resilience. Section III outlines the architectural principles and key technological enablers. Section IV presents key metrics for assessing resilience. Sec-

TABLE 1. Comparison of existing survey works and this paper in terms of resilience focus.

Reference	Network/Context	Main Resilience Focus	Key Resilience Aspects
Batista et al. [10]	Information-sharing in communication networks	Survey and taxonomy of resilience techniques for information sharing	Malicious threats, network disruptions, performance issues, availability, integrity, confidentiality, authentication, redundancy, and monitoring.
Vlacheas et al. [14]	Future communication networks / end-to-end network resilience	End-to-end resilience ontology and cognitive framework	Threats, means, domains, threat agents, properties, ontology-based concept relationships, domain interactions, and cognitive enablers (profiles, context, and policies).
Tipper et al. [9]	Next-generation cellular backhaul networks	Connectivity resilience challenges and resilience strategies for NextG backhaul	Commodity hardware failures, RAN disaggregation, edge/MEC integration, network densification, power and environmental outages, single-operator resilience, collaborative multi-operator resilience, and overlay approaches.
Massimo et al. [11]	Wired, wireless, and converged communication networks	Survey of resiliency methodologies against weather-based disruptions	Weather/disaster disruption modeling, wireless-channel degradation, structural impacts on communication infrastructure, protection and reconfiguration strategies, alert-based recovery, and advanced resilient architectures (e.g., DTN, NFV, ICN).
Grigorjew et al. [13]	Time-Sensitive Networks (TSN)	Systems-level overview of TSN resilience mechanisms and open research directions	Time synchronization, bounded low latency, high availability, resource reservation, mechanism interdependencies, fault scenarios, configuration challenges, filtering/policing, frame replication, and monitoring.
Owen et al. [12]	Mobile and fixed-line IP telecommunications networks	Failure-centric survey of sovereign and supporting functions in telecom resilience	Routing, addressing and naming, time synchronization, authentication and access control, licensing, configuration and change management, firewall/traffic control, and real-world outage case studies.
Our work	IP-based mobile and fixed networks	Survey of resilience principles, enabling technologies, metrics, and emerging resilience approaches	Resilience frameworks and lifecycle phases, architectural enablers (monitoring, redundancy, isolation, security, configuration consistency, traffic engineering), resilience metrics, integrated TN–NTN networks, AI/ML-enabled resilience, mobile core innovation, and open research challenges.

tion V discusses strategies for advancing resilience through integration, intelligence, and innovation, followed by a discussion of open research challenges in Section VI. Finally, Section VII concludes the study.

II. NETWORK RESILIENCE DEFINITIONS AND FRAMEWORKS

There are several definitions of network resilience proposed by various organizations and academics, some of which are highlighted as following.

European Union Agency for Cybersecurity (ENISA) [17] defines resilient networks as "*networks that provide and maintain an acceptable level of service in the face of faults (unintentional, intentional, or naturally caused) affecting their normal operation*."

National Institute of Standards and Technology (NIST) [18] defines resilience as "*the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruption. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents*."

The Cybersecurity and Infrastructure Security Agency (CISA) [19] defines resilience as "*the ability to prepare for threats and hazards, adapt to changing conditions, and withstand and recover rapidly from adverse conditions and disruptions*".

The European Telecommunications Standards Institute, Emergency Telecommunications (ETSI EMTEL) [20] frames resilience as "*measures taken during a system outage alleviating the direct consequences of the outage and allowing the system to return to normal operation*".

The International Telecommunication Union (ITU) [21] defines network resilience as "*the ability to provide and maintain an acceptable level of service in the face of faults and challenges to normal operation of a given communication network, based on prepared facilities*".

Smith et al. [22] define network resilience as *the ability of a network to defend against and maintain an acceptable level of service in the presence of such challenges* and Steinberg et al. [16] defines it as *the ability of the network to sustain an acceptable level of service, functionality, and performance when subjected to disruptions, failures, human error, and other external events*.

Taken together, these definitions emphasize resilience as both the ability to maintain acceptable service levels and the capacity to recover and adapt under disruptive conditions. Along with various definitions, several frameworks for building resilient networks also exist. These widely recognized resilience frameworks are discussed below.

A. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY CYBERSECURITY FRAMEWORK (NIST CSF)

NIST [23] specifies Govern, Identify, Protect, Detect, Respond, and Recover as core functions of the Cybersecurity framework. Briefly,

- **Govern function** establishes the risk management strategy, defines expectations and policies, and assigns roles and responsibilities.
- **Identify function** ensures current cybersecurity risks are understood and identified, and that an organization's policies, plans, and processes are continuously improved.
- **Protect function** safeguards and secures the assets and mitigates the likelihood and impact of adverse events.
- **Detect function** identifies possible attacks, anomalies, and any indicators of compromise.
- **Respond function** addresses the anomalies and contains the incident. Relevant incident information is conveyed to stakeholders.
- **Recover function** ensures recovery of operations affected by the cybersecurity incident.

B. RESILIENT-BY-DESIGN

Mahmood et al. [24] note application awareness, novel Key Performance Indicators (KPIs), scalability, and security as key characteristics of a resilient wireless network and propose the 6G-ready framework *Resilient-by-Design*. Predict, Preempt, Protect, and Progress are four main stages in this framework. Briefly,

- **Predict** possible network events using context-aware Artificial Intelligence (AI)/Machine Learning (ML) techniques for monitoring and detecting failures.
- **Preempt** the predicted event by proactively allocating resources and intelligently multiplexing traffic with different Service Level Agreements (SLA).
- **Protect** the network by minimizing fault impact through fault isolation and traffic engineering.
- **Progress** by initiating upgrades to resilience mechanisms.

C. MAPE-K

The MAPE-K framework captures the Management-Analysis-Plan-Execute loop, supported by a common Knowledge system to build self-adaptive systems as demonstrated in the work [25]. While the framework is reactive, it remains applicable to enhance network resilience as discussed in [26]. The framework's four stages are:

- **Monitor** the network continuously to collect and process information for further analysis.
- **Analyze** and verify the collected information to develop insights on possible adversary network events.
- **Plan** the post-analysis steps to address the fault and implement changes.
- **Execute** proposed planned changes.

Camelo et al. [27]'s work, Network intelligence for aDAptive and sElf-Learning MObile Networks (DAEMON), has adopted and modified the MAPE-K framework to develop the Network Intelligence Plane (NI) as part of the EU's Horizon 2020 project. They extend the original MAPE-K framework to include i) an inference loop, ii) a training loop, and iii) a different training loop for online learning. These loops are implemented by a Network Intelligence Function block (NIF) of an NI. This enhanced model, suitable for network management is called Network Monitor-Analyze-Plan-Execute (N-MAPE-K).

D. ANTICIPATION, ABSORPTION, ADAPTATION, AND RECOVERY OVER TIME (A^3RT)

A^3RT framework captures the system's ability to *anticipate* adversaries and known risks, *absorb* their impact, and *adapt* to evolving conditions using available resources to maintain functionality [28]. The framework structures resilience across three layers: (i) *robustness*, (ii) *short-term resilience*, and (iii) *long-term resilience*.

- **Robustness** stage focuses on anticipating, resisting, and absorbing faults and preventing immediate service disruption using reactive defense mechanisms, redundancy, and fault isolation.
- **Short-term resilience** refers to the network's ability to detect faults quickly and recover essential functions by adapting resource allocation and configurations.
- **Long-term resilience** is achieved by diagnosing root causes, learning from past disruptions, refining system

processes, updating system functions, and implementing long-term improvements.

E. RESILIENT AND SURVIVABLE NETWORKS (RESILINETS)

ResiliNets [29] adopts the $D^2R^2 + DR$ strategy (i.e., Defend, Detect, Remediate, Recover, Diagnose, and Refine) as a systematic approach for building resilient networks. It is a successor to the EU-funded ResumeNet project. The framework has two operational loops: (i) the inner loop to execute the Defend-Detect-Recover-Remediate (D^2R^2) cycle and (ii) the outer loop to execute the Diagnose-Refine cycle. The core components of this framework are:

- **Defend** the network from potential risks and faults by proactively monitoring the network, assessing risks, identifying vulnerable system resources, and securing the network with firewalls.
- **Detect** anomalies and identify the root cause, by monitoring the network, traffic, and comparing with normal operational baselines to classify anomalies.
- **Remediate** the symptoms by taking corrective actions to mitigate issues.
- **Recover** by restoring operations through infrastructure redeployment, traffic rerouting, and load balancing.

During outer DR loop phase, deeper root cause analysis is conducted, and $D^2R^2 + DR$ process is refined for future resilience.

F. SUMMARY

Despite their different application domains, all the aforementioned frameworks share common attributes for building resilient systems. For example, NIST's detect function and ResiliNETs' detect function share a similar goal of detecting a network anomaly. Resilient-by-Design's predict function predicts a possible anomaly, and MAPE-K's monitor and analyze function monitors and analyses a given state to predict or highlight anomalies.

Similarly, NIST's respond and recover function, Resilient-by-design's protect and progress functions, MAPE-K's plan and execute function, and ResiliNETs' remediate and recover functions capture the system transition from a degraded to a stable process via recovery and remediation.

NIST CSF's govern function, Resilient-by-Design's progress function, MAPE-K's knowledge base adaption, A3RT's long-term resilience loop, and ResiliNETs' diagnose and refinement functions all contribute to improving system performance over the long term. These common resilience attributes provide the conceptual basis for the architectural discussion in Section III, where the architecture of a resilient network is presented and these attributes are mapped to their corresponding technology enablers.

It is also worth noting that, in addition to the aforementioned frameworks, several standardized resilient network architectures, such as IEEE Time-Sensitive Networking (TSN) [15] and IETF Deterministic Networking (DetNet) [30], incorporate mechanisms such as redundancy, time-aware scheduling, and fault tolerance to constrain degradation during faults, reduce latency, and provide deterministic performance and resilience at the data plane. These architectural mechanisms align with the resilience enablers discussed in later sections of this paper. When complemented by adaptive resilience control loops, such deterministic architectures can support holistic network resilience for mission-critical and industrial applications.

III. NETWORK RESILIENCE ARCHITECTURE, LIFECYCLE AND OPERATIONAL PHASES

From the definition of network resilience introduced in Section I, four primary capabilities emerge:

- The ability to *prepare* for potential disruptions;
- The ability to *resist and absorb* the disruption while maintaining function;
- The ability to *respond and adapt* to evolving situations; and
- The ability to *recover* quickly and resume normal operation.

Network resilience architecture is a continuous closed-loop control mechanism that enables these capabilities. The architecture shown in Figure 2, comprises monitoring and telemetry functions to observe the network state, analysis and decision-making functions to detect anomalies and assess system degradation, and techniques to mitigate operational degradation through redundancy, isolation, configuration management and security controls.

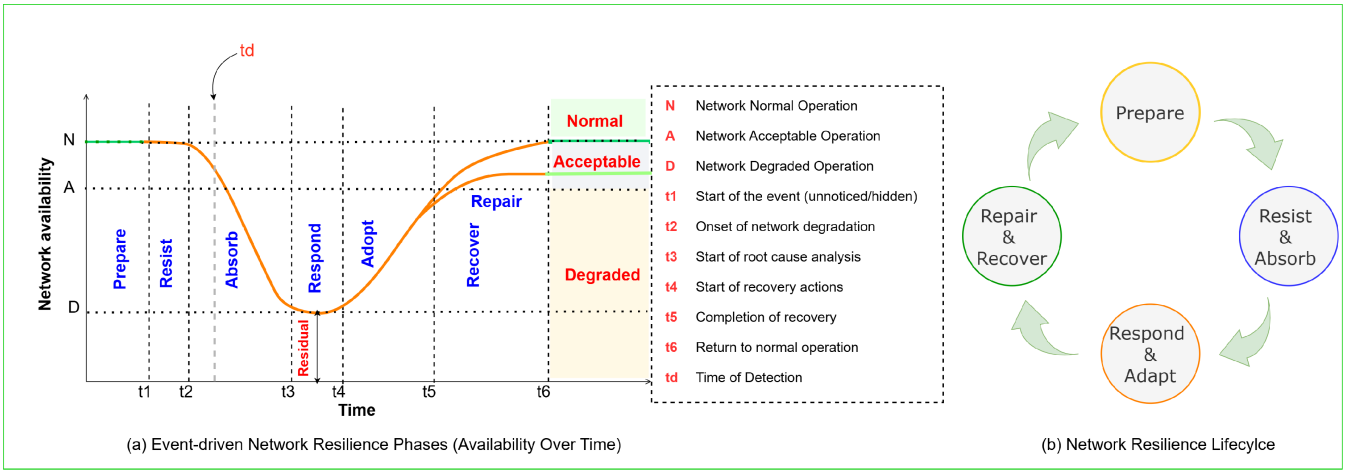
From this architectural framework, four network operational stages emerge during a disruption. These are (i) Prepare, (ii) Resist and Absorb, (iii) Respond and Adapt, and (iv) Repair and Recover. These phases represent the observable system behavior resulting from the interaction of architectural components.

These operational stages of a network during a disruption are depicted using a resilience graph presented in the Figure 1 (a), adapted from [31].

A. OPERATIONAL PHASES AND ENABLING TECHNOLOGIES

A resilience graph is a conceptual representation used to quantify a system's performance (e.g., availability or reliability) as a function of time, with time depicted on the x-axis and the corresponding performance metric on the y-axis. During a disruption, a system operates below its normal performance level and subsequently restores functionality during the recovery phase. Resiliency curves capture this behavior by quantifying the periods in which the system is operating normally, experiencing degradation, or undergoing recovery. Key temporal indicators derived from these curves such as time to detect (TTD), time to respond, and time to recover provide insight into the effectiveness of deployed resilience mechanisms. For instance, a shorter TTD indicates more effective monitoring and alerting capabilities.

Since resilience graphs apply to different domains, the number of stages and the corresponding definitions vary



(a) Event-driven Network Resilience Phases (Availability Over Time)

(b) Network Resilience Lifecylce

FIGURE 1. Timeline of network resilience phases.

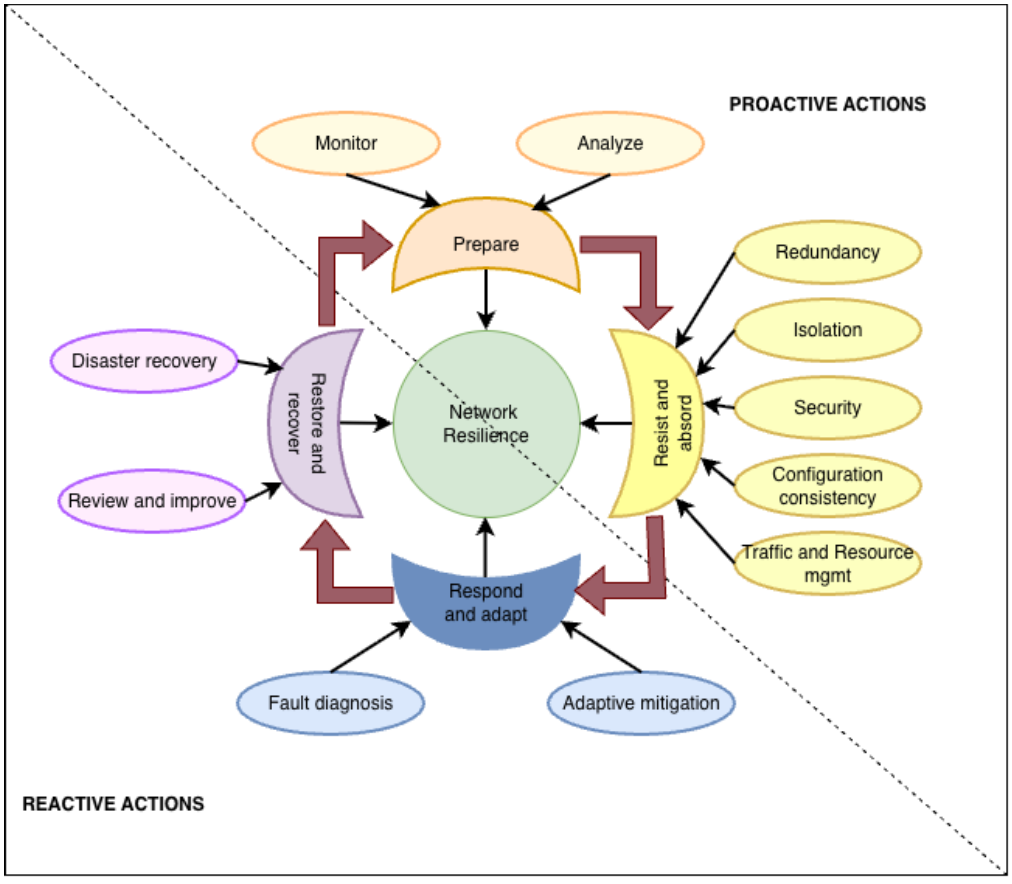


FIGURE 2. The network resilience architecture: Capabilities and enabling technologies.

across domains. For example, Reifert et al. [28] identify anticipation, absorption, adaptation, and recovery as the four key abilities of a network and examine network resilience in conditions with varying levels of criticality.

The following subsections will discuss the network operation at each specific stage and discuss corresponding technology enablers as summarized in Figure 2.

B. PREPARE

In this stage, the network operates normally, focusing on anticipating and preparing to withstand potential failures. This stage is subdivided into two sub-stages: (i) monitoring and (ii) analysis. Monitoring and analysis are two joint activities. The information gathered during the monitoring phase is interpreted and analyzed to guide timely interventions during

the analysis phase. The following subsections further describe each of these processes.

1) MONITORING

Monitoring different aspects of a network, such as traffic distribution, infrastructure (links, devices, and cloud-based systems), configuration, and security, provides early indicators of potential network incidents.

Protocols such as Simple Network Management Protocol (SNMP) [32] and Remote Monitoring (RMON) [33] are examples of network monitoring protocols. SNMP is a request-response protocol between an SNMP manager and an SNMP agent, with the manager periodically querying the agent for information in the form of Managed Information Bases (MIBs). The SNMP agent also generates notifications to the manager for network events. RMON is an extension of SNMP and monitors physical, media, and IP parameters of a network. Unlike SNMP, it can be configured on a single interface in a subnet to remotely capture network statistics for later transmission to the SNMP manager.

For monitoring traffic, protocols such as IPFix [34]and eBPF [35] exist. A group of packets sharing the same parameters (e.g., Source IP, Destination IP, Port numbers) is called a flow. A device configured with IPFlow Information eXport (IPFix) can periodically send flow statistics (L2, L3, and L4) to a collector. The extended Berkeley Packet Filter (eBPF) provides a development environment to run programs in the Linux kernel without modifying the kernel. eBPF can attach to specific kernel points (such as a socket) to inspect, modify, and filter traffic. Shen et al. [36] develop a network-centric distributed tracing tool by extending existing eBPF functions.

Alongside device and traffic monitoring, security vulnerabilities, configuration consistency, and faults must be proactively monitored and identified.

Tracing techniques samples and stores the traced samples for further analysis. While helpful for analyzing application performance, trace data must be securely protected [37]. *Distributed tracing* is a technique for tracing request flows in microservice-based systems, such as the 5G core. Commercial tools like Microsoft's Azure Private 5G tracing [38] capture end-to-end user call traces, which aid in diagnosing configuration errors and identifying network performance issues.

Mechanisms such as Chaos engineering may be used to assess the network tolerance towards unforeseen incidents by introducing faults in a controlled way [39]. However, since fault injection into production networks carries inherent risks, emulation platforms such as Mininet [40] and GNS3 [41] are used to build test networks and apply configurations. More recently, Digital Twins (DTs) [42], [43] are a safer alternative, as they are virtual replicas of physical entities and their functionality. They enable real-time monitoring, system optimization, and resilience validation and experimentation [44].

2) ANALYSIS

Network monitoring generates rich data that can be analyzed to determine the next course of action. ML and AI tools can detect unusual traffic patterns, inspect packets, and predict impending component failures, enabling rapid response. Abbasi et al. [45] identify four key application areas of AI and ML in network management and analysis as: (i) traffic classification based on port, payload, and flow, (ii) fault detection, isolation, and correction, (iii) anomaly and malware detection, and (iv) traffic prediction.

Shi et al. [46] propose leveraging Time-Series data on faults, anomalies, and failures to detect and predict router failures. Islam et al. [47] introduce a prediction scheme based on Long Short-Term Memory (LSTM) [48] for identification and rectification of communication link failures. Camargo et al. [49] present an ML-based approach to predict traffic demand and dynamically reconfigure each network slice to allocate computational resources and ensure Quality of Service (QoS). While AI and ML applications can provide insights into the current state of networks, the decision to act must ultimately lie with network engineers and be guided by a core set of performance metrics, such as network uptime, availability, packet loss, retransmission rates, failure rates, and the operational team's expertise.

In addition to analyzing operational telemetry, networks must also analyze security risks and potential attack paths. Vulnerability scanning tools, such as OpenVAS [50] and Nessus [51], can proactively identify known weaknesses in software, devices, services, and configurations by comparing them against vulnerability databases, vendor advisories, and threat intelligence sources [52], [53]. This supports early detection of exposed assets and helps operators prioritize remediation before vulnerabilities are exploited. Proactive threat modeling methods are also helpful for identifying vulnerabilities and anticipating attack progression. For example, attack graphs represent possible attack scenarios and paths using information such as network configuration, vulnerability distribution, threats, and attack templates [54], [55], [56].

It is also important to verify device configurations. In proactive static analysis, parsing and symbolic analysis techniques are used to validate the configuration's adherence to constraints. These techniques do not require configuring the network. For example, Feamster and Balakrishnan [57] present a tool to validate BGP configurations against constraints of path visibility (propagate all usable paths) and route validity (propagate only valid routes) constraints. Similarly, Tang et al. [58] analyze the configuration of OSPF, BGP, ACLs, and RouteMaps, to highlight behavioral and structural inconsistencies. Such a static analysis can reveal a variety of faults, including unauthorized network partitions, invalid route propagation, and incorrect policy expressions.

C. RESIST & ABSORB

During the *Resist* phase, the network actively withstands the adverse event, leading to a limited scope and severity of the failure, though customer impact is minimal. As failures

cascade and network performance degrades significantly, the network enters the *Absorption* phase, during which customers begin to experience a noticeable impact on service. Automated disaster and data recovery processes must be established during this phase (as discussed in Section III-E) to ensure rapid service restoration and continuity of critical functions.

Redundancy (logical and physical), isolation (network and traffic), and security are fundamental aspects of a resilient network. Additionally, consistent network configuration and proactive traffic management policies ensure the network remains operational even under the most adverse conditions. The following subsections provide a detailed discussion on corresponding technology enablers for each design aspect.

1) REDUNDANCY

Redundancy is one of the important principles of a resilient network. Redundancy can be achieved at both physical and logical layers. Commonly, physical redundancy reinforces single points of failure by adding additional components (i.e., *N+x*) to ensure high network availability. *N+x* redundancy is a fault-tolerant system design where *x* extra components are added to the components required for normal operation (N) [59]. The devices are configured to operate in either active-active or active-passive mode, providing a highly available network. In the active-active mode, all *N+x* devices concurrently process traffic, thereby maximizing resource utilization and fault tolerance. In contrast, the active-passive mode designates *N* devices as active, while the remaining *x* devices remain on standby to take over in the event of a failure. This *N+x* principle applies to both physical infrastructure such as routers, firewalls, switches, and cables, and to virtual infrastructure, such as Cloud-Native Network Functions (CNF). For instance, 5G CNFs are deployed across at least two independent and geographically separate Container-as-a-Service (CaaS) clusters [60].

Beyond the physical layer (Layer 1), logical redundancy mechanisms operate at Layers 2 (L2) and 3 (L3). At L2, aggregation protocols such as the Link Aggregation Control Protocol (LACP) [61] bundle multiple ports into a single logical link (trunk). In the event of a primary link failure, LACP automatically reroutes traffic through the remaining active links, thereby minimizing network downtime and maintaining connectivity. Because LACP aggregates only the number of ports supported at both ends, any additional links are placed in a hot-standby state. This configuration reduces the effective bandwidth and demonstrates that redundancy can lead to underutilized resources when port channels are established between mismatched hardware [61].

Protocols such as Fast Spanning Tree Reconnection (FSTR) [62] and Rapid Spanning Tree Protocol (RSTP) [63] provide redundancy at the network topology level by preserving alternate loop-free paths and enabling rapid re-convergence following link or node failures. Nevertheless, they cannot address higher-level L3 routing protocol malfunctions.

For end-to-end Layer 3 continuity, link-state routing protocols such as Open Shortest Path First (OSPF) [64] and Intermediate System to Intermediate System (IS-IS) [65] support redundancy by maintaining alternate next hops in their routing tables. When the primary path fails, these precomputed or newly recomputed alternative routes can be used to restore packet forwarding continuity.

While routing protocols such as OSPF and IS-IS provide path redundancy and end-to-end forwarding continuity, first-hop redundancy protocols such as the Virtual Router Redundancy Protocol (VRRP) [66] provide resilience at the default gateway. Where redundant gateways are deployed, VRRP assigns a single virtual IP address to multiple gateways, with one router acting as the designated primary router and forwarding traffic through that virtual IP address. The remaining routers remain in standby mode and assume the virtual IP only when the active router fails, thereby maintaining uninterrupted gateway access. End hosts continue sending packets to the same virtual IP address and require no configuration changes. However, VRRP provides no inherent authentication mechanism and therefore cannot prevent unauthorized routers from impersonating the active router through spoofing [66].

Beyond gateway redundancy, networks also employ fast failover and high-availability mechanisms that operationalize redundancy by rapidly switching to backup paths, forwarding state, or standby resources when failures occur deeper in the path or within the router itself.

Fast Reroute (FRR) [67] and Failure-Insensitive Routing (FIR) [68] are examples of fast-failover mechanisms that automatically reroute packets around link or node failures. When MPLS is enabled with FRR [69], the router adjacent to the failed link is notified and performs local rerouting using pre-configured backup paths as new forwarding paths. Since these backup routes are established prior to failure, they must be carefully planned to ensure effective recovery and avoid routing loops [70]. Similarly, FIR [68] enables routers to react to failures locally without waiting for global routing convergence. Routers detect packets arriving on unexpected interfaces and autonomously infer the set of potential link failures that may have caused the deviation, then use alternative exit interfaces to bypass the suspected failed links, thereby enabling fast localized recovery.

At the device level, high-availability features such as Non-Stop Forwarding (NSF) and Non-Stop Routing (NSR) [71] provide additional fault tolerance by allowing packet forwarding and routing operation to continue during certain reboot scenarios. NSF allows a device to reboot without disrupting packet forwarding, because the forwarding tables stored in Application-Specific Integrated Circuits (ASICs) remain active. This enables continued forwarding based on the last-known-good state during a control-plane restart. NSF is effective only when either the control plane or the data plane is rebooted, but not both. Similarly, NSR preserves interface and kernel state information during a reboot, while routing protocol processes continue to run on backup routing

engines, allowing seamless switchover. One prerequisite for configuring NSF is that all neighboring devices must be NSF-aware and support the same protocol extensions [72]. However, relying on the last-known-good state may cause routers to continue forwarding packets to non-responsive peer routers [73].

2) ISOLATION

Network isolation restricts and contains fault propagation, preventing cascading network failures by segmenting the network and segregating traffic at both the physical and logical levels.

Physical separation of infrastructure (nodes and links) and the use of diverse media technologies (copper, fiber, microwave) create distinct network segments to contain faults. Since faults are localized, it leads to faster recovery and better management. Isolation also strengthens security while ensuring service continuity during failures or maintenance activities.

Logical isolation of network resources can be categorized into (i) network isolation and (ii) traffic isolation. Network-level isolation creates separate administrative and forwarding domains. Enterprises commonly use Virtual Local Area Networks (VLANs) [74] to segment networks at L2 to restrict the L2 broadcast domain. Nevertheless, VLANs need manual configuration and are static. At L3, Border Gateway Protocol (BGP) [75] Autonomous System (AS) isolates an ISP's administrative domains. Within an AS, internal BGP (iBGP) confederations [76] restrict routing advertisements and BGP communities [77] localize traffic and filter routing updates by tagging routes with policies, resulting in controlled isolation.

Further isolation can be achieved by enabling Virtual Routing and Forwarding (VRF) [78]. VRF extends network isolation by creating a unique routing table for each network tenant on a router, enabling tenant isolation and fault containment. Each virtual routing table maintains an independent Forwarding Information Base (FIB) and consumes router resources (CPU and memory), leading to increased router loading times, extended maintenance windows, and frequent memory upgrades [79]. Vendor-specific optimizations, such as selective VRF table download, address this issue by creating only the necessary routing tables [79].

For traffic-level isolation, techniques such as tunneling and virtualization are used to build overlay networks [80] on top of existing physical network infrastructure. Protocols such as Generic Routing Encapsulation (GRE) [81], Virtual Extensible LAN (VXLAN) [82], Network Virtualization using GRE (NVGRE) [83], and Ethernet Virtual Private Network (EVPN) [84] provide L2 segmentation over an underlying L3 network while using a different encapsulation mechanisms. For instance, VXLAN encapsulates packets in a UDP header, whereas GRE uses a simpler, protocol-type-based header without UDP encapsulation. In mobile networks, the GPRS Tunneling Protocol (GTP) [85] is used to transport user traffic between the Radio Access Network (RAN) and the core network, supporting per-user session isolation over shared IP transport infrastructure.

3) SECURITY HARDENING

Security threats are a significant risk to network stability, operation, and availability. It is hence important to identify, plan, and implement proactive security measures. To identify threats and discover vulnerabilities, tools such as CVSS and attack graphs can be used as discussed in section III-B2.

Once these risks have been identified, preventive controls must be deployed to reduce exposure and restrict unauthorized access. A first level of defense can be established by enabling Network Access Control (NAC) mechanisms to monitor users and devices attempting to connect to the network and by enforcing measures such as role-based access control, multi-factor authentication, and the principle of least privilege. These measures reduce the likelihood of adversarial access by requiring additional authentication and contextual validation before access is granted to critical applications or transactions.

Access Control Lists (ACLs) and firewalls provide an additional traffic-level barrier by filtering unauthorized or malicious traffic, including traffic originating from compromised or misused accounts. ACLs can also be configured for rate limiting and protection against multiple protocol-based attacks, such as TCP SYN, RST, ping, and UDP flooding attacks [86]. They are also used in Source Address Validation (SAV) processes to help prevent IP address spoofing.

Additionally, network segmentation can be used to create logical or virtual boundaries between domains with different levels of criticality and trust. For instance, demilitarized zones (DMZs) are commonly deployed to separate external-facing services from internal networks [87]. Such isolation policies help contain faults and attacks within defined security zones and limit their lateral movement across the network.

Encryption techniques such as Secure Shell version 2 (SSHv2) [91], Transport Layer Security (TLS) [92], IP Security (IPsec) [93], and MAC Security (MACsec) protect data and preserve confidentiality even when network paths are compromised. TLS protects application-layer communications, IPsec provides network-layer encryption for VPNs and secure tunnels, and MACsec offers link-layer encryption for LAN segments.

4) CONFIGURATION CONSISTENCY AND VALIDITY

To effectively resist and absorb disruptions, fundamental network settings must be configured consistently across the infrastructure. Assigning IP addresses, configuring VLANs, enabling routing and trunking, allocating bandwidth, setting buffer sizes, and time synchronization are a few basic settings that must be applied uniformly across physical and virtual infrastructures. Security settings, such as configuring ACLs, enabling role-based access, and configuring DMZs to protect network infrastructure and resources while supporting reliable service continuity, are also necessary, along with

TABLE 2. Summary of some of the recent telecommunications outages caused by misconfiguration.

Year	Provider	Country	Cause	Duration	Total Call Failures	Failed Emergency Calls
2024	AT&T [88]	US	Misconfiguration	12 hrs	92 million	25000
2023	Optus [3]	Australia	Configuration oversight	$\geq$ 12 hrs	51.3 million	2697
2022	KDDI [89]	Japan	Misconfiguration	61 hrs:25 min	22.78 million VoLTE impacted	undisclosed
2020	T-Mobile [90]	US	Misconfiguration and optical link failure	12 hrs	41%	23621

virtualization techniques for creating overlay networks and network slices. Any misconfiguration in the above settings can affect network availability, reliability, performance, and security, leading to outages and service degradation, as listed in Table 2.

Since communication networks are distributed, configuration consistency and accuracy across the network are essential. To enforce such consistency and ensure that the intended resilience design is accurately reflected in deployed configurations, a Single Source of Truth (SSoT) [94] can be used to store the network model and provide a single point of reference for both network engineers and automation tools. Network automation frameworks such as Ansible [95] query the SSoT, use templates to generate vendor-specific configurations, and reliably deploy them at scale. Automation engines, together with a well-maintained SSoT, help enforce consistency and significantly reduce the likelihood of human error during network deployment. They also support uniform deployment and version-controlled rollback.

While misconfiguration may be identified using the proactive static analysis techniques discussed in Section III-B2, outages do not always result from misconfiguration. Various other causes, such as weather-induced incidents, faulty infrastructure, faulty updates, and security breaches, can also result in network failures or outages. Therefore, the intended resilience mechanisms, including redundancy, isolation, failover logic, and security protections, must be explicitly incorporated into network configurations and applied consistently across the infrastructure so that they function as expected during disruptions.

5) TRAFFIC AND RESOURCE MANAGEMENT

Proactive traffic engineering and resource planning help maintain connectivity during partial network failures by enabling traffic to be redistributed away from failed, congested, or degraded paths. RFC 9522 [96] describes several traffic engineering approaches, including capacity planning, Equal-Cost Multi-Path (ECMP)-based load balancing, backup path configuration, and other redundancy mechanisms discussed in Section III-C1.

Additionally, constraint-based traffic engineering mechanisms such as Resource Reservation Protocol-Traffic Engineering (RSVP-TE) and Segment Routing Traffic Engineering (SR-TE) enable explicit path control based on traffic demands and administrative policy constraints. RSVP-TE establishes label-switched paths (LSPs) with bandwidth reservations through hop-by-hop signaling and can be combined with MPLS Fast Reroute (FRR) to provide rapid local protection following failures [69]. In contrast, SR-TE encodes explicit paths as segment identifiers in packet headers, enabling the ingress node to steer traffic along selected routes without per-path signaling at each hop. When combined with Topology-Independent Loop-Free Alternate (TI-LFA), SR-based forwarding can support sub-50 ms local repair [97]. Owing to its stateless architecture, SR-TE also enables rapid path updates by modifying the segment list at the tunnel ingress, whereas RSVP-TE typically requires re-signaling along the new path. During incidents, Path Computation Elements (PCEs) can centrally recompute paths that satisfy the required traffic engineering constraints.

D. RESPOND & ADAPT

In the Respond and Adapt state, focus shifts from proactive mechanisms to reactive intervention to identify the root cause of the outage and develop mitigation strategies to minimize impact. While pre-configured mechanisms such as redundancy, traffic engineering, resource allocation, access controls, and rate limiting provide immediate protection, as discussed in Section III-C1, the respond and adapt stage involves taking deliberate actions to mitigate ongoing disruptions. These actions are taken after the pre-configured proactive mechanisms have activated, but the service disruption persists.

1) FAULT DIAGNOSIS

To identify faults, network operators and automated diagnostic tools analyze observed symptoms by parsing data, detecting patterns, and correlating related events. Telemetry data, logs, performance metrics, and configuration states are common data sources for anomaly detection. Pattern-matching techniques, such as LTMatch [98], transform unstructured logs into structured templates, while statistical methods identify deviations from normal behavior.

Event correlation techniques further identify temporal and spatial relationships among log entries and telemetry records. For example, Kobayashi et al. [99] propose a method for extracting contextual information from network logs and correlating events across multiple log streams to detect fault patterns. Similarly, Liu et al. [100] present CoCaTel, a causal telemetry framework that correlates events from multiple sources for fault and anomaly diagnosis. To achieve this, they extend in-band telemetry with additional information to trace event causality. Such techniques enable rapid diagnosis by processing large volumes of operational data to isolate root causes and inform mitigation strategies. The Simple Event Correlator [101] is another example of an open-source

tool for advanced event correlation in network and security management.

Among the different causes of network faults, misconfiguration remains one of the most prominent. Two common approaches for identifying misconfiguration are (i) proactive static analysis and (ii) reactive data-plane derivation techniques [58], [102]. Proactive approaches are used to identify configuration faults before deployment, whereas reactive data-plane derivation techniques validate misconfiguration by analyzing traffic snapshots that capture unintended network behavior after deployment. Tools such as Batfish [103] integrate both proactive and reactive approaches to derive the actual data plane from device configurations and environmental context, and generate data-plane snapshots for analysis. Batfish can also combine multi-vendor configurations to construct a control-plane model. Similarly, Libra [104] leverages MapReduce to partition the topology into prefix-based subgraphs and analyze forwarding tables to detect loops, inconsistencies, and black holes.

2) ADAPTIVE MITIGATION

Root cause analysis is often an elaborate process involving multiple diagnostic steps and coordination across teams. In the meantime, service continuity may need to be preserved through interim adaptive measures. Such measures can be applied manually by network operators, or automatically through policy-driven control mechanisms, to modify flow priorities, steer traffic, reallocate bandwidth, reconfigure tunnels, and update ACLs or firewall rules to contain the impact of the fault.

Additional mitigation actions may also be used to restore or maintain service continuity, such as instantiating additional Virtual Network Functions (VNFs) [105] to replace failed instances or increase capacity, reconfiguring service function chains to bypass faulty components, and applying graceful degradation strategies. These adaptive measures help maintain acceptable service levels while permanent repairs or longer-term corrective actions are being developed.

E. REPAIR & RECOVER

Restoration activities commence after the incident and fault have been identified. These activities involve correcting the fault and restoring the last-known optimal configuration. A Single Source of Truth (SSoT), combined with automation tools such as Ansible, can be used to reapply configurations and return the network to a known operational state. Configuration restoration is followed by health checks to verify that routing protocols, end-to-end paths, and virtual networks, including tunnels and overlay networks, have been successfully re-established. Any manually applied mitigation policies should then be rolled back gradually to ensure that no further inconsistencies are introduced.

Post-incident review is a crucial part of the recovery process and should include a blameless post-mortem aimed at identifying, documenting, and addressing the root cause of the incident. This approach fosters a culture of accountability, transparency, and continuous improvement. Once root cause analysis is complete, the incident, its impact, the corrective actions taken, and the lessons learned should be formally documented.

F. SUMMARY

This section has outlined the current landscape of technical enablers for network resilience. Collectively, these technologies enable networks to anticipate, withstand, absorb, adapt to, and recover from outages and service disruptions. Some enablers, such as redundancy planning, capacity engineering, security hardening, and network isolation, are primarily proactive, whereas others, such as adaptive traffic rerouting, dynamic resource reallocation, and policy modification, are applied reactively during or after incidents.

Although these enablers have been discussed individually, many operate across multiple stages of the resilience life cycle. Network monitoring, analysis, configuration management, security assessment, and traffic engineering all span across preparation, response, adaptation, and recovery stages. For example, proactive configuration validation during the preparation stage helps ensure configuration consistency across network devices and verifies that fallback mechanisms are correctly deployed. Only when such mechanisms are configured and maintained correctly can the network withstand faults and limit service degradation. In contrast, reactive configuration validation may be required during the respond-and-adapt phase to diagnose inconsistencies and support mitigation actions. Similarly, security mechanisms such as segmentation, encryption, and ACL enforcement help the network withstand cyber threats, but these controls may also need to be updated dynamically during incident response.

Virtualization further strengthens resilience by decoupling logical network functions and services from the underlying physical infrastructure, thereby enabling flexible resource management and adaptive recovery. Through mechanisms such as VNFs, Virtual Routing and Forwarding (VRF), and segment routing, logical resources can be dynamically created, isolated, relocated, and reconfigured. From a resilience perspective, virtualization and network slicing act as architectural enablers that support fault isolation, resource reallocation, adaptive reconfiguration, and accelerated recovery, allowing services to be sustained or restored even when parts of the physical infrastructure are degraded or unavailable.

More broadly, resilience is strengthened when network isolation, configuration management, and pre-established recovery mechanisms are combined. Mechanisms such as redundant paths, failover strategies, backup configurations, and secure isolated Out-of-Band (OOB) management channels can significantly accelerate service restoration when planned and implemented in advance [106]. Security-oriented resilience frameworks, including the Cyber Resilience Engineering Framework (CREF) [107] and the NIST Cybersecurity Framework [108], likewise emphasize goals such as anticipation, withstanding disruption, recovery, and

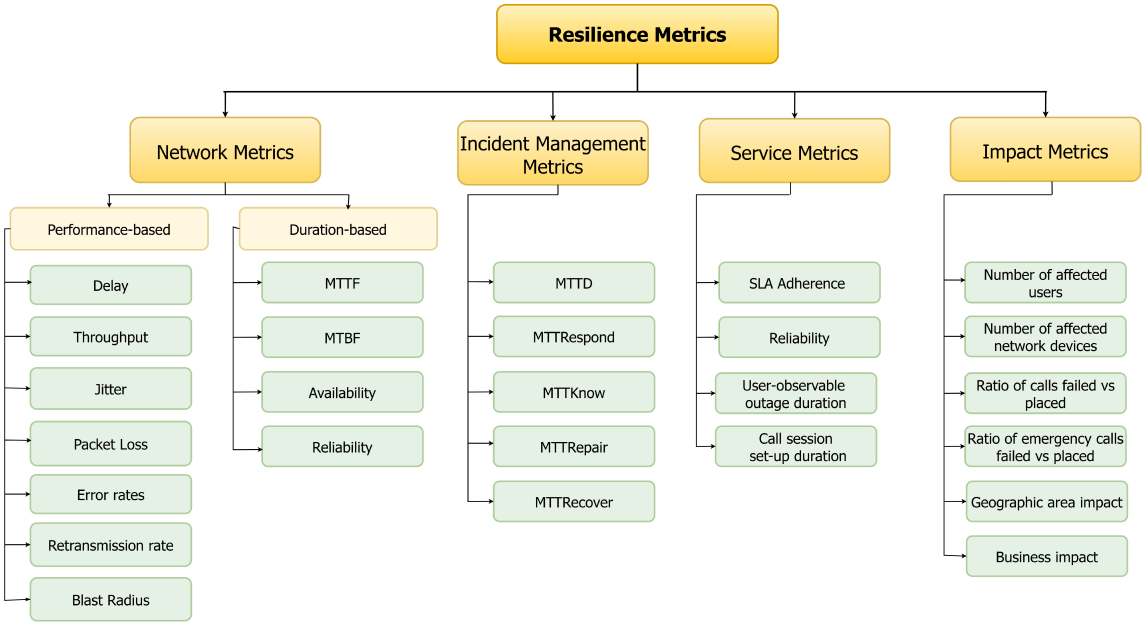


FIGURE 3. Network resilience metrics.

adaptation or evolution [107], [108]. Continuous monitoring to detect vulnerabilities and anomalies, together with infrastructure protections such as firewalls and intrusion detection systems, are among the hardening measures identified by Bodeau et al. [109] to strengthen cyber resilience.

Lastly, regular backups, rigorous testing of automated changes, and the use of SSoTs with version control help ensure that recovery procedures can be executed reliably during outages. By ensuring that only validated and verified configurations are propagated, these practices reduce the risk of outages, performance degradation, and security breaches.

In the following section, we discuss widely used metrics for measuring network resilience.

IV. NETWORK RESILIENCE METRICS

Metrics such as reliability, blast radius, service degradation, and Mean Time To Failure measure network health. Duration based metrics described below, measure the duration the network was up, recovering or degraded as shown in network resilience graph. For systematic analysis, metrics are classified into network, incident management, service, and impact metrics as described in the following subsections and summarized in Figure 3.

A. NETWORK METRICS

We classify network metrics into two categories: (i) performance-based metrics to serve as lagging indicators of faults; and (ii) duration-based metrics to measure time-based aspects of system reliability and recovery.

Following are common network performance-based metrics as defined by Secgin [110]:

- **Delay** is the total time required to transmit all bits of a packet, including propagation, queuing, processing, and transmission delays. Faulty hardware (e.g., faulty ports and media), misconfiguration (e.g., incorrect routing leading to longer paths, incorrect queue sizes) can cause higher delays.
- **Throughput** is the actual amount of traffic successfully transmitted over a network link in a given period. Reduced throughput may indicate network congestion, inefficient routing, or suboptimal link utilisation.
- **Jitter** is the variation in packet delay over time. High jitter can significantly impact real-time applications such as VoIP and video streaming. It often indicates network congestion or route instability.
- **Packet Loss** quantifies the number of data packets that never reached the intended destination. Network congestion, hardware issues, software problems, and lossy media are some of the factors that contribute to packet loss.
- **Error Rates** is the ratio of incorrectly transmitted packets to the total number of packets. These erroneous packets may include runt packets (unusually small packets), packets with Cyclic Redundancy Check (CRC) errors, or packets corrupted due to other transmission issues.
- **Retransmission Rate** is the ratio of retransmitted packets to the total number of transmitted packets. Transmission Control Protocol (TCP) retransmissions are common and often indicate network issues such as link congestion, packet loss, or excessive delay.

Network operation is characterized by uninterrupted working intervals (uptime) followed by repair periods (downtime). These durations can be used to model reliability and availability of a network [111]. Thus, duration-based metrics quantify uptime, downtime, availability, and reliability (See Figure 1):

- **Mean Time To Failure (MTTF)** is the expected average time that the network is likely to operate as intended before a failure occurs [112], [113].
- **Mean Time Between Failures (MTBF)** is a measure of the average time between two consecutive failures [113]. In practice, MTTF and MTBF are used interchangeably to measure uptime. For *non-repairable* faults, MTTF measures uptime and for *repairable* faults, MTBF measures the uptime of a system [112].
- **Availability** is the probability that the network is operational at a given point in time. It measures network uptime and is given by [111].

$$Availability = \frac{Uptime}{Uptime + Downtime}$$

,
- **Reliability** is defined as the probability that the network has not failed after a time period t. It is typically modeled as a function using the exponential distribution and given by [111] and [113].

$$R(t) = e^{\frac{-t}{Uptime}}$$

In addition to the metrics listed, blast radius is a term commonly used in the context of network security breaches to describe the extent of the impact caused by a network fault. A larger blast radius indicates poor fault isolation and fault propagation across a wider portion of the network.

B. INCIDENT MANAGEMENT METRICS

Operational teams use Incident management metrics to assess both frequency of incidents and the efficiency in their responses. While definitions may vary across organizations, these metrics generally measure the (i) effectiveness of detection, diagnosis, and recovery during incidents (e.g., MTTD, MTTI and MTTR) and (ii) proactive preparedness efforts (MTBT). Together, these metrics not only measure operational performance but also support continuous improvement across both the response and preparation phases. Briefly,

- **Mean Time To Detect (MTTD)** [114], [115]:
  Time to Detect (TTD) [116] is the time taken to detect a fault. In Figure 1(a), it is the interval between *t1* and *td*. MTTD is the average of all TTDs over a given observation period. This metric reflects the effectiveness of monitoring systems and operational alertness. TTD is sometimes referred to as *Time to Identify*.
- **Mean Time To Respond (MTTRespond)** [114]:
  Time To Respond (TTRespond) [116] indicates the time taken to elicit a response from the Operations team. In Figure 1 (a), it corresponds to the interval between *td* and *t3*. This metric is usually used in conjunction with Mean Time to Repair and Recover as discussed below. MTTRespond is the average of TTRespond durations of all incidents over a period of time.
- **Mean Time To Know (MTTK)** [114], [115]:
  Time to Know (TTK) [116] is the time required for the operations team to diagnose and characterize the fault. MTTK averages this duration across incidents and indicates diagnostic efficiency.
- **Mean Time To Repair (MTTRepair)** [114], [115]:
  Time to Repair (TTRepair) [116] is the time taken to implement mitigation or repair strategies once a fault is diagnosed. In Figure 1 (a), this corresponds to the interval between *t4* and *t6*. MTTRepair measures the efficiency of operational teams in restoring functionality, though it does not necessarily imply full resolution of the root cause.
- **Mean Time To Recover (MTTRecover)** [114], [115]:
  Time to Recover (TTRecover) represents the end-to-end duration required to detect, diagnose, respond, and restore service. It aggregates detection, diagnosis, repair, and verification activities. MTTRecover is thus reflects the overall effectiveness of incident management.

In addition to the metrics mentioned above, the Mean Time Between Tests (MTBT) refers to the average interval between successive tests conducted on the network to identify potential issues. This metric measures the preparedness of a network operations team.

C. SERVICE METRICS

Service metrics evaluate the network's ability to maintain service commitments to end-users during normal and adverse or disrupted conditions. They measure user experience, contractual obligations, and availability of critical services such as emergency calls [117].

- **Service Level Adherence** (SLA) is a KPI to assess the network's ability to adhere to uptime and availability commitments.
- **Reliability** from the end-user perspective, can be assessed through the following sub-metrics [118]:
  - **Signal Availability** is the proportion of time users can successfully access a mobile network.
  - **Data Connectivity** is the proportion of time when the user device can connect to the internet while the network is available.
  - **Task Completion** is the proportion of times a user-initiated task such as call initiation, file upload, browsing session, is completed.
- **User-Observable Outage Duration** quantifies the period during which users, including those attempting emergency communication were unable to access network.
- **Call Session Set-up Duration** [119], [120] is the time between a user initiating a call and receiving an alerting signal (e.g., ringtone) from the destination.

D. IMPACT METRICS

Impact-based metrics measure the over-all impact of the network outages. Below are some of the impact metrics [121]:

- **Number of Affected Users** quantifies the total users impacted by the network service disruption.

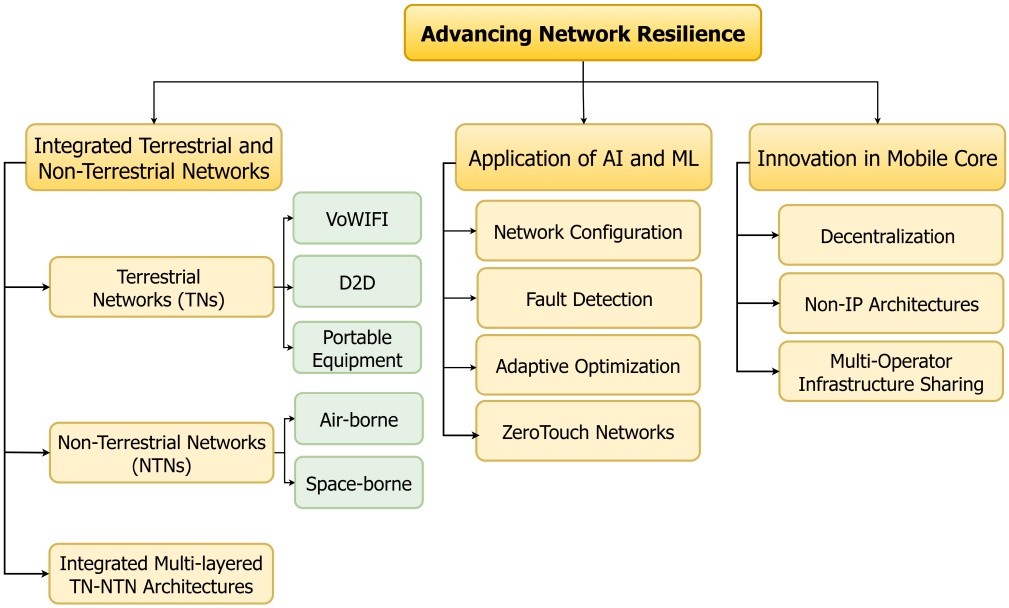


FIGURE 4. Emerging strategies for advancing network resilience.

- **Number of Affected Network Devices** quantifies the total number of impacted devices.
- **Ratio of Calls Fulfilled vs. Placed** is the proportion of users unable to access the network during an outage.
- **Ratio of Emergency Calls Failed vs. Placed** serves as a critical indicator of a network's performance during a crisis, directly measuring the proportion of failed attempts of making emergency calls.
- **Geographic Area Impacted** indicates the geographic area affected by the network outage.
- **Business Impact** such as monetary loss, market share loss, loss of reputation and customer churn.

All the metrics discussed thus far provide valuable insights into both network performance and the effectiveness of operational teams. However, they must be used and interpreted with caution. Metrics such as Time to Detect (TTD) and Time to Repair (TTR) do not capture factors beyond a team's scope and thus may not accurately reflect the actual duration for resolving an incident [122]. While performance metrics can quantify network behavior, they do not provide insight into the root cause of an issue. Since various underlying causes may display similar symptoms; they must be identified and resolved appropriately. Finally, for deeper diagnosis, previously discussed techniques such as distributed tracing and telemetry analysis are required.

V. ADVANCING NETWORK RESILIENCE WITH INTEGRATION, INTELLIGENCE, AND INNOVATION

Mechanisms discussed in Section III may not be sufficient for ensuring network resilience. Despite deploying state-of-art infrastructure, misconfiguration may create cascading failures and lead to large-scale outages such as the Optus outage in 2023 [3]. Such incidents underscore the necessity to further reinforce network resilience through alternative strategies beyond conventional techniques. We now explore three such emerging strategies - (i) integration of diverse networks for infrastructure redundancy and isolation, (ii) application of AI and ML in future networks for fault detection, configuration management and optimization and (iii) innovative architectures as shown in Figure 4.

A. INTEGRATED TERRESTRIAL AND NON-TERRESTRIAL NETWORKS

Current landscape of networks can be broadly divided into (i) terrestrial networks and (ii) non-terrestrial networks. Terrestrial Networks (TNs) form the backbone of modern communication systems and continue to evolve rapidly. Although widely deployed, they remain vulnerable to natural disruptions and are costly to provision in sparsely populated or remote regions [123]. Non-Terrestrial Networks (NTNs) comprise of Air-borne and Space-borne infrastructure.

The integration of Terrestrial Networks (TN) and Non-Terrestrial Networks (NTN) has emerged as a key research focus in the development of next-generation communication systems, as exemplified in Figure 5. Combining the cost-effectiveness and reliability of TN with the global coverage of NTN offers significant potential to enhance overall network resilience. However, there is a growing need to move beyond basic interoperability and towards a fully unified *Network of Networks*, for end devices to seamlessly connect to terrestrial or non-terrestrial components based on availability and performance requirements [124], [125].

The following sections briefly introduce the main components of TN and NTN before discussing their integration. Table 3, presents a comparative summary of key attributes for terrestrial and non-terrestrial solutions, including energy requirements, coverage capability, and the time of

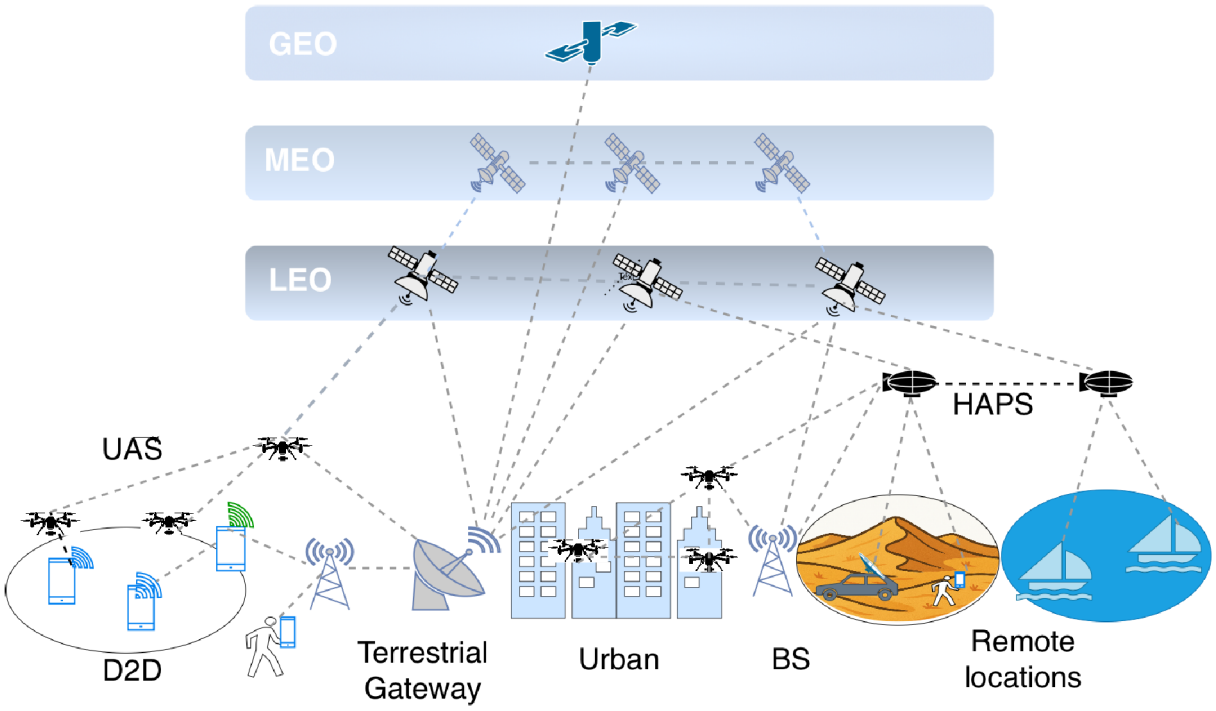


FIGURE 5. Network of networks.

TABLE 3. Comparison of key attributes of terrestrial and non-terrestrial solutions.

Technology	Infrastructure Dependency	Power Requirements	Coverage Scope	Reactive/Proactive	Latency(Round Trip Time)
D2D/ad hoc	Low	Low to High [139]	Localized	Reactive	19.003 ms (one-way UE to BS) [139]
Network-in-a-box	High	Plug-in [140]	Campus Area	Reactive	10.01 ms [141]
Cell-on-Wheels	High	Plug-in	10 - 15 kms [142]	Reactive	50 - 100 ms (4G), $\leq$ 10 ms (5G)
HAPS	Very High	Battery [143]	5 -200 km [144]	Proactive and Reactive	$\leq$ 10 ms [145]
AAV/Drone BS	High	Battery	5 -200 km [144]	Reactive	$\leq$ 10 ms [145]
LEO satellite	Very High	Solar-powered	100 - 1000 km [144]	Proactive	$\leq$ 50 ms [145]
MEO satellite	Very High	Solar-powered	100 - 1000 km [144]	Proactive	$\leq$ 150 ms [145]
GEO satellite	Very High	Solar-powered	200 - 3500 km [144]	Proactive	$\leq$ 700 ms [145]

intervention (i.e., when the solution becomes operational relative to the onset of an outage).

1) TERRESTRIAL NETWORKS (TNS)

Beyond traditional cellular systems such as 4G and 5G, the TN landscape also consists of technologies like Device-to-Device (D2D) communications [126] and portable cellular equipment. These technologies are discussed in following subsections.

a) Voice-over-WiFi (VoWiFi)

VoWiFi enables user devices to access the 4G or 5G core network using existing WiFi infrastructure, particularly when cellular radio access is unavailable. In 4G, the User Equipment (UE) connects via the Evolved Packet Data Gateway (ePDG) through IPsec over untrusted non-3GPP access [127] and in 5G, the Non-3GPP Interworking Function (N3IWF) provides similar functions [128]. ePDG and N3IWF facilitate secure authentication, manage mobility, and enable session continuity between Wi-Fi and cellular domains. This capability is especially beneficial for routing voice traffic via fixed broadband networks in the event of failure of cellular networks.

b) Device-to-Device Communication

Device-to-device (D2D)communication enables UEs (e.g., smartphones, tablets, and wearables) in proximity to each other, establish direct links for localized data exchange. D2D network operate in either: (i) infrastructure-assisted mode, and (ii) infrastructure-less mode [129]. In infrastructure-assisted mode, a central entity (e.g., a base station (BS)) manages device discovery, connection setup, resource allocation, and synchronization. In infrastructure-less D2D, devices handle discovery, synchronization, and resource allocation autonomously and often adopt Mobile Ad hoc Network (MANET) principles to self-organize. They might also use multi-hop routing with on-demand protocols such as Dynamic Source Routing (DSR) [130] and Ad hoc On-Demand Distance Vector (AODV) [131]. To enable external connectivity (e.g., Internet access) in such scenarios, a gateway node with access to the broader IP backbone is required.

The rapidly self-organization ability of D2D networks makes them particularly valuable for emergency communications during disasters, especially when cellular infrastructure is partially or entirely unavailable. Several studies [132], [133], [134] propose D2D-based emergency protocols that extend coverage by relaying messages through neighboring devices until an operational BS is reached.

Despite these advantages, D2D-based solutions face practical limitations. They depend on sufficient UE density in the affected area and may introduce relaying delays before traffic reaches an active gateway or BS. Some protocols buffer emergency calls for later delivery [132], [133], which, although useful, increases latency. Additionally, enabling D2D requires pre-configuration of devices such as dedicated interfaces and protocol support, which may not be universally available. Finally, multi-hop D2D are susceptible to eavesdropping, false data injection, and Sybil attacks [135].

c) Portable Communication Equipment

An alternative to distributed network such as D2D, is a centralized and portable infrastructure to restore network functionality in disconnected regions. Devices participating in D2D communications might not reach the gateway, due to sparse distribution, power depletion, or protocol limitations. A portable cell site can temporarily restore services.

A Network-in-a-Box (NIB [136]) is a compact, self-contained system designed to provide a rapidly deployable, on-demand network connectivity in challenging environments, such as disaster zones or remote areas with limited or no existing network infrastructure. Each NIB is equipped with radio interfaces to deliver services directly to end users. A key advantage of NIBs is availability of a various backhaul connectivity options. NIB can connect to satellite, microwave, Ethernet, or WiFi links. Depending on the required coverage area and user density, one or more NIBs can be deployed to provide connectivity.

A Cell-on-Wheels (CoW) [137] is a portable cellular site designed for quick deployment and retrieval. CoWs typically consists of RAN, a power supply, and backhaul connectivity realized via operational fiber infrastructure, satellite links, or radio transmission. Some advanced CoWs are also capable of performing core network functions, enabling local communication within the coverage area in the absence of external connectivity thus creating self-reliant mobile network. The U.S. FirstNet [138] initiative is a prominent example of such a system.

2) NON-TERRESTRIAL NETWORKS (TNS)

Non-Terrestrial Network infrastructure (NTNs) can be subdivided into (i) Air-borne and (ii) Space-borne networks. Air-borne (aerial) systems typically operate between 8–50 km and include Autonomous Aircraft Systems (AAS) at lower altitudes and High-Altitude Platform Stations (HAPS) in the stratosphere. Space-borne systems comprise of satellite systems operating at different altitudes and with varying beam footprint. Low Earth Orbit (LEO) satellites operate at an altitude of 300 km - 1500 km, Medium Earth Orbit (MEO) satellites, operating at altitudes between 7,000 km and 25,000 km [144] Geostationary Equatorial Orbit (GEO) orbit at 35,786 km altitude [144]. There are two modes of operation for the space /aerial systems [146]: (i) bent-pipe, (ii) regenerative.

- **Bent-pipe payload** is also known as transparent payload. The aerial or satellite components perform functions such as frequency filtering, conversion, and amplification.
- **Regenerative payload** requires components such as modulation and demodulation onboard the aerial or satellite devices to perform base station functions in addition to the components require to perform frequency filtering, conversion and amplification.

a) Air-borne

An *Autonomous Aircraft Systems (AAS)* consists of a Autonomous Aerial Vehicle (AAV) and a controller, communicating with terrestrial or satellite networks [147], [148]. They are rapidly deployed to establish temporary networks in areas with damaged infrastructure or sparse populations, especially for emergency communication.

Multiple studies [149], [150], [151], [152] propose operating Autonomous Aerial Vehicles (AAVs) as Aerial Base Stations (ABSs) to relay user data to other AAVs [149], [150] or forwarding it to a terrestrial base station (BS) [152]. Ali et al. [153] propose an on-demand Drone Small Cell (DSC)-based coverage network to support emergency communications in disaster-affected regions by using a dynamic scheduling strategy to prioritize emergency requests thus effectively reducing access delay and minimizing the probability of denial of service for high-priority users.

High-Altitude Platform Station (HAPS) make a powerful communication platform with minimal signal delay [154] and have a wider beam area than AAS. They operate at higher altitudes than AAS and are particularly well-suited to enhance connectivity in remote or isolated regions lacking cellular access or to address coverage gaps in terrestrial networks [145]. They can also operate as private networks or serve as wireless backhaul links between base stations and edge data centers. These capabilities position them as effective backup solutions during emergencies for sustaining critical services such as emergency calling.

HAPS platforms comprise of balloons and aircrafts. Project Loon [155] balloons are examples of *lighter-than-air* platforms while fixed-wing, solar-powered aircraft such as Airbus Zephyr [156] is an example of *heavier-than-air* HAPS platform. Notably, project Loon was deployed to provide emergency calling services during Hurricane Maria in Puerto Rico in 2017 [157].

While AAS and HAPS are quick to deploy in remote areas, AAS-based networks face several limitations such as restricted battery life, limited coverage areas, and increased network complexity when scaling to larger fleets particularly in terms of synchronization and handover management [152], [158]. In contrast to AAS, HAPS exhibits high endurance, operate on solar-power, and position in the stratosphere.

b) Space-borne

Satellite networks operate above Air-borne systems and provide wider beam footprint. Telecom operators are increasingly adopting LEO-based satellite backhaul to complement terrestrial networks. For example, in Australia, Telstra has partnered with OneWeb to connect remote sites using LEO satellite backhaul [159]. Similarly in South Africa, MTN group collaborated with US-based LEO provider, Lynk Global, to integrate terrestrial network with LEO infrastructure [160].

Meshed LEO constellations use inter-satellite links (ISLs) for direct satellite-to-satellite communication [161], [162] and route data packets autonomously in space, reducing dependence on terrestrial gateways and resulting in lower end-to-end latency. Examples of ISL-enabled systems include Starlink [163], Project Kuiper [164], and Telesat Lightspeed [165]. In contrast, OneWeb [166] constellation uses a bent-pipe model, with heavy reliance on ground stations. Other notable mesh LEO constellations include China's Guowang [167] and Qianfan [168], Russia's Sfera [169], and Europe's IRIS^2 program [170].

LEO satellite constellations offer low-latency NTN connectivity, but they can incur a large number of handovers (approximately 9912/s at a user density of 33.36/km2) [171] and rely heavily on terrestrial infrastructure for mobility and handover management [172]. GEO constellations require fewer satellites and provide reliable communication, but with high latency. MEO constellations are positioned between LEO and GEO and offer acceptable latency with fewer satellites than LEO. MEO and GEO satellite constellations have fewer satellites than LEO and cover a larger area and operate at lower orbital velocities than LEO satellites, resulting in fewer handovers. Examples of MEO and GEO satellites are the O3b mPower constellation [173] and ViaSat [174], respectively.

Despite their reliable connectivity and wide-area coverage, space-based systems require substantial capital investment and infrastructure. Satellite constellations cannot be rapidly deployed in response to sudden disasters. Although their mesh architecture enables fast inter-satellite data exchange, they still rely on ground gateways for access to terrestrial infrastructure (e.g., data centers) which might also get affected during a disaster.

3) INTEGRATED MULTI-LAYERED TN–NTN ARCHITECTURES

Emerging hierarchical architectures that integrate terrestrial networks with GEO, MEO, LEO, HAPS, and AAV layers can enhance network resilience by combining the coverage, latency, and control advantages of different network tiers.

Most integrated TN–NTN architectures adopt a hierarchical control structure in which LEO satellites are coordinated or managed by higher-orbit MEO and GEO satellites [171], [175], [176], [177]. This hierarchical design leverages the complementary strengths of each layer, including wide-area coverage, lower latency, and reduced handover frequency. For instance, Qin et al. [171] propose a Hierarchical Distributed Mobility Management Architecture (HDMMA) to leverage MEO's high capacity and LEO's low latency to improve overall system stability by reducing handover frequency. The architecture leverages MEO satellites as controllers for a LEO cluster, overseeing intra-cluster handover by using a global view. LEO satellites acting as local controllers within a LEO cluster also enable simple local handover within the cluster. Similarly, Huang et al. [175] propose Integrated Computing and Networking for LEO Satellite Mega Constellations (ICN-LSMC). In this architecture, MEO satellites act as domain controllers, performing network control and service scheduling for clusters of LEO satellites. As LEO satellites move along their orbital paths, MEO satellites assist with handover to adjacent LEO domains. In addition, a ground controller serves as a master controller, coordinating the MEO satellites, handling inter-domain functions, and maintaining a global network view.

Bi et al. [176] also propose an SDN-based integration architecture. In their approach, terrestrial SDN controllers manage OpenFlow (OF)-enabled GEO, MEO, and LEO satellites. OF-enabled GEO satellites act as a space backbone interconnecting clusters of MEO and LEO satellites. These satellites use onboard flow tables to forward packets either within the same layer or across different layers.

The three-tier control hierarchy discussed above comprises GEO satellites acting as backbone nodes and high-level controllers, MEO satellites serving as domain controllers for LEO clusters and regional aggregation, and LEO satellites providing low-latency access and local control feedback. This hierarchical architecture introduces redundancy and supports localized fault detection, thereby strengthening the network's ability to resist and respond to physical failures.

While satellite networks provide long-term and wide-area coverage, they are generally not suitable for immediate deployment in response to emergency situations. In contrast, AASs and HAPs can provide on-demand and maneuverable connectivity, serving as either access platforms or backhaul nodes [178], [179], [180], [181]. When integrated with satellite networks, these aerial platforms can extend connectivity to areas with sparse or disrupted terrestrial coverage [179], [181].

For example, Lyu et al. [179] propose deploying AAVs along mobile cell edges to maximize the minimum throughput of terrestrial users by optimizing AAV trajectories, allowing the AAVs to function as aerial base stations jointly with ground base stations. Arani et al. [178] develop a deep reinforcement learning algorithm for aerial base stations, including HAPS and AAVs, to autonomously optimize aerial trajectories for data service provision while relying on LEO satellites for backhaul connectivity.

Alternatively, AAVs and HAPs can themselves serve as backhaul platforms, as proposed in [180] and [181]. Jia et al. [181] propose a LEO-backhaul-enabled AAV/HAP aerial base station architecture to serve mobile users in areas lacking terrestrial coverage, using game theory to match

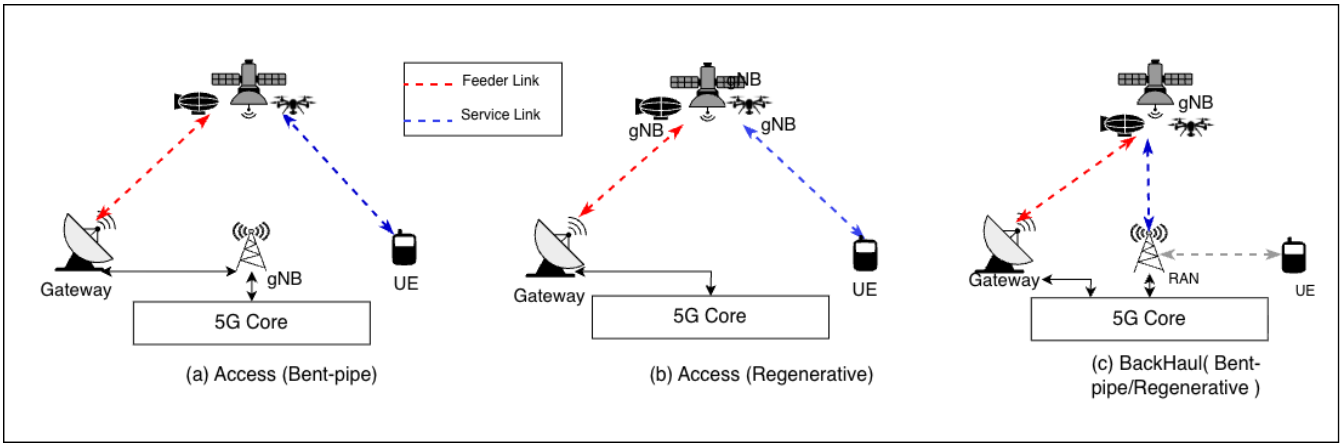


FIGURE 6. NTN as access and backhaul networks.

users with HAPS and LEO satellites. Similarly, Challita and Saad [180] propose an on-demand multi-hop aerial AAV backhaul network for scenarios where terrestrial backhaul is unavailable. Their approach learns air-to-air and air-to-ground links to provide reliable connectivity, resulting in a self-organized tree of AAVs connected to ground stations and operating as a backhaul network.

End-to-end integration across terrestrial, aerial, and space networks results in a multi-domain, multi-path architecture with inherent path diversity, isolation, and improved service continuity. However, such cross-layer integration requires more than physical interconnection; it also depends on standardized protocols and coordinated cross-layer management to address challenges including synchronization, localization, handover management, indoor coverage limitations, and power efficiency, particularly for regenerative satellites and HAPS. Alongside 3GPP studies, such as 3GPP TR 38.811 [182], 3GPP TR 38.821 [183], and 3GPP TR 38.832 [184], several academic and industrial organizations have proposed architectures to support this integration.

In integrated networks, NTN can operate as either a backhaul network or an access network. Service links connect UEs to non-terrestrial nodes, feeder links connect non-terrestrial components to terrestrial gateways, and inter-satellite links connect satellites to one another [146]. Service links can support basic connectivity, such as emergency voice calls, whereas services requiring access to data centers or the public Internet rely on feeder-link connectivity to terrestrial infrastructure [123]. In the Satellite-Terrestrial Backhaul Network (STBN) architecture discussed in [124], UEs access the mobile core through either terrestrial or satellite backhaul, as shown in Figure 6 (c). When NTN operates as an access network, UEs may access the mobile core through either terrestrial or satellite connectivity for broadband services, depending on network availability, while aerial base stations bridge the terrestrial and space segments to reduce latency and signal attenuation and improve coverage, as illustrated in Figure 6 (a) and (b).

3GPP's Integrated Access and Backhaul (IAB) [185] is another promising architecture for integrating terrestrial and non-terrestrial networks. In this architecture, Radio Access Network (RAN) functions are distributed, while a central unit remains connected to the core network and to a wireless backhaul that relays user traffic toward the central unit. The architecture mainly comprises IAB nodes, which relay traffic for UEs, and an IAB donor, which operates as a regular gNB and connects to the core network [186]. Pugliese et al. [187] summarize several possible deployment models in which satellites, including LEO and GEO systems, operate either exclusively as IAB nodes or jointly as IAB nodes and IAB donors. In such architectures, satellites can receive traffic from remote locations, relay signals among themselves through inter-satellite links (ISLs), and forward traffic toward the terrestrial core network.

Taken together, these architectures exploit the complementary failure characteristics of different network segments: terrestrial infrastructure is susceptible to localized physical damage, satellite systems are exposed to orbital and solar risks, and aerial platforms are constrained by weather and endurance limitations. Through hierarchical control, on-demand aerial coverage, and standardized end-to-end protocols, integrated TN–NTN architectures can provide the path diversity, redundancy, and fault isolation required to maintain resilient connectivity across diverse operating conditions.

B. APPLICATIONS OF AI AND ML

AI and ML techniques have permeated nearly every industry, including communication networks. The real-time nature of data transmission makes Network Intelligence (NI) a challenge and an active area of research. Like so, there has been a growing body of work applying AI and ML techniques to the areas of network design and configuration, fault detection, optimization, analysis and management respectively. Following sections briefly describe recent works in these areas. By automating the resilience cycle (Figure 1 (b)), AI/ML-enabled self-healing networks can proactively detect anomalies, predict potential failures, localize faults for faster

recovery, and ultimately reduce downtime. These capabilities contribute to improved service continuity, enhanced user experience, and minimized business disruption.

1) NETWORK CONFIGURATION

In recent years, AI and ML techniques have been increasingly leveraged to detect and mitigate configuration errors, thereby preventing cascading failures. For example, in [188], two Graph Neural Network (GNN) models are proposed for:(i) detecting routing misconfiguration between customer and provider edge routers, and (ii) identifying VPN routing configuration errors across different providers' edge routers. Beurer-Kellner et al. [189] train a GNN-based neural synthesizer. They adopt an encoder-process-decode architecture to train the synthesizer to produce the distribution for unknown parameters provided as part of the input. Thus, generating low-level device configurations from high-level intents or specifications.

More recently, several studies have explored the use of Large Language Models (LLMs) to assist with network configuration generation and translation. For instance, Wang et al. [190] propose NETBUDDY, an LLM-powered network configuration generator. NETBUDDY employs three LLMs to convert natural-language policies into formal specifications, then into high-level configurations, and finally into low-level configurations, such as P4 and BGP, using network-specific information. A verifier is applied at each stage of the pipeline to validate the generated output. Fang et al. [191] fine-tune an LLM with vendor-specific knowledge to generate device configurations. Wei et al. [192] propose an Intent-based Retrieval-Augmented Generation (IRAG) framework to extract configuration intents and incrementally translate them, thereby improving correctness during migration across heterogeneous vendor devices.

Mondal et al. [193] observe that GPT-4 alone is insufficient for generating reliable draft network configurations and therefore propose a strategy termed Verified Prompt Programming (VPP). This approach integrates GPT-4 with formal verification tools, such as BatFish [103], to validate generated configurations. Rather than eliminating manual verification entirely, VPP aims to significantly reduce overall human effort by incorporating automated validation into the workflow. In this framework, GPT-4 primarily interacts with structured, human-readable outputs from verification and testing tools, while only the final validated outcome is presented to the human operator. The authors further note that additional evaluation is necessary to assess whether GPT-4 can perform incremental modifications in complex network environments without inadvertently impacting existing configurations.

2) FAULT DETECTION

Proactive fault detection minimizes the likelihood of faults evolving into catastrophic failures, and reactively, it accelerates the recovery process to restore the network to an acceptable operational state. Thus, fault detection serves as both a proactive and reactive measure. A wide range of AI and ML algorithms have been applied in this domain. Support Vector Machines (SVMs), Long Short-Term Memory (LSTM) networks for time-series forecasting, and Neural Networks (NNs) such as Convolutional NNs and Recurrent NNs combined with encoders and clustering techniques [194], [195] are some of the commonly applied ML algorithms.

Due to their usefulness in long sequences of data-based predictions (e.g, historical network telemetry), LSTM-based methods are prominent. Nam et al. [196] conduct anomaly detection using both log data and resource usage data. The model uses LSTM to calculate the probability of an event at time $t+1$ based on input data until time t. A mismatch between the predicted probability from the baseline probability (calculated as an Anomaly score) determines if the event is an anomaly. Islam et al. [47] used LSTM to correlate historical radio and weather data with link failures proactively.

Camargo et al. [49] applied ML models for dynamic slice reconfiguration. The management, orchestration, and automation layer collects telemetry and predict the probability of alarms. Network slices are reconfigured based on this probability. The workflow uses a FeedForward Neural Network(FNN) ML model to generate alarm probability. Foroughi et al. [197] in their proposed model AI-driven network Telemetry (ADT), use principal-angle comparisons to assess changes in network state, detect deviations in time-series streams, and flag anomalies as potential precursors to service faults. Shi et al. [46] apply a Change Point (CP)-based anomaly detection scheme. They first establish all the CP and build CP windows using information around CP. They then apply ML techniques (cluster techniques and expert rule filtering) to the CP windows to distinguish normal windows from abnormal windows. CPs thus identified for new data is classified as either normal or abnormal.

Chen et al. [198] propose a transformer-based Language Model for Network Traffic (NetLM). NetLM automates the fault-localization, strategy generation, and verification cycle. The tool also autonomously handles fault repairs based on learning outcomes.

Finally, industry frameworks, such as ITU-T Y.3173, explicitly identified predictive fault management as a cornerstone of AI-driven, self-healing future networks.

3) ADAPTIVE OPTIMIZATION

Unlike traditional resource management methods, AI/ML-based models can dynamically adapt to the diverse nature of 5G and 6G services. 5G and 6G offer enhanced Mobile Broadband (eMBB), Ultra-Reliable Low-Latency Communication (URLLC), massive Machine Type Communication (mMTC) services for applications and require dynamic resource (network slicing and route) optimization and management, leading several works [199], [200], [201], [202] to propose AI and ML-powered network optimization techniques.

Jain et al. [201] propose a RL-based dynamic network slicing mechanism. Agents use RL to learn optimal allocation strategies and receiving rewards for positive behaviors. The authors evaluate their RL model against supervised and unsupervised learning for throughput and energy consumption, observing that latency for URLLC has reduced by 30% and throughput has increased by 20% for eMBB services.

Beyond resource allocation, AI/ML has been used to improve traffic engineering. Gorshenin et al. [202] use a deep Gaussian mixture model (DGMM) for event reconstruction and forecasting. They compare it against other methods such as SVMs, gradient boosting, and LSTM-based TE models and conclude that their DGMM model is 6.82 to 22.8 times faster than other models. Hussien et al. [203] compare various models such as SARIMA, FB Prophet, AdaBoost, XGBoost LSTM, CNN, ensembles CNN+LSTM, and hybrid CNN-LSTM for traffic prediction. Ensemble CNN+LSTM and hybrid CNN-LSTM, while being accurate, were also the slowest, with longer computation times.

Alongside academic endeavors, global projects are pushing toward operational deployment of AI and ML. For example, the EU-funded DAEMON project [27] proposed an Intelligence Orchestration Platform (NIO) for coordinating multiple Network Intelligence Instances (NIIs). NIO continuously monitors performance, accuracy, and health of AI-driven control functions for fully autonomous operation and functions within the Management and Orchestration (MANO) framework.

4) ZEROTOUCH NETWORKS

Zero-Touch network and Service Management (ZSM) is a fully autonomous network management with minimal human intervention. A ZSM-enabled network can interpret its current state, reason over observed conditions, and propose configuration updates that network engineers can verify, validate, and deploy [204]. AI and ML models for decision-making and programmable infrastructure such as SDN, NFV, and DT [205], are core components of ZSM. ZSM networks are designed to be self-managed, guided by intent-based service specifications provided by network engineers [206]. ZSM is also foundational for the AI-native communication architecture proposed in the EU's Hexa-X project [6], [207].

ZSM architectures are self-healing, possess local autonomy, effectively isolate faults, and rapidly reconfigure, thereby leading to an overall improvement in network resilience [208]. The EU-funded Automated Zero-Touch Cross-Layer Provision (ACROSS) project is a prominent work in this direction. The architecture is distributed, consisting of autonomous domain-level orchestrators arranged in a grid formation. An AI engine automates service deployment and life cycle management across these orchestrators. They are responsible for managing local edge environments and are coordinated by a global orchestrator.

In summary, Network Intelligence (NI) is a significant step toward developing self-healing and adaptive networks. Such integration, however, comes with several challenges. Firstly, communication networks are delay-intolerant, and real-time analysis can introduce additional delays. Also, NI models are often not transparent enough to support human-in-the-loop operations, which is essential for troubleshooting the NI components. Finally, user data privacy and energy efficiency are additional, but important challenges that need to be addressed. Despite these challenges, AI and ML offer substantial potential to enhance network resilience by proactively addressing outages and dynamically allocating resources.

C. INNOVATION IN MOBILE CORE

This section explores several innovative architectures within the mobile core and control infrastructure that directly influence network resilience and complement the integration- and intelligence-driven techniques discussed in the earlier subsections. These include: (i) decentralization and autonomy, (ii) non-IP architectures, and (iii) multi-operator resource sharing. Together, these approaches illustrate how rethinking mobile core network design can improve resilience in the face of large-scale disruptions.

1) DECENTRALIZATION

Distributed mobile core creates self-sufficient network segments, and reduce reliance on centralised infrastructure and enhance resilience, particularly in emergency communication scenarios. The central idea is to deploy RAN-related functions at the network edge. Hassan et al. [210] describe a low-cost wireless access network called Magma to abstract the access network from the core architecture. They introduce access gateways, to perform essential 5G functions such as Access and Mobility Function (AMF), Unified Data Management (UDM), Session Management Function (SMF), and User Plane Function (UPF), crucial for local session establishment and management. Additionally, Magma adopts a hierarchical SDN control plane architecture, where a global centralised orchestrator maintains authoritative network-wide information, and a local control plane manages the runtime state of user activity. Mukherjee et al. [211] argue that the gateways and Mobility Management Entity (MME) are bottlenecks in mobile core and propose a distributed mapping system to map identifiers associated with devices, services and context to a set of locators while also mapping end-devices to locations. They further propose a flat core network design, where routers (similar to IP network), eliminating the need for gateways. This design requires embedding routing functionality directly into base stations.

Corici et al. [209] investigate different edge-core network split models for 5G core network as shown in Figure 7. Among the three proposed models, *Autonomous Edge split* ensures that the edge network implements all the core functions and is capable of operating as a fully standalone network. In contrast, the *Locally Administered Edge Split* deploys AMF and SMF locally, for access control, mobility, and session management. Split-core models can reduce the fault domain and establish highly resilient zones, particularly in regions prone to disasters or infrastructure outages.

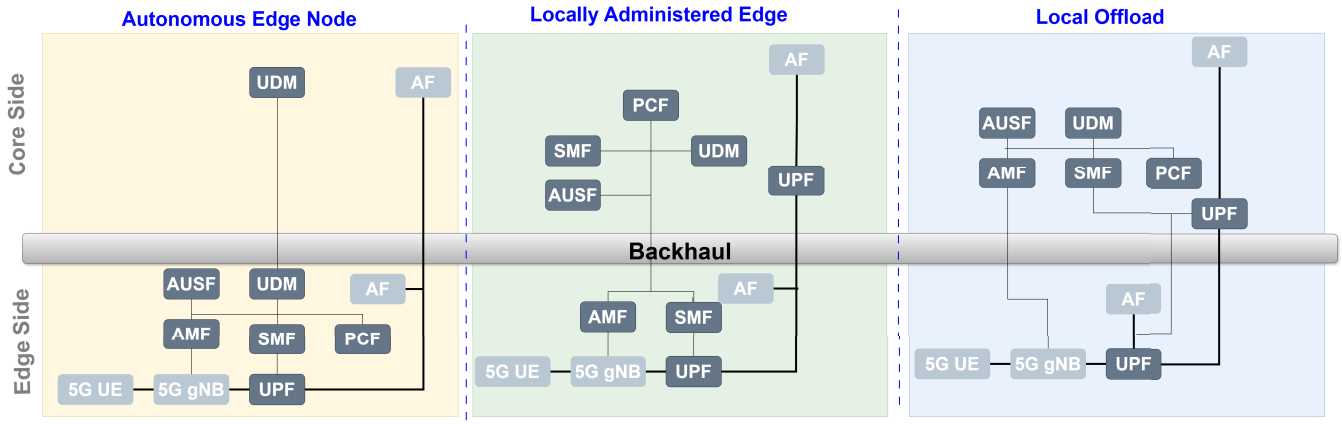


FIGURE 7. Splitting core functions across edge and core [209].

However, while they significantly improve resilience, they also introduce complexity, especially in synchronizing and integrating user data [209].

Saleem et al. [212] argue that, although the 5G core adopts a service-based architecture (SBA), many existing approaches for improving end-to-end core resilience still rely on optimization techniques originally developed for NFV-based monolithic designs, such as shared-memory interfaces to reduce inter-service delay or implementing functions as a single binary to reduce latency. To address these limitations, they propose TEGRA, a scalable and resilient SBA-based 5G core that supports fine-grained auto-scaling, load balancing, and fault tolerance within the mobile core. Their evaluation shows that TEGRA significantly reduces latency while keeping the code base relatively compact.

2) NON-IP ARCHITECTURES

5G core's service-based architecture is flexible but constrained by IP-based point-to-point signaling that couples data with a physical location (IP address). IP is resource-intensive and prone to disruption. Atalay et al. [213] thus propose adopting Named Data Networking (NDN) as a core architectural principle to build next-generation mobile networks. NDN decouples content from addresses, allowing in-network caching, multi-path data retrieval, and eliminating centralized dependencies. These properties collectively enhance fault tolerance and improve overall network resilience.

NDN represents one of the prominent realizations of Information-Centric Networking (ICN) [214]. In NDN, data is requested by *name* rather than by endpoint address. A requester posts an *interest packet* for the desired data, and any intermediate node (e.g., router or cache) can reply with its cached copy of requested *data packet*. This content-centric retrieval makes NDN suitable for resource-constrained or disrupted environments by offering improved scalability and resilience in the presence of failures.

Atalay et al. [213] present an NDN-enabled 5G core prototype aimed at: (i) reducing the signaling overhead required for Virtual Network Function (VNF) registration with the Network Repository Function (NRF), (ii) for point-to-point security management and (iii) transporting end-user traffic between the RAN and the core user plane as shown in Figure 8. NDN inherently signs every data packet, thereby eliminating the need for a central trust anchor such as NRF [215] which overseas VNFs OAuth-based secure channel operation. Atalay et al's evaluation demonstrates that session setup time for service chains was significantly lower compared to the 5G-AKA procedure. Due to in-network caching, redundant VNF deployments are present for seamless failover mechanism. This distributed, content-centric approach highlights the potential of NDN as a building block for more resilient beyond-5G core architectures.

Despite the benefits NDN, it comes with challenges. Firstly. while NDN can coexist with existing IP infrastructure [216], existing IP devices cannot support NDN and require development and deployment of new infrastructure. Secondly, while in-network caching provides data redundancy, such content is also prone to poisoning attacks among other attacks [217].

3) MULTI-OPERATOR INFRASTRUCTURE SHARING

Multiple operators can share infrastructure through standardized mechanisms such as the Multi-Operator Core Network (MOCN) [218]. MOCN enables multiple operators to share RAN. Such cooperation among operators improves service continuity when the network of a single provider fails. For example, in Australia, Optus and TPG have recently entered into an MOCN agreement to share RANs and spectrum [219], thereby extending their combined network reach to 98.4% of the population.

Tipper et al. [9] extend this concept by proposing that operators *pool* a portion of their resources to serve as backups for collaborating operators. Along the same lines, Abhishek et al. [220] propose a virtualization framework that allows 5G operators to recover from base station and backhaul failures cooperatively.

Network faults or vulnerabilities propagate across all collaborating operators, and resource responsibility, sharing agreements are some of the challenges that need to be

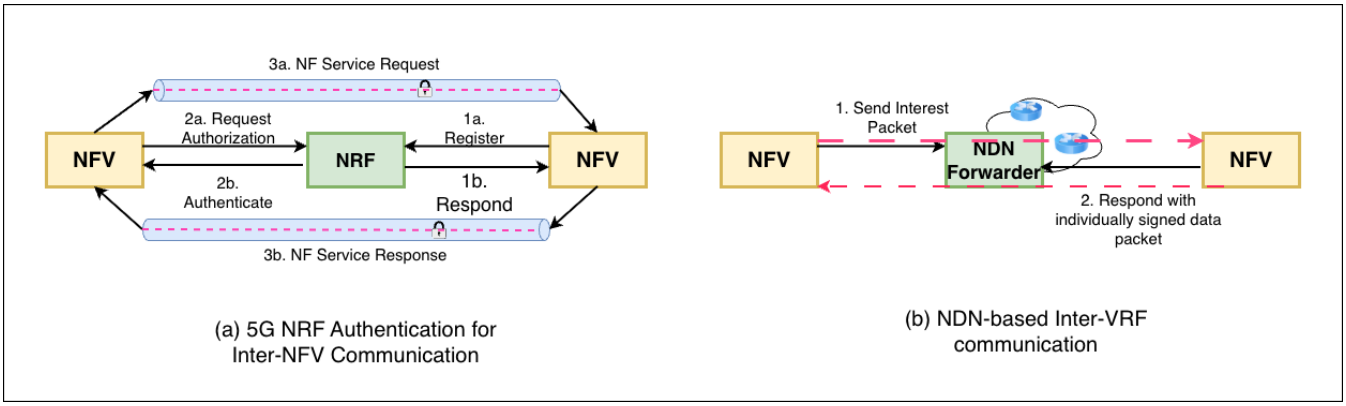


FIGURE 8. Service chaining in traditional vs NDN setup [213].

addressed. Also, though operators can configure custom network slices for their customers, large-scale geographic disruptions would still impact all slices equally [9].

D. CONTRIBUTIONS TO NETWORK RESILIENCE

The integration of terrestrial and non-terrestrial networks, intelligent network control, and advances in mobile core design enhance network resilience by enabling redundancy, isolation, improved monitoring, fault prediction, and proactive response.

The TN–NTN integration establishes alternative physical and virtual paths, thereby increasing path diversity. In the event of a terrestrial network outage caused by natural disasters or other disruptions, aerial platforms such as AAVs and HAPS can provide broad coverage and operate as access networks. In addition, space-based networks, including LEO and MEO constellations, can serve as backup backhaul solutions to reinforce or replace terrestrial infrastructure and maintain critical communications. This integrated approach strengthens the network's ability to absorb disruptions, adapt to degraded conditions, and respond to failures.

With AI- and ML-driven control, network anomalies can be detected and identified before they escalate into service disruptions. Such proactive identification reduces the time required for detection and response and helps prevent cascading failures that may otherwise lead to large-scale outages. Furthermore, dynamic and autonomous reconfiguration of network slices, routing paths, and resources can support adaptation during disruptions and reduce recovery time.

Innovation in mobile core design can reduce dependence on centralized components and address architectural limitations of existing core networks. Within the mobile core, NDN enables seamless failover among VNFs through in-network caching. By eliminating reliance on IP-based addressing, NDN allows any node with the requested content to respond to an Interest packet, thereby enabling a content-centric core architecture. In addition, edge-core splits allow selected core functions to be deployed at the edge. Such distributed edge-core architectures support localized operation when connectivity to centralized core components is impaired, thereby improving isolation and service continuity within the core.

When implemented together, these architectural and control innovations shift network resilience from static redundancy toward more autonomous, adaptive, and pervasive resilience.

VI. OPEN RESEARCH CHALLENGES

Despite adopting and implementing principles and technologies discussed in Section III, major outages still occur and are caused by insufficient operational preparedness, misconfiguration, or human errors. While the previously discussed technologies in Section V demonstrates considerable potential in building resilience in networks, there are substantial technical and operational challenges that are discussed in the following sections and need to be addressed. These challenges not only constrain broader adoption but also guide the direction of future research.

A. INTEGRATION

Integrating terrestrial and non-terrestrial networks introduces challenges at multiple levels. These arise not only within each individual infrastructure domain, including D2D, aerial, and space networks, but also across the vertical integration of these domains.

D2D networks face several challenges, including neighbour discovery, synchronization, security, and scalability under high UE density. These functions can also increase power consumption, introduce computational overhead, and generate signal interference [139], [221]. Recent studies have focused on addressing these limitations through distributed intelligence techniques, including Federated Learning (FL), Graph Neural Networks (GNNs), and Multi-Agent Reinforcement Learning (MARL) [222]. For example, Hosseinalipour et al. [223] propose an FL-based technique to reduce base station overhead, Noman et al. [224] propose an energy-optimization mechanism, and Qi et al. [225] propose an FL-enabled resource allocation scheme. Ioannou et al. [222] further propose a Belief-Desire-Intention-Extension (BDIx) framework. Unlike conventional AI- and ML-based

approaches, their framework aims to provide complete autonomy for D2D devices.

Similarly, aerial systems such as HAPS and AAVs face several key challenges, including platform instability, limited onboard energy, trajectory planning, and security. Under adverse weather conditions, these platforms may experience drift and instability, which can lead to jitter, footprint variation, and beam misalignment, thereby increasing the demand for high-capacity backhaul and corrective control mechanisms [143]. To mitigate the effects of HAPS instability, Chabbouh et al. [226] propose the use of AAVs as a backup network, where AAV positioning is determined based on the drift of the HAPS platform. Other recent studies have explored distributed AI- and ML-based techniques, such as reinforcement learning (RL), to compare HAPS position against ground reference beacons and compensate for positional variations [143]. Limited onboard energy, particularly for HAPS and AAV platforms, can also be supplemented through solar power. In addition, Yan et al. [227] model each AAV as an agent and propose a deep RL-based multi-agent framework to optimize system performance under energy constraints.

The high altitudes and orbital velocities of space-borne satellite networks introduce significant propagation delays, path loss, stale channel estimation, and frequency shifts due to Doppler effects [228]. Their continuous movement at high speed also necessitates frequent handovers [183] and makes synchronization challenging [123]. In LEO constellations, the handover burden is further aggravated by the highly dynamic topology and the large number of satellites [172]. As a result, a large number of simultaneous handovers within a short time interval may overload the network. Satellite systems are also exposed to harsh environmental conditions, including temperature fluctuations and solar activity. For example, elevated solar activity on June 1, 2025, reportedly led to an unusually high number of Starlink satellites re-entering Earth's atmosphere [229]. To address handover challenges, 3GPP TS 38.821 [183] proposes Conditional Handover (CHO), in which handover conditions are preconfigured by the network and the handover is triggered only when initiated by the UE. Juan et al. [230] note that although CHO can reduce handover failures to zero, it may increase the handover rate by 60%. In addition, 3GPP Release 17 proposes exploiting predictable satellite motion to improve handover preparation as an enhancement to CHO. Alongside standardization efforts, AI- and ML-based optimization techniques are also promising. For instance, Cao et al. [231] propose a UE-driven deep reinforcement learning mechanism for accessing non-terrestrial base stations (NT-BSs) in order to reduce frequent handovers and improve long-term throughput.

In addition to the challenges discussed above, the vertical integration of TN and NTN requires coordination across domains with distinct capabilities and constraints, including differences in energy requirements, availability, and resource limitations. For example, satellite networks exhibit a dynamic yet predictable topology with frequent handovers, aerial networks comprising HAPS and AAVs have a dynamic but less predictable topology [232], and terrestrial networks generally operate over a relatively static topology. This heterogeneity creates challenges for protocol interoperability, end-to-end resource management, seamless mobility, and security.

Conventional routing protocols such as OSPF are designed for terrestrial networks and are not well suited to environments with frequent topology changes, such as those caused by satellite handovers. Orbit Prediction Shortest Path First (OPSPF) is one example of an adaptive routing protocol for such scenarios [233]. OPSPF is a link-state protocol, similar to OSPF, that detects link changes and updates routing tables by exploiting the dynamic yet predictable topology of LEO satellite constellations. In addition, newer routing frameworks such as Dyna-STN [232] partition space and ground domains into service cubes and cells, which are managed by virtual nodes to form a stable virtual topology. Dyna-STN then applies terrestrial routing protocols, such as OSPF, to route traffic between these virtual nodes.

Research is also underway to address cross-layer resource management, particularly because 5G and beyond services such as Ultra-Reliable Low-Latency Communication (URLLC) and enhanced Mobile Broadband (eMBB) require reliable and consistent resource allocation. Through network slicing, operators can create virtual networks tailored to specific bandwidth, latency, and reliability requirements, thereby supporting the service guarantees expected for URLLC and eMBB. However, latency, topology, and bandwidth vary significantly across terrestrial and non-terrestrial networks, making the provisioning of end-to-end network slices across multiple domains particularly challenging. Taleb et al. [234] note that a multi-domain network slice must be supported by coordinated underlying physical and virtual infrastructure. To address this, they propose a network slice management and orchestration architecture that incorporates SDN and NFV. Similarly, Pan et al. [235] propose a Graph Attention Network (GAT)-based Deep Reinforcement Learning (DRL) mechanism for dynamically allocating network resources to network slices. Their proposed algorithm outperforms several baseline ML approaches, including DQN.

When non-terrestrial networks operate as access networks, UEs must select between terrestrial and non-terrestrial connectivity, which necessitates handover mechanisms for transitions across coverage types. Such transitions are challenging because of differences in latency, bandwidth, coverage, and energy constraints, all of which can affect communication continuity and Quality of Service (QoS) guarantees. Mohamed et al. [236] identify several approaches to address these challenges, including SDN-enabled centralized control and resource allocation, support for UEs maintaining multiple simultaneous connections, the use of context-aware protocols, and predictive AI- and ML-based algorithms to anticipate satellite motion, user mobility, and AAV trajectories in order to prepare for handovers.

B. SECURITY

Alongside the development of end-to-end protocols and control mechanisms, ensuring end-to-end security is equally crucial. This is particularly challenging in integrated terrestrial and non-terrestrial networks because security mechanisms must operate across domains with different latency, mobility, and resource characteristics. For example, terrestrial transport protocols such as TCP are intolerant to large delays and may incorrectly interpret delay as congestion. Since non-terrestrial networks inherently experience long propagation delays, TCP Performance Enhancing Proxies (PEPs) are often used to split long flows into shorter segments and improve TCP performance. However, terrestrial security protocols such as IPsec can conflict with PEP operation, making conventional end-to-end protection difficult to maintain. To address this issue, Djeddai and Liu [237] propose applying IPsec between the UE and the PEP at the ground station, while maintaining a mapping between the original TCP header and the corresponding IPsec header.

In addition to transport-layer challenges, each network segment is exposed to distinct security threats. Terrestrial components, such as D2D networks, are vulnerable to attacks including address spoofing, eavesdropping, packet sniffing, and masquerading [238]. Aerial systems such as AAVs are susceptible to spoofing, wireless intrusions, and physical hardware attacks [239]. Satellite communications are similarly exposed to signal interception, spoofing, jamming, and eavesdropping, while frequent handovers over inter-satellite links and terrestrial gateways create additional challenges for maintaining secure and seamless connectivity [124]. Other security concerns include insecure routing, insecure handover procedures, and weak key management [240], as well as man-in-the-middle, TCP-level, and penetration attacks [241].

Alongside 3GPP efforts to secure terrestrial and non-terrestrial communications, the research community has proposed a range of mechanisms to address these issues. For example, Eiza et al. [242] propose an SDN-based architecture for secure and QoS-aware routing in integrated terrestrial and non-terrestrial networks. Ren et al. [243] propose a password-based authenticated key exchange model for LEO constellations. Xinhang et al. [244] further exploit the predictability of satellite motion to propose an SDN-based handover mechanism that pre-authenticates users and transfers security context based on the satellite trajectory.

C. COST

Building network redundancy requires additional enterprise-grade infrastructure, which can substantially increase capital expenditure (CapEx). These financial constraints have proven prohibitive even for well-funded initiatives. For example, Project Loon [245], despite its potential to provide balloon-based Internet services, was discontinued because of mounting infrastructure-related costs. Similarly, LEO satellite networks, although capable of supporting global communications, are also subject to significant economic constraints. Such systems require large-scale constellations to maintain persistent coverage. Given that LEO satellites typically have an operational lifespan of around five years [246], satellite replenishment over time, ground-station maintenance, and launch infrastructure can together result in costs amounting to billions of dollars.

This expanded infrastructure also increases operational expenditure (OpEx), as it must be configured, managed, and maintained by skilled personnel. In addition, larger number of devices increases system complexity and amplifies the risk of misconfiguration, which can itself lead to outages and thereby partially undermine the resilience benefits expected from the added redundancy.

D. AI AND ML INTEGRATION

The integration of AI and ML can enable Zero-Touch Management and self-healing networks. However, the practical realization of these capabilities remains challenging. Cui et al. [247] highlight the reliability and stability limitations of AI models when exposed to extreme variations in input signals, which are relatively common in communication networks due to factors such as public events (e.g., concerts) or security attacks. Kourouklidis et al. [248] propose a model-driven engineering approach to detect and respond to events that degrade the performance of ML algorithms. Similarly, Pu et al. [249] study the robustness of link prediction under network attacks. Despite this progress, the practical deployment of AI and ML remains hindered by challenges related to real-time analytics, data privacy, model transparency, and high computational requirements. Troubleshooting complex AI models in live networks also remains an open research challenge. In response, 3GPP TS 28.105 [250] specifies requirements for model correctness verification, bias reporting, and anomaly detection, while TS 38.331 [251] includes provisions related to model activation, rollback, and model integrity verification. Finally, limited understanding of the internal behavior of AI models may reduce engineers' trust or, conversely, encourage over-reliance on automated decisions.

E. CONFIGURATION COMPLEXITY

5G and 6G cores are microservice-based architectures. Configuring resources, security, and quality of service to provision virtual network functions and network slices for different services (e.g., URLLC or mMTC) increases the management overhead [252].

Future networks will further integrate AI and ML, further increasing configuration complexity. They would require frequent training and configuration updates to adapt continuously to evolving traffic patterns. While such updates are essential for enabling proactive self-healing and maintaining quality of service, they are also challenging to verify and troubleshoot. Though automated tools such as BatFish [103] can assist, network personnel must be adequately trained and supported with up-to-date documentation to resolve issues effectively.

VII. CONCLUSION

All five frameworks surveyed in this paper namely, NIST CSF, Resilient-by-Design, MAPE-K, A3RT, and ResiliNets exhibit a common operational lifecycle consisting of anticipate or prepare, resist and absorb, respond and adapt, and repair and recover, despite differences in terminology and application domains. This convergence reflects the fundamental system capabilities required to build a resilient network.

Resilience emerges from the coordinated interaction of technological enablers such as redundancy, isolation, configuration management, fault diagnosis, and intelligent design. Physical redundancy without configuration consistency may not prevent failures, as demonstrated by several large-scale outages, including AT&T (2024) [88], Optus (2023) [3], and KDDI (2022) [89]. Similarly, advanced monitoring capabilities without corresponding isolation mechanisms may enable earlier fault detection, but they cannot by themselves prevent cascading failures. Likewise, intelligent self-healing requires both sound architectural foundations and correctly maintained configuration baselines. Therefore, network operators should invest in cross-functional alignment across infrastructure, configuration management, security, monitoring, and AI/ML operations, rather than relying on siloed technology initiatives.

Effective resilience management also requires robust metrics. Existing KPIs serve only as proxy measures of resilience; they are not standardized, remain context-dependent, and cannot capture end-to-end resilience across heterogeneous networks. This lack of standard metrics prevents telecom operators from objectively comparing resilience strategies, grounding service-level agreements, and performing cross-domain resilience verification. Establishing a unified telecom-specific resilience measurement framework therefore remains an important research challenge.

The evolution toward integrated and intelligent next-generation architectures introduces both opportunities and challenges. The integration of terrestrial and non-terrestrial networks offers genuine path diversity, multi-path redundancy, and geographic diversity that terrestrial networks alone cannot provide. However, cross-layer synchronization, handover management, protocol interoperability, and broader cross-domain coordination remain significant challenges requiring further research. Moreover, technical feasibility does not guarantee operational viability, as illustrated by the discontinuation of Project Loon [155]. Advancing TN/NTN integration therefore requires coordinated progress in cross-layer control, dynamic scheduling, and ML-driven adaptation, alongside continued standardization efforts and novel cost-sharing models.

Ultimately, true network resilience will be measured not only by how well systems perform under normal conditions, but by their ability to sustain life-saving communication when it matters most.

REFERENCES

[1] *Digital 2025: Global Overview Report*. Accessed: Aug. 12, 2025. [Online]. Available: https://datareportal.com/reports/digital-2025-global-overview-report

[2] Google. *Sharing Details on a Recent Incident Impacting One of Our Customers*. Accessed: Jul. 22, 2025. [Online]. Available: https://cloud.google.com/blog/products/infrastructure/details-of-google-cloud-gcve-incident

[3] *Chapter 2-The Optus Network Outage*. Accessed: Jul. 22, 2025. [Online]. Available: https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Environment_and_Communications/OptusNetworkOutage/Report/Chapter_2_-_The_Optus_network_outage

[4] B. H. R. Brito and J. Wilson. (2025). [Online]. Available: https://apnews.com/article/spain-portugal-power-outage-electricity-b0c5fbca49b8422248c4f933e20303b3

[5] (2020). *About Hexa-X*. Accessed: Jul. 22, 2025. [Online]. Available: https://5g-ppp.eu/hexa-x/

[6] (2025). *European Level 6G Flagship Project*. [Online]. Available: https://hexa-x-ii.eu/vision/

[7] EU. (2022). *PhoenixIIX*. Accessed: Jul. 22, 2025. [Online]. Available: https://phoeni2x.eu/project/objectives/

[8] (2025). *How Does 5G Enhance Mission-Critical Communication*. [Online]. Available: https://publicsafety.ieee.org/topics/how-does-5g-enhance-mission-critical-communication/#:~:text=The%20arrival%20of%205G%20networks,ultimately%20save%20lives%20during%20emergencies

[9] D. Tipper, A. Babay, B. Palanisamy, and P. Krishnamurthy, "Network connectivity resilience in next generation backhaul networks: Challenges and future opportunities," *IEEE Trans. Netw. Service Manage.*, vol. 21, pp. 5321–5334, 2024.

[10] A. D. S. Batista and A. L. Dos Santos, "A survey on resilience in information sharing on networks: Taxonomy and applied techniques," *ACM Comput. Surveys*, vol. 56, no. 12, pp. 1–36, Dec. 2024.

[11] T. Massimo et al., "A survey of network resiliency methodologies against weather-based disruptions," in *Proc. 8th Int. Workshop Resilient Netw. Des. Model. (RNDM)*, Sep. 2016, pp. 1–9.

[12] R. Owen, A. Bryant, L. Finch, D. R. Franklin, M. Abdollahi, and M. Abolhasan, "Resilience in the IP era: Navigating the fragility of modern telecommunications networks: The sovereign functions," *Authorea Preprints*, vol. 13, pp. 155759–155777, Jul. 2025.

[13] A. Grigorjew, S. Geißler, P. Diederich, T. Hoßfeld, and W. Kellerer, "Resilience in time-sensitive networking: An overview and open research directions," in *Proc. 13th Int. Workshop Resilient Netw. Design Model. (RNDM)*, Sep. 2023, pp. 1–8.

[14] P. Vlacheas, V. Stavroulaki, P. Demestichas, S. Cadzow, D. Ikonomou, and S. Gorniak, "Towards end-to-end network resilience," *Int. J. Crit. Infrastructure Protection*, vol. 6, nos. 3–4, pp. 159–178, Dec. 2013.

[15] Task Group. (2025). *Time-Sensitive Networking (TSN) Task Group*. [Online]. Available: https://1.ieee802.org/tsn/

[16] P. Steinberg, J. Peterson, M. Ennis, F. Gabbard, and R. Owen, "A resilience framework for telecommunications networks: Methodology, assessment, and best practices," Tech. Rep. [Online]. Available: https://img1.wsimg.com/blobby/go/90526c83-8429-464d-8025-a3ba5a28a84f/resilience%20framework%20v5.pdf

[17] European Union Agency for Cybersecurity (ENISA). (2025). *Getting the Right Concept By Using the Right Words: Obtaining a Common Glossary for Resilience*. [Online]. Available: https://www.enisa.europa.eu/news/enisa-news/getting-the-right-concept-by-using-the-right-words-ontology-taxonomies-for-critical-infrastructures

[18] (2021). *National Institute of Standards and Technology (NIST)*. [Online]. Available: https://csrc.nist.rip/glossary/term/resilience

[19] (2025). *Cybersecurity and Infrastructure Security Agency*. [Online]. Available: https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/resilience-services

[20] *ETSI EMTEL (European Telecommunications Standards Institute, Emergency Telecommunications)*, document TR 102 445 V1.2.1, Apr. 2023. [Online]. Available: https://www.etsi.org/deliver/etsi_tr/102400_102499/102445/01.02.01_60/tr_102445v010201p.pdf

[21] International Telecommunication Union (ITU). (Dec. 2019). *ITU-T Recommendation E.102 (12/2019): Terms and Definitions for Disaster Relief Systems, Network Resilience and Recovery*. [Online]. Available: https://www.itu.int/rec/T-REC-E.102-201912-I

[22] P. Smith et al., "Network resilience: A systematic approach," *IEEE Commun. Mag.*, vol. 49, no. 7, pp. 88–97, Jul. 2011.

[23] NIST. (2025). *The NIST Cybersecurity Framework (CSF) 2.0*. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

[24] N. Huda Mahmood, S. Samarakoon, P. Porambage, M. Bennis, and M. Latva-aho, "Resilient-by-design: A resiliency framework for future wireless networks," 2024, *arXiv:2410.23203*.

[25] A. Ismaili-Aoui, E. Zimmermann, Y. Liu, G. Demesure, and H. Bril el Haouzi, "Towards a digital twin architecture based on mape-k framework and holonic paradigm: Application to an emergency department and smart manufacturing cases studies," in *Proc. Int. Workshop Service Oriented, Holonic Multi-Agent Manuf. Syst. Ind. Future*. Cham, Switzerland: Springer, 2024, pp. 373–384.

[26] R.-J. Reifert et al., "Toward resilience in mixed critical industrial control systems: A multi-disciplinary view," *IEEE Access*, vol. 10, pp. 124563–124581, 2022.

[27] M. Camelo et al., "DAEMON: A network intelligence plane for 6G networks," in *Proc. IEEE Globecom Workshops (GC Wkshps)*, Dec. 2022, pp. 1341–1346.

[28] R.-J. Reifert, Y. Karacora, C. Chaccour, A. Sezgin, and W. Saad, "Resilience and criticality: Brothers in arms for 6G," 2024, *arXiv:2412.03661*.

[29] D. Hutchison and J. P. G. Sterbenz, "Architecture and design for resilient networked systems," *Comput. Commun.*, vol. 131, pp. 13–21, Oct. 2018.

[30] A. G. Malis, X. Geng, M. Chen, B. Varga, and C. J. Bernardos. (2025). *A Framework for Deterministic Networking (DetNet) Controller Plane*. [Online]. Available: https://datatracker.ietf.org/doc/draft-ietf-detnet-controller-plane-framework/

[31] C. Poulin and M. B. Kane, "Infrastructure resilience curves: Performance measures and summary metrics," *Rel. Eng. Syst. Saf.*, vol. 216, Dec. 2021, Art. no. 107926.

[32] D. Harrington, B. Wijnen, and R. Presuhn, *An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks*, document RFC 3411, Dec. 2002. [Online]. Available: https://www.rfc-editor.org/info/rfc3411

[33] S. Waldbusser, *Remote Network Monitoring Management Information Base Version 2*, document RFC 4502, May 2006. [Online]. Available: https://www.rfc-editor.org/info/rfc4502

[34] P. Aitken, B. Claise, and B. Trammell, *Specification of the IP Flow Information Export (IPFIX) Protocol for the Exchange of Flow Information*, document RFC 7011, Sep. 2013. [Online]. Available: https://www.rfc-editor.org/info/rfc7011

[35] D. Soldani et al., "EBPF: A new approach to cloud-native observability, networking and security for current (5G) and future mobile networks (6G and Beyond)," *IEEE Access*, vol. 11, pp. 57174–57202, 2023.

[36] J. Shen et al., "Network-centric distributed tracing with DeepFlow: Troubleshooting your microservices in zero code," in *Proc. ACM SIGCOMM 2023 Conf.*, 2023, pp. 420–437.

[37] B. Li et al., "Enjoy your observability: An industrial survey of microservice tracing and analysis," *Empirical Softw. Eng.*, vol. 27, no. 1, Jan. 2022.

[38] *Distributed Tracing*. Accessed: Jul. 22, 2025. [Online]. Available: https://learn.microsoft.com/en-us/azure/private-5g-core/distributed-tracing

[39] T. Pierce, J. Schanck, A. Groeger, R. Salih, and M. R. Clark, "Chaos engineering experiments in middleware systems using targeted network degradation and automatic fault injection," *Proc. SPIE*, vol. 11753, Apr. 2021, Art. no. 117530A.

[40] (2022). *Mininet*. Accessed: Jul. 22, 2025. [Online]. Available: https://mininet.org

[41] *GNS3 -The Software That Empowers Network Professionals*. Accessed: Jul. 22, 2025. [Online]. Available: https://www.gns3.com

[42] F. Poltronieri, M. Tortonesi, and C. Stefanelli, "A chaos engineering approach for improving the resiliency of IT services configurations," in *Proc. IEEE/IFIP Netw. Oper. Manage. Symp. (NOMS)*, Budapest, Hungary, Apr. 2022, pp. 1–6.

[43] M. Attaran and B. G. Celik, "Digital twin: Benefits, use cases, challenges, and opportunities," *Decis. Analytics J.*, vol. 6, Mar. 2023, Art. no. 100165. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S277266222300005X

[44] M. Singh, E. Fuenmayor, E. Hinchy, Y. Qiao, N. Murray, and D. Devine, "Digital twin: Origin to future," *Appl. Syst. Innov.*, vol. 4, no. 2, p. 36, May 2021.

[45] M. Abbasi, A. Shahraki, and A. Taherkordi, "Deep learning for network traffic monitoring and analysis (NTMA): A survey," *Comput. Commun.*, vol. 170, pp. 19–41, Mar. 2021.

[46] J. Shi, Z. Zhang, K. Chakrabarty, and X. Gu, "Failure prediction based on anomaly detection for complex core routers," in *Proc. IEEE/ACM Int. Conf. Comput.-Aided Des. (ICCAD)*, San Diego, CA, USA, 2018, pp. 1–6.

[47] M. A. Islam, H. Siddique, W. Zhang, and I. Haque, "A deep neural network-based communication failure prediction scheme in 5G RAN," *IEEE Trans. Netw. Service Manage.*, vol. 20, no. 2, pp. 1140–1152, Jun. 2023.

[48] S. Hochreiter and J. Schmidhuber, "Long short-term memory," *Neural Comput.*, vol. 9, no. 8, pp. 1735–1780, Nov. 1997.

[49] J. S. Camargo et al., "Dynamic slicing reconfiguration for virtualized 5G networks using ML forecasting of computing capacity," *Comput. Netw.*, vol. 236, Nov. 2023, Art. no. 110001.

[50] (2026). *OPENVAS SCAN: Managing Security Information*. [Online]. Available: https://docs.greenbone.net/GSM-Manual/gos-24.10/en/managing-secinfo.html

[51] (2026). *Nessus 10.11 User Guide*. [Online]. Available: https://docs.tenable.com/nessus/Content/PDF/Nessus_10_11.pdf

[52] (2026). *National Institute of Standards and Technology (NIST)*. [Online]. Available: https://nvd.nist.gov/

[53] *Reducing the Significant Risk of Known Exploited Vulnerabilities*. Accessed: Aug. 12, 2025. [Online]. Available: https://www.cisa.gov/known-exploited-vulnerabilities

[54] K. Zenitani, "Attack graph analysis: An explanatory guide," *Comput. Secur.*, vol. 126, Mar. 2023, Art. no. 103081.

[55] B. Kordy, L. Piètre-Cambacédès, and P. Schweitzer, "DAG-based attack and defense modeling: Don't miss the forest for the attack trees," *Comput. Sci. Rev.*, vols. 13–14, pp. 1–38, Nov. 2014.

[56] K. Durkota, V. Lisý, B. Bošanský, C. Kiekintveld, and M. Pěchouček, "Hardening networks against strategic attackers using attack graph games," *Comput. Secur.*, vol. 87, Nov. 2019, Art. no. 101578.

[57] N. Feamster and H. Balakrishnan. *Detecting BGP Configuration Faults With Static Analysis*. [Online]. Available: http://nms.csail.mit.edu/rcc/

[58] A. Tang et al., "Campion: Debugging router configuration differences," in *Proc. ACM SIGCOMM Conf.*, Aug. 2021, pp. 748–761.

[59] D. Thankachan. (2023). *Network Redundancy Vs Diversity: Building a Resilient Network for Maximum Uptime*. [Online]. Available: https://lightyear.ai/blogs/guide-to-building-redundant-and-diverse-internet-connectivity

[60] D. Muznikas. (2025). *In-Service Upgrades for Telco 5G Cloud-Native Core CaaS Infrastructure With No Service Disruption*. [Online]. Available: https://www.redhat.com/en/blog/service-upgrades-telco-5g-cloud-native-core-caas-infrastructure-no-service-disruption#

[61] (2026). *Link Aggregation Control Protocol(LACP)(802.3ad) for Gigabit Interfaces*. [Online]. Available: https://www.cisco.com/c/en/us/td/docs/ios/12_2sb/feature/guide/gigeth.html

[62] J. Qiu, Y. Liu, G. Mohan, and K. C. Chua, "Fast spanning tree reconnection mechanism for resilient metro Ethernet networks," *Comput. Netw.*, vol. 55, no. 12, pp. 2717–2729, Aug. 2011.

[63] (2023). *Understanding Rapid Spanning Tree Protocol(802.1w)*. [Online]. Available: https://www.cisco.com/c/en/us/support/docs/lan-switching/spanning-tree-protocol/24062-146.html

[64] J. Moy. (2025). *OSPF V2*. [Online]. Available: https://www.ietf.org/rfc/rfc2328.txt

[65] R. Callon. (2025). [Online]. Available: https://datatracker.ietf.org/doc/html/rfc1195

[66] A. D. Acee Lindem. (2024). *Virtual Router Redundancy Protocol*. Accessed: 2025-08-08. [Online]. Available: https://www.rfc-editor.org/rfc/rfc9568

[67] (2025). *Evolution of IP Fast-Reroute Stratergies*. [Online]. Available: https://home.agh.edu.pl/~andrzejk/pub/2018_rndm_ipfrr.pdf

[68] S. Nelakuditi, S. Lee, Y. Yu, and Z.-L. Zhang, "Failure insensitive routing for ensuring service availability," in *Proc. 11th Int. Conf. Quality Service*, 2003, pp. 287–304.

[69] P. P. A. Atlas and G. Swallow. *Fast Reroute Extensions To RSVP-TE for LSP Tunnels*. Accessed: Aug. 12, 2025. [Online]. Available: https://datatracker.ietf.org/doc/html/rfc4090

[70] M. Chiesa, A. Kamisinski, J. Rak, G. Rétvári, and S. Schmid, "A survey of fast-recovery mechanisms in packet-switched networks," *IEEE Commun. Surveys Tuts.*, vol. 23, no. 2, pp. 1253–1301, 2nd Quart., Feb. 2021.

[71] L. Xihan. (2025). *What Is NSR*. [Online]. Available: https://info.support.huawei.com/info-finder/encyclopedia/en/NSR.html

[72] (2025). *Chapter: Configuring Nonstop Forwarding*. [Online]. Available: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ha/configuration/xe-16/ha-xe-16-book/ha-config-nonstop-forwarding.html

[73] (2025). *Nonstop Forwarding*. [Online]. Available: https://infocenter.nokia.com/public/7750SR227R1A/index.jsp?topic=%2Fcom.nokia.Basic_System_Configuration_Guide%2Fnonstop_forward-ai9emdyolr.html

[74] S. Varadarajan. (2025). *Virtual Local Area Networks*. [Online]. Available: https://www.cse.wustl.edu/

[75] Y. Rekhter, S. Hares, and T. Li. *A Border Gateway Protocol 4 (BGP-4)*. Accessed: Jul. 22, 2025. [Online]. Available: https://datatracker.ietf.org/doc/html/rfc4271

[76] *BGP Confederations*. Accessed: Jul. 22, 2025. [Online]. Available: https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-networking-admin/bgp/bgp-confederations

[77] *Routing Policies for BGP Communities*. Accessed: Jul. 22, 2025. [Online]. Available: https://www.juniper.net/documentation/us/en/software/junos/bgp/topics/topic-map/routing-policies-communities.html

[78] Y. Rekhter and E. C. Rosen. (2025). *BGP/MPLS IP Virtual Private Networks*. [Online]. Available: https://datatracker.ietf.org/doc/html/rfc4364#section-3

[79] *Selective Virtual Routing and Forwarding Table Download: A Solution To Increase Layer3 VPN Scale*, Cisco, San Jose, CA, USA, 2011.

[80] (Jul. 2001). *Overlay Networks*. [Online]. Available: https://book.systemsapproach.org/applications/overlays.html

[81] D. M. D. Farinacci, S. P. Hanks, and P. S. Traina. *Generic Routing Encapsulation*. Accessed: Aug. 12, 2025. [Online]. Available: https://datatracker.ietf.org/doc/html/rfc2784

[82] M. Mahalingam et al. *Virtual EXtensible Local Area Network (VXLAN): A Framework for Overlaying Virtualized Layer 2 Networks Over Layer 3 Networks*. Accessed: Jul. 22, 2025. [Online]. Available: https://datatracker.ietf.org/doc/html/rfc7348

[83] P. Garg and Y.-S. Wang. *NVGRE: Network Virtualization Using Generic Routing Encapsulation*. Accessed: Jul. 22, 2025. [Online]. Available: https://www.rfc-editor.org/info/rfc7637

[84] J. Rabadan, K. Nagaraj, W. Lin, and A. Sajassi. *BGP EVPN Multihoming Extensions for Split-Horizon Filtering*. Accessed: Jul. 22, 2025. [Online]. Available: https://www.rfc-editor.org/rfc/rfc9746

[85] (2025). *GPRS Tunnelling Protocol for User Plane (GTPv1-U) (3GPP TS 29.281 Version 8.0.0 Release 8)*. [Online]. Available: https://www.etsi.org/deliver/etsi_ts/129200_129299/129281/08.00.00_60/ts_129281v080000p.pdf

[86] ExtremeNetworks. (2026). *ACL-based Rate Limiting Use Cases*. [Online]. Available: https://documentation.extremenetworks.com/Extreme%20SLX-OS%2020.7.2%20QoS%20and%20Traffic%20Mgmt%20Guide/DatacenterNetworking/extreme_slx_os_qos_and_traffic_mgmt_guide/acl_based_rate_limiting_use_cases_slxc.shtml

[87] *Implementing Network Segmentation and Segregation*. Accessed: Aug. 12, 2025. [Online]. Available: https://www.cyber.gov.au/resources-business-and-government/maintaining-devices-and-systems/system-hardening-and-administration/network-hardening/implementing-network-segmentation-and-segregation

[88] (2025). *AT&T Mobility Network Outage REPORT AND FINDINGS*. [Online]. Available: https://docs.fcc.gov/public/attachments/DOC-404150A1.pdf

[89] (2022). *The July 2 Communication Failure and Our Response*. [Online]. Available: https://www.kddi.com/english/important-news/20220729_01/

[90] (2020). *Jun. 15, 2020 T-Mobile Network Outage Report*. Accessed: Jul. 22, 2025. [Online]. Available: https://docs.fcc.gov/public/attachments/DOC-367699A1.pdf

[91] (2026). *The Secure Shell (SSH) Transport Layer Protocol*. [Online]. Available: https://www.rfc-editor.org/info/rfc4253

[92] E. Rescorla. (2018). *The Transport Layer Security (TLS) Protocol Version 1.3*. [Online]. Available: https://www.rfc-editor.org/info/rfc8446

[93] K. Seo and S. Kent. (2005). *Security Architecture for the Internet Protocol*. [Online]. Available: https://www.rfc-editor.org/info/rfc4301

[94] *Single Source of Truth in Network Automation White Paper*. Accessed: Jul. 22, 2025. [Online]. Available: https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/technology-perspectives/ssot-nw-automation-wp.html

[95] *Getting Started With Ansible*. Accessed: Jul. 22, 2025. [Online]. Available: https://docs.ansible.com/ansible/latest/getting_started/index.html

[96] A. Farrel. (2024). *Overview and Principles of Internet Traffic Engineering*. [Online]. Available: https://www.rfc-editor.org/info/rfc9522

[97] A. Bashandy, S. Litkowski, C. Filsfils, P. Francois, B. Decraene, and D. Voyer. (2025). *Topology Independent Fast Reroute Using Segment Routing*. [Online]. Available: https://www.rfc-editor.org/info/rfc9855

[98] X. Wang, Y. Zhao, H. Xiao, X. Wang, and X. Chi, "LTmatch: A method to abstract pattern from unstructured log," *Appl. Sci.*, vol. 11, no. 11, p. 5302, Jun. 2021.

[99] S. Kobayashi, K. Otomo, and K. Fukuda, "Causal analysis of network logs with layered protocols and topology knowledge," in *Proc. 15th Int. Conf. Netw. Service Manage. (CNSM)*, Halifax, NS, Canada, 2019, pp. 1–9.

[100] Y. Liu, N. Foster, and F. B. Schneider, "Causal network telemetry," in *Proc. 5th Int. Workshop P4 Eur.*, Dec. 2022, pp. 46–52.

[101] R. Vaarandi, B. Blumbergs, and E. Çaliskan, "Simple event correlator–best practices for creating scalable configurations," in *Proc. IEEE Int. Multi-Disciplinary Conf. Cognit. Methods Situation Awareness Decis.*, Mar. 2015, pp. 96–100.

[102] A. Fogel, S. Fung, L. Pedrosa, R. Govindan, and T. Millstein, "A general approach to network configuration analysis," in *Proc. USENIX*, 2015, pp. 469–483.

[103] M. R. Jaya Srikanth. (2018). *BatFish*. Accessed: Jul. 22, 2025. [Online]. Available: https://batfish.org

[104] H. Zeng et al., "Libra: Divide and conquer to verify forwarding tables in huge networks," in *Proc. 11th USENIX Symp. Networked Syst. Design Implement.*, 2014, p. 546.

[105] *Network Functions Virtualisation (NFV)*. Accessed: Aug. 12, 2025. [Online]. Available: https://www.etsi.org/technologies/nfv

[106] (2020). *Performing Out-of-Band Network Management*. [Online]. Available: https://media.defense.gov/2020/Sep/17/2002499616/-1/-1/0/PERFORMING_OUT_OF_BAND_NETWORK_MANAGEMENT20200911.PDF

[107] D. J. Bodeau and R. Graubart, "Cyber Resiliency Engineering Framework," MITRE Corp., Bedford, MA, USA, Tech. Rep. MTR110237, 2011.

[108] R. Ross, V. Pillitteri, R. Graubart, D. Bodeau, and R. McQuaid. (2021). *Developing Cyber-Resilient Systems: S Security Engineering Approach*. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v2r1.pdf

[109] D. J. Bodeau, R. D. Graubart, and E. R. Laderman, "Cyber resiliency engineering overview of the architectural assessment process," *Proc. Comput. Sci.*, vol. 28, pp. 838–847, 2014.

[110] S. Secgin, *Evolution of Wireless Communication Ecosystems*. Hoboken, NJ, USA: Wiley, 2023.

[111] *Network Functions Virtualisation (NFV); Reliability; Report on Models and Features for end-to-end Reliability*. Accessed: Jul. 30, 2025. [Online]. Available: https://www.etsi.org/deliver/etsi_gs/NFV-REL/001_099/003/01.01.01_60/gs_nfv-rel003v010101p.pdf

[112] D. J. Smith, *Reliability, Maintainability and Risk - Practical Methods for Engineers*, 10th ed., Amsterdam, The Netherlands: Elsevier, 2022.

[113] E. Bauer, X. Zhang, and D. A. Kimber, *Practical System Reliability*. Piscataway, NJ, USA: IEEE Press, 2009.

[114] (2024). *Top Metrics That Every Data Engineer Should Use*. [Online]. Available: https://herovired.com/learning-hub/blogs/top-metrics-that-every-data-engineer-should-use/

[115] M. Rodrigues. (2025). *Incident Management for High-velocity Teams*. [Online]. Available: https://www.logicmonitor.com/blog/whats-the-difference-between-mttr-mttd-mttf-and-mtbf#h-what-is-mttk

[116] Information Technology ? Information Security Incident Management Part 1: Principles and Process, Standard ISO/IEC 27035-1:2023, 2016. [Online]. Available: https://www.iso.org/standard/78973.html

[117] (2025). *SLA Adherence*. [Online]. Available: https://www.ibm.com/think/topics/sla-metrics

[118] R. Wyrzykowski. *The Opensignal Global Reliability Experience Report*. Accessed: Jul. 30, 2025. [Online]. Available: https://www.opensignal.com/2024/02/08/the-opensignal-global-reliability-experience-report

[119] *5G Management and Orchestration 5G Performance Measurements*. Accessed: Jul. 30, 2025. [Online]. Available: https://www.etsi.org/deliver/etsi_ts/128500_128599/128552/16.09.00_60/ts_128552v160900p.pdf

[120] *VoNR Call Setup Time ? 5G Performance Analysis*. Accessed: Jul. 30, 2025. [Online]. Available: https://www.techplayon.com/5g-vonr-call-setup-time/

[121] *Enhancing the Resilience of Communication Networks*. Accessed: Aug. 12, 2025. [Online]. Available: https://www.oecd.org/content/dam/oecd/en/publications/reports/2025/05/enhancing-the-resilience-of-communication-networks_a47d78a1/d6920477-en.pdf

[122] S. A. Chamkar, Y. Maleh, and N. Gherabi, "The human factor capabilities in security operation center (SOC)," *EDPACS*, vol. 66, no. 1, pp. 1–14, Jul. 2022.

[123] M. A. Jamshed and A. Nauman, *Integrated Terrestrial and Non- Terrestrial Network*. Cham, Switzerland: Springer, 2025.

[124] X. Zhu and C. Jiang, "Integrated satellite-terrestrial networks toward 6G: Architectures, applications, and challenges," *IEEE Internet Things J.*, vol. 9, no. 1, pp. 437–461, Jan. 2022.

[125] H. Jiao et al., "Use case analysis and architecture design for 5G emergency communications," in *Proc. Signal Inf. Process., Netw. Comput.*, 2022, pp. 108–119.

[126] 3GPP. (2025). *Study on Further Enhancements To LTE Device To Device (D2D), UE To Network Relays for Internet of Things (IoT) and Wearable*. [Online]. Available: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3110

[127] *IMS Profile for Voice, Video and SMS Over Untrusted Wi-Fi Access*. Accessed: Jul. 30, 2025. [Online]. Available: https://www.gsma.com/newsroom/wp-content/uploads//IR.51-v8.0-2.pdf

[128] *TS.63 UE Wi-Fi Calling Requirements Specification*. Accessed: Jul. 30, 2025. [Online]. Available: https://www.gsma.com/get-involved/working-groups/gsma_resources/ts-63-v1-0-ue-wi-fi-calling-requirements-specification/

[129] A. Förster et al., "A beginner's guide to infrastructure-less networking concepts," *IET Netw.*, vol. 13, no. 1, pp. 66–110, Jan. 2024. [Online]. Available: https://ietresearch.onlinelibrary.wiley.com/doi/abs/10.1049/ntw2.12094

[130] D. Johnson, Y. Hu, and D. Maltz. (2007). *The Dynamic Source Routing Protocol (DSR) for Mobile Ad Hoc Networks for IPv4*. Accessed: Jul. 30, 2025. [Online]. Available: https://www.rfc-editor.org/info/rfc4728

[131] S. R. Das, C. E. Perkins, and E. M. Belding-Royer. (2007). *Ad Hoc On-Demand Distance Vector (AODV) Routing*. [Online]. Available: https://www.rfc-editor.org/info/rfc3561

[132] V. Basnayake, H. Mabed, D. N. K. Jayakody, P. Canalda, and M. Beko, "Adaptive emergency call service for disaster management," *J. Sensor Actuator Netw.*, vol. 11, no. 4, p. 83, Nov. 2022.

[133] A. Thomas and G. Raja, "FINDER: A D2D based critical communications framework for disaster management in 5G," *Peer-Peer Netw. Appl.*, vol. 12, no. 4, pp. 912–923, Jul. 2019.

[134] Q. T. Minh, K. Nguyen, and S. Yamada, "DRANs: Resilient disaster recovery access networks," in *Proc. IEEE 37th Annu. Comput. Softw. Appl. Conf. Workshops*, Jul. 2013, pp. 754–759.

[135] D. Quercia and S. Hailes, "Sybil attacks against mobile users: Friends and foes to the rescue," in *Proc. IEEE INFOCOM*, Mar. 2010, pp. 1–5.

[136] M. Pozza, A. Rao, H. Flinck, and S. Tarkoma, "Network-in-a-box: A survey about on-demand flexible networks," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 3, pp. 2407–2428, 3rd Quart., 2018.

[137] *The Versatality and Importance of Cell on Wheels*. [Online]. Available: https://mtstower.com/what-is-cell-on-wheels-max-connectivity/#:~:text=Disaster%20Relief:%20Following%20hurricanes%2C%20floods,enhancements%2C%20which%20COWs%20can%20provide

[138] *FirstNet Response and Recovery*. Accessed: Jul. 22, 2025. [Online]. Available: https://www.firstnet.com/power-of-firstnet/response-to-disasters.html

[139] A. Iqbal et al., "Device discovery in D2D communication: Scenarios and challenges," *Comput., Mater. Continua*, vol. 75, no. 1, pp. 1735–1750, 2023. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1546221823004095

[140] (2025). *What is Private 5G Network in a Box*. [Online]. Available: https://www.echelonedge.com/blogs/what-is-a-private-5g-network-in-a-box/#:~:text=In%20essence%2C%20the%20Network%20in,do%2Dit%2Dyourself%20solution

[141] A. Aijaz, B. Holden, and F. Meng, "Open and programmable 5G network-in-a-box: Technology demonstration and evaluation results," in *Proc. IEEE 7th Int. Conf. Netw. Softwarization (NetSoft)*, Jun. 2021, pp. 369–371.

[142] P. LTE. (2019). *Telecommunication Trailers (CoW) for All Needs*. Accessed: Jul. 22, 2025. [Online]. Available: https://privatelte.com/telco-trailer/#:~:text=4G/5G%20Mobile%20Network%20:%20*%20The%20trailer,on%20technology%2C%20frequency%20band%2C%20power%2C%20and%20landscape

[143] O. Abbasi, A. Yadav, H. Yanikomeroglu, N. -Dáo, G. Senarath, and P. Zhu, "HAPS for 6G networks: Potential use cases, open challenges, and possible solutions," *IEEE Wireless Commun.*, vol. 31, no. 3, pp. 324–331, Jun. 2024.

[144] 3GPP. *Non-Terrestrial Networks Overview and Scenarios*. Accessed: Jul. 22, 2025. [Online]. Available: https://www.tech-invite.com/3m38/toc/tinv-3gpp-38-821_b.html#e-4-1

[145] (2025). *High Altitude Platform Systems Towers in the Skies*. [Online]. Available: https://www.gsma.com/solutions-and-impact/technologies/networks/wp-content/uploads/2022/02/HAPS-Towers-in-the-skies-draft-v-2.1-clean.pdf

[146] *Study on New Radio (NR) To Support Non-terrestrial Networks (Release 15)*, 3GPP, Valbonne, France, 2020. [Online]. Available: http://www.3gpp.org

[147] TSGS, *TS 122 125-V17.6.0-5G; Unmanned Aerial System (UAS) Support in 3GPP (3GPP TS 22.125 Version 17.6.0 Release 17)*, document TS 122 125, Apr. 2022. [Online]. Available: https://www.etsi.org/deliver/etsi_ts/122100_122199/122125/17.06.00_60/ts_122125v170600p.pdf

[148] A. S. Abdalla and V. Marojevic, "Communications standards for unmanned aircraft systems: The 3GPP perspective and research drivers," *IEEE Commun. Standards Mag.*, vol. 5, no. 1, pp. 70–77, Mar. 2021.

[149] A. Alnoman, "UAV-to-UAV communication scheme for enabling emergency services during network failure," in *Proc. Int. Conf. Electr. Comput. Technol. Appl. (ICECTA)*, Nov. 2022, pp. 291–294.

[150] G. Peng, Y. Xia, X. Zhang, and L. Bai, "UAV-aided networks for emergency communications in areas with unevenly distributed users," *J. Commun. Inf. Netw.*, vol. 3, no. 4, pp. 23–32, Dec. 2018.

[151] Z. Kaleem et al., "UAV-empowered disaster-resilient edge architecture for delay-sensitive communication," *IEEE Netw.*, vol. 33, no. 6, pp. 124–132, Nov. 2019.

[152] Z. Yao, W. Cheng, W. Zhang, T. Zhang, and H. Zhang, "The rise of UAV fleet technologies for emergency wireless communications in harsh environments," *IEEE Netw.*, vol. 36, no. 4, pp. 28–37, Jul. 2022.

[153] K. Ali, H. X. Nguyen, Q.-T. Vien, P. Shah, and M. Raza, "Deployment of drone-based small cells for public safety communication system," *IEEE Syst. J.*, vol. 14, no. 2, pp. 2882–2891, Jun. 2020.

[154] Y. Xing, F. Hsieh, A. Ghosh, and T. S. Rappaport, "High altitude platform stations (HAPS): Architecture and system performance," in *Proc. IEEE 93rd Veh. Technol. Conf.*, Apr. 2021, pp. 1–6.

[155] *LOON*. Accessed: Jul. 22, 2025. [Online]. Available: https://www.scientificamerican.com/article/puerto-rico-looks-to-alphabets-x-project-loon-balloons-to-restore-cell-service/

[156] *Zephyr High Altitude Platform Station (HAPS)*. Accessed: Jul. 22, 2025. [Online]. Available: https://www.airbus.com/en/products-services/defence/uas/zephyr

[157] (2025). *Turning on Project Loon in Puerto Rico*. [Online]. Available: https://x.company/blog/posts/turning-on-project-loon-in-puerto-rico/

[158] M. H. Rahman, M. A. S. Sejan, M. A. Aziz, R. Tabassum, J.-I. Baik, and H.-K. Song, "A comprehensive survey of unmanned aerial vehicles detection and classification using machine learning approach: Challenges, solutions, and future directions," *Remote Sens.*, vol. 16, no. 5, p. 879, Mar. 2024.

[159] (2025). *Telstra Abd OneWeb Launch Largest LEO Bakhaul, First Voice Call*. [Online]. Available: https://regionaltechhub.org.au/telstra-oneweb-launch-largest-leo-backhaul-first-voice-call/

[160] (2025). *MTN, Lynk Make Africa's First Satellite Voice Call Using Smartphone*. [Online]. Available: https://www.reuters.com/business/media-telecom/mtn-lynk-make-africas-first-satellite-voice-call-using-smartphone-2025-03-27/

[161] F. Kagai, P. Branch, J. But, R. Allen, and M. Rice, "Rapidly deployable satellite-based emergency communications infrastructure," *IEEE Access*, vol. 12, pp. 139368–139410, 2024.

[162] I. del Portillo, B. G. Cameron, and E. F. Crawley, "A technical comparison of three low Earth orbit satellite constellation systems to provide global broadband," *Acta Astronautica*, vol. 159, pp. 123–135, Jun. 2019. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0094576518320368

[163] A. U. Chaudhry and H. Yanikomeroglu, "Laser inter-satellite links in a starlink constellation," 2021, *arXiv:2103.00056*.

[164] *Better Delivery of Universal Services Discussion Paper*. Accessed: Jul. 22, 2025. [Online]. Available: https://www.infrastructure.gov.au/sites/default/files/documents/bdus2024-amazon-kuiper.pdf

[165] G. Jansson, "Telesat Lightspeed-enabling mesh network solutions for managed data service flexibility across the globe," in *Proc. IEEE Int. Conf. Space Opt. Syst. Appl. (ICSOS)*, Mar. 2022, pp. 232–235.

[166] *ONEWEB LEO CONSTELLATION*. Accessed: Jul. 22, 2025. [Online]. Available: https://www.eutelsat.com/satellite-network/oneweb-leo-constellation

[167] *Developing and Testing China's Guowang Constellation*. Accessed: Jul. 22, 2025. [Online]. Available: https://www.thespacereview.com/article/5004/1

[168] *China Launches Fourth Batch of Thousand Sails Megaconstellation Satellites*. Accessed: Jul. 22, 2025. [Online]. Available: https://spacenews.com/china-launches-fourth-batch-of-thousand-sails-megaconstellation-satellites/

[169] (2025). *Sfera*. [Online]. Available: https://www.deagel.com/Aerospace%20Forces/Sfera/a004297

[170] *Infrastructure for Resilience, Interconnectivity and Security By Satellite IRIS*. Accessed: Jul. 22, 2025. [Online]. Available: https://www.euspa.europa.eu/eu-space-programme/secure-satcom/iris2

[171] X. Qin, T. Ma, X. Zhang, Y. Wang, H. Zhou, and L. Zhao, "Ultra-dense LEO-MEO constellation integrated 6G: A distributed hierarchical mobility management approach," *IEEE Trans. Wireless Commun.*, vol. 24, no. 1, pp. 323–339, Jan. 2025.

[172] S. S. S. G. Seeram, L. Feltrin, M. Ozger, S. Zhang, and C. Cavdar, "Handover challenges in disaggregated open RAN for LEO satellites: Tradeoff between handover delay and onboard processing," *Frontiers Space Technol.*, vol. 6, Jun. 2025.

[173] (2026). *O3b MPOWER*. [Online]. Available: https://www.ses.com/o3b-mpower

[174] (2026). *Viasat*. [Online]. Available: https://www.viasat.com

[175] T. Huang et al., "Integrated computing and networking for LEO satellite mega-constellations: Architecture, challenges and open issues," *IEEE Wireless Commun.*, vol. 31, no. 5, pp. 92–100, Oct. 2024.

[176] Y. Bi et al., "Software defined space-terrestrial integrated networks: Architecture, challenges, and solutions," *IEEE Netw.*, vol. 33, no. 1, pp. 22–28, Jan. 2019.

[177] I. Nakas and T. N. Kaifas, "Low Earth orbit satellite network routing," Institute of Electrical and Electronics Engineers, Bulgaria, Balkans, Tech. Rep., pp. 1–6.

[178] A. H. Arani, P. Hu, and Y. Zhu, "HAPS-UAV-enabled heterogeneous networks: A deep reinforcement learning approach," 2023, *arXiv:2303.12883*.

[179] J. Lyu, Y. Zeng, and R. Zhang, "UAV-aided offloading for cellular hotspot," *IEEE Trans. Wireless Commun.*, vol. 17, no. 6, pp. 3988–4001, Jun. 2018.

[180] U. Challita and W. Saad, "Network formation in the sky: Unmanned aerial vehicles for multi-hop wireless backhauling," in *Proc. IEEE Global Commun. Conf.*, Dec. 2018, pp. 1–6.

[181] Z. Jia, M. Sheng, J. Li, D. Zhou, and Z. Han, "Joint HAP access and LEO satellite backhaul in 6G: Matching game-based approaches," *IEEE J. Sel. Areas Commun.*, vol. 39, no. 4, pp. 1147–1159, Apr. 2021.

[182] *TS 38.811 Study on New Radio (NR) To Support Non-terrestrial Networks*, document TS 38.811, 2025. [Online]. Available: https://www.3gpp.org/ftp/Specs/archive/38_series/38.811

[183] *38.821 Solutions for NR To Support Non-Terrestrial Networks (NTN)*. Accessed: Jul. 22, 2025. [Online]. Available: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3525

[184] *TR 38.832 Study on Enhancement of Radio Access Network (RAN) Slicing*. Accessed: Jul. 22, 2025. [Online]. Available: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3726

[185] *5G;NR;Integrated Access and Backhaul (IAB) Electromagnetic Compatibility (EMC) Release 16)*. Accessed: Jan. 13, 2026. [Online]. Available: https://www.etsi.org/deliver/etsi_ts/138100_138199/138175/16.00.00_60/ts_138175v160000p.pdf

[186] M. Quadrini and C. Roseti, "Architectures for non-terrestrial RAN: Integrated satellite access and backhaul," in *Proc. Int. Symp. Netw., Comput. Commun. (ISNCC)*, Oct. 2023, pp. 1–6.

[187] D. Pugliese et al., "Integrating terrestrial and non-terrestrial networks via IAB technology: System-level design and evaluation," *Comput. Netw.*, vol. 253, Nov. 2024, Art. no. 110726.

[188] E.-H. Mohammedi, E. Lavinal, and G. Fleury, "Detecting and locating configuration errors in IP VPNs with graph neural networks," in *Proc. IEEE/IFIP Netw. Operations Manage. Symp.*, Apr. 2022, pp. 1–6.

[189] L. Beurer-Kellner, M. Vechev, L. Vanbever, and P. Veličković, "Learning to configure computer networks with neural algorithmic reasoning," 2022, *arXiv:2211.01980*.

[190] C. Wang, M. Scazzariello, A. Farshin, D. Kostic, and M. Chiesa, "Making network configuration human friendly," 2023, *arXiv:2309.06342*.

[191] Y. Fang, K. Lu, J. Xue, F. Li, and Z. Lyu, "LLMNDC: A novel approach for network device configuration based on fine-tuned large language models," in *Proc. 5th Int. Conf. Comput. Eng. Intell. Control (ICCEIC)*, Oct. 2024, pp. 283–289.

[192] Y. Wei et al., "INTA: Intent-based translation for network configuration with LLM agents," 2025, *arXiv:2501.08760*.

[193] R. Mondal, A. Tang, R. Beckett, T. Millstein, and G. Varghese, "What do LLMs need to synthesize correct router configurations?," 2023, *arXiv:2307.04945*.

[194] E. Edozie, A. N. Shuaibu, B. O. Sadiq, and U. K. John, "Artificial intelligence advances in anomaly detection for telecom networks," *Artif. Intell. Review*, vol. 58, p. 100, Jan. 2025.

[195] A. Menaceur, H. Drid, and M. Rahouti, "Fault tolerance and failure recovery techniques in software-defined networking: A comprehensive approach," *J. Netw. Syst. Manage.*, vol. 31, no. 4, Oct. 2023.

[196] S. Nam, E.-D. Jeong, and J. W.-K. Hong, "Log-TF-IDF and NETCONF-based network switch anomaly detection," *Int. J. Netw. Manage.*, vol. 35, no. 1, Jan. 2025, Art. no. e2322.

[197] P. Foroughi, F. Brockners, and J.-L. Rougier, "ADT: AI-driven network telemetry processing on routers," *Comput. Netw.*, vol. 220, Jan. 2023, Art. no. 109474.

[198] Y. Chen et al., "NetGPT: A native-AI network architecture beyond provisioning personalized generative services," 2023, *arXiv:2307.06148*.

[199] D. C. Mu et al., "AI and ML-enablers for beyond 5G networks," 5G PPP Technol. Board, Brussels, Belgium, Tech. Rep., 2021. [Online]. Available: http://doi.org/10.5281/zenodo.4299895

[200] A. Sheoran, S. Fahmy, L. Cao, and P. Sharma, "AI-driven provisioning in the 5G core," *IEEE Internet Comput.*, vol. 25, no. 2, pp. 18–25, Mar. 2021.

[201] A. Jain, P. Jain, A. Verma, L. Gopal, and P. Chaudhary, "AI-driven dynamic network slicing for resource optimization in 5G networks: Implementation and performance evaluation," in *Proc. Int. Conf. Cybernation Comput. (CYBERCOM)*, Nov. 2024, pp. 720–724.

[202] A. Gorshenin, A. Kozlovskaya, S. Gorbunov, and I. Kochetkova, "Mobile network traffic analysis based on probability-informed machine learning approach," *Comput. Netw.*, vol. 247, Jun. 2024, Art. no. 110433.

[203] A. A. Hussien, H. Nashaat, and R. F. Abdel-Kader, "Machine learning techniques for spatiotemporal traffic prediction in 5G cellular networks," *Discover Appl. Sci.*, vol. 7, no. 10, p. 1047, Sep. 2025. [Online]. Available: https://link.springer.com/10.1007/s42452-025-06746-3

[204] (2019). *Zero-Touch Network and Service Management (ZSM); Reference Architecture*. [Online]. Available: https://www.etsi.org/deliver/etsi_gs/ZSM/001_099/002/01.01.01_60/gs_ZSM002v010101p.pdf

[205] E. Coronado et al., "Zero touch management: A survey of network automation solutions for 5G and 6G networks," *IEEE Commun. Surveys Tuts.*, vol. 24, no. 4, pp. 2535–2578, 4th Quart., 2022.

[206] M. E. Rajab, L. Yang, and A. Shami, "Zero-touch networks: Towards next-generation network automation," *Comput. Netw.*, vol. 243, Apr. 2024, Art. no. 110294.

[207] N. Linder. (2025). *AI@EDGE Network Architecture and Automation of Future Telecom Networks AI@Edge WP2 Leader on Architecture*. [Online]. Available: https://hexa-x-ii.eu/wp-content/uploads/2023/06/05-Neiva_AI@Edge_EuCNC2023-6G-AI@EDGE-Hexa-X-2_NLfinal.pdf

[208] D. Giannopoulos et al., "ACROSS: Automated zero-touch cross-layer provisioning framework for 5G and beyond vertical services," in *Proc. Joint Eur. Conf. Netw. Commun. 6G Summit (EuCNC/6G Summit)*, Jun. 2023, pp. 735–740.

[209] M. Corici, P. Chakraborty, and T. Magedanz, "A study of 5G edge-central core network split options," *Network*, vol. 1, no. 3, pp. 354–368, Dec. 2021.

[210] S. Hasan et al., "Building flexible, low-cost wireless access networks with magma," 2022, *arXiv:2209.10001*.

[211] S. Mukherjee, R. Ravindran, and D. Raychaudhuri, "A distributed core network architecture for 5G systems and beyond," in *Proc. Workshop Netw. Emerg. Appl. Technol.*, 2018, pp. 33–38.

[212] B. Saleem et al., "TEGRA: A flexible & scalable NextGen mobile core," 2025, *arXiv:2509.07410*.

[213] T. O. Atalay, A. Stavrou, and L. Zhang, "Envisioning the next-generation cellular architecture with named data networking," *Computer*, vol. 58, no. 8, pp. 20–29, Aug. 2025.

[214] L. Zhang et al., "Named data networking," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 44, no. 3, pp. 66–73, Jul. 2014, doi: 10.1145/2656877.2656887.

[215] (2024). *5G;Security Architecture and Procedures for 5G System (3GPP TS 33.501 Version 15.4.0 Release 15)*. [Online]. Available: https://www.etsi.org/deliver/etsi_ts/133500_133599/133501/15.04.00_60/ts_133501v150400p.pdf

[216] R. E. Hattachi and J. Erfanian. (2015). *A Deliverable By NGMN Alliance NGMN 5G White Paper*. [Online]. Available: https://www.ngmn.org/wp-content/uploads/NGMN_5G_White_Paper_V1_0.pdf

[217] A. Anjum, P. Agbaje, A. Mitra, E. Oseghale, E. Nwafor, and H. Olufowobi, "Towards named data networking technology: Emerging applications, use cases, and challenges for secure data communication," *Future Gener. Comput. Syst.*, vol. 151, pp. 12–31, Feb. 2024.

[218] *TS 123 251-V18.0.0-Universal Mobile Telecommunications System (UMTS); LTE; Network Sharing; Architecture and Functional Description (3GPP TS 23.251 Version 18.0.0 Release 18)*, document TS 123 251, 2024. [Online]. Available: https://www.etsi.org/deliver/etsi_ts/123200_123299/123251/18.00.00_60/ts_123251v180000p.pdf

[219] (2025). *TPG Telecom and Optus Sign Network Sharing Agreement Marking New Era of Mobile Services for Regional Australia*. [Online]. Available: https://www.optus.com.au/about/media-centre/media-releases/2024/04/tpg-telecom-and-optus-sign-network-sharing-agreement

[220] R. Abhishek, D. Tipper, and D. Medhi, "Network virtualization and survivability of 5G networks: Framework, optimization model, and performance," in *Proc. IEEE Globecom Workshops (GC Wkshps)*, Dec. 2018, pp. 1–6.

[221] U. N. Kar and D. K. Sanyal, "An overview of device-to-device communication in cellular networks," *ICT Exp.*, vol. 4, no. 4, pp. 203–208, Dec. 2018.

[222] I. Ioannou, C. Christophorou, and V. Vassiliou, "AI/ML for D2D communication in 5G/6G networks and beyond: Concept, applications, challenges, and future directions," Tech. Rep., 2025, doi: 10.36227/techrxiv.176619129.98487483/v1.

[223] S. Hosseinalipour et al., "Multi-stage hybrid federated learning over large-scale D2D-enabled fog networks," *IEEE/ACM Trans. Netw.*, vol. 30, no. 4, pp. 1569–1584, Aug. 2022.

[224] H. Muhammad Fahad Noman, K. Dimyati, K. Ariffin Noordin, E. Hanafi, and A. Abdrabou, "FeDRL-D2D: Federated deep reinforcement learning-empowered resource allocation scheme for energy efficiency maximization in D2D-assisted 6G networks," *IEEE Access*, vol. 12, pp. 109775–109792, 2024.

[225] Q. Guo, F. Tang, and N. Kato, "Federated reinforcement learning-based resource allocation in D2D-enabled 6G," *IEEE Netw.*, vol. 37, no. 5, pp. 89–95, Sep. 2023.

[226] M. Chabbouh, N. Zorba, T. Khattab, and M. Mabrok, "UAV-assisted HAPS in intelligent transportation systems under wind disturbances," in *Proc. Int. Wireless Commun. Mobile Comput. (IWCMC)*, May 2025, pp. 1009–1014.

[227] M. Yan, L. Zhang, W. Jiang, C. A. Chan, A. F. Gygax, and A. Nirmalathas, "Energy consumption modeling and optimization of UAV-assisted MEC networks using deep reinforcement learning," *IEEE Sensors J.*, vol. 24, no. 8, pp. 13629–13639, Apr. 2024.

[228] C. T. Nguyen et al., "Emerging technologies for 6G non-terrestrial-networks: From academia to industrial applications," *IEEE Open J. Commun. Soc.*, vol. 5, pp. 3852–3885, 2024.

[229] I. Todd. *Solar Storms Are Causing Elon Musk's Starlink Satellites To Fall From the Sky Faster Than Expected*. Accessed: Jul. 22, 2025. [Online]. Available: https://www.skyatnightmagazine.com/news/solar-storms-starlink-satellites

[230] E. Juan, M. Lauridsen, J. Wigard, and P. Mogensen, "Performance evaluation of the 5G NR conditional handover in LEO-based non-terrestrial networks," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Apr. 2022, pp. 2488–2493.

[231] Y. Cao, S.-Y. Lien, and Y.-C. Liang, "Deep reinforcement learning for multi-user access control in non-terrestrial networks," *IEEE Trans. Commun.*, vol. 69, no. 3, pp. 1605–1619, Mar. 2021.

[232] S. Li, Q. Wu, R. Wang, and R. Lu, "Toward networking and routing in 6G satellite-terrestrial integrated networks: Current issues and a potential solution," *IEEE Commun. Mag.*, vol. 63, no. 3, pp. 92–98, Mar. 2025.

[233] T. Pan, T. Huang, X. Li, Y. Chen, W. Xue, and Y. Liu, "OPSPF: Orbit prediction shortest path first routing for resilient LEO satellite networks," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2019, pp. 1–6.

[234] T. Taleb, I. Afolabi, K. Samdanis, and F. Z. Yousaf, "On multi-domain network slicing orchestration architecture and federated resource control," *IEEE Netw.*, vol. 33, no. 5, pp. 242–252, Sep. 2019.

[235] L. Pan, X. Yang, and Z. Bu, "Intelligent network slicing optimization for satellite-terrestrial integrated networks," *IEEE Commun. Lett.*, vol. 28, no. 10, pp. 2342–2346, Oct. 2024.

[236] E. M. Mohamed, S. Hashima, K. Hatano, and M. Rihan, "Mobility management in 3D unified 6G networks: Challenges, opportunities and future directions," *ICT Exp.*, vol. 12, no. 1, pp. 255–266, Feb. 2026.

[237] L. Djeddai and R. Ke Liu, "IPSecOPEP: IPSec over PEPs architecture, for secure and optimized communications over satellite links," in *Proc. 7th IEEE Int. Conf. Softw. Eng. Service Sci. (ICSESS)*, Aug. 2016, pp. 264–268.

[238] M. H. Adnan and Z. Ahmad Zukarnain, "Device-to-device communication in 5G environment: Issues, solutions, and challenges," *Symmetry*, vol. 12, no. 11, pp. 1–22, Oct. 2020.

[239] I. Chandran and K. Vipin, "Multi-UAV networks for disaster monitoring: Challenges and opportunities from a network perspective," *Drone Syst. Appl.*, vol. 12, pp. 1–28, Jan. 2024.

[240] H. Guo, J. Li, J. Liu, N. Tian, and N. Kato, "A survey on space-air-ground-sea integrated network security in 6G," *IEEE Commun. Surveys Tuts.*, vol. 24, no. 1, pp. 53–87, 1st Quart., 2022.

[241] I. Ahmad, J. Suomalainen, P. Porambage, A. Gurtov, J. Huusko, and M. Höyhtyä, "Security of satellite-terrestrial communications: Challenges and potential solutions," *IEEE Access*, vol. 10, pp. 96038–96052, 2022.

[242] M. H. Eiza and A. Raschellà, "A hybrid SDN-based architecture for secure and QoS aware routing in space-air-ground integrated networks (SAGINs)," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Mar. 2023, pp. 1–6.

[243] S. Ren, J. Liu, R. Ji, S. S. Ge, and D. Li, "A secure authentication scheme for satellite-terrestrial networks," *IEEE Trans. Netw. Sci. Eng.*, vol. 11, no. 6, pp. 6470–6482, Nov. 2024.

[244] X. Ding, Z. Zhang, and D. Liu, "Low-delay secure handover for space-air-ground integrated networks," in *Proc. IEEE 31st Annu. Int. Symp. Pers., Indoor Mobile Radio Commun.*, Aug. 2020, pp. 1–6.

[245] M. Koziol. (2025). *Alphabet's Loon Failed To Bring Internet To the World. What Went Wrong*. [Online]. Available: https://spectrum.ieee.org/why-did-alphabets-loon-fail-to-bring-internet-to-the-world

[246] L. S. Mukherjee. (2025). *Musk Says May Need $30 Bln To Keep Starlink in Orbit*. [Online]. Available: https://www.reuters.com/business/aerospace-defense/musk-sees-starlink-winning-500000-customers-next-12-months-2021-06-29/#:~:text=Musk%20says%20may%20need%20$30%20bln%20to%20keep%20Starlink%20in%20orbit%20%7C%20Reuters

[247] Q. Cui et al., "Overview of AI and communication for 6G network: Fundamentals, challenges, and future research opportunities," *Sci. China Inf. Sci.*, vol. 68, no. 7, Jul. 2025, Art. no. 171301.

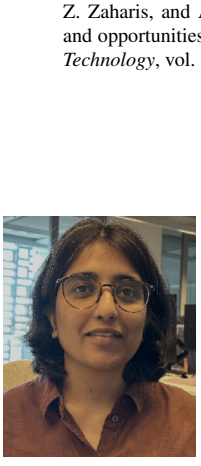
[248] P. Kourouklidis, D. Kolovos, J. Noppen, and N. Matragkas, "A model-driven engineering approach for monitoring machine learning models," in *Proc. ACM/IEEE Int. Conf. Model Driven Eng. Lang. Syst. Companion (MODELS-C)*, 2021, pp. 160–164.

[249] C. Pu, K. Wang, and Y. Xia, "Robustness of link prediction under network attacks," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 67, no. 8, pp. 1472–1476, Aug. 2020.

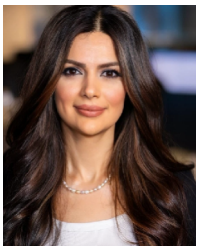
[250] (2023). *TS 128 105-V17.4.0-5G; Management and Orchestration; Artificial Intelligence/ Machine Learning (AI/ML) Management (3GPP TS 28.105 Version 17.4.0 Release 17)*. [Online]. Available: https://www.etsi.org/deliver/etsi_ts/128100_128199/128105/17.04.00_60/ts_128105v170400p.pdf

[251] 3GPP. (2022). *TS 38.331: NR; Radio Resource Control (RRC); Protocol Specification*. [Online]. Available: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3197

[252] I. P. Chochliouros, A. S. Spiliopoulou, P. Lazaridis, A. Dardamanis, Z. Zaharis, and A. Kostopoulos, "Dynamic network slicing: Challenges and opportunities," in *IFIP Advances in Information and Communication Technology*, vol. 585. Cham, Switzerland: Springer, 2020.



VIJAYA DURGA CHEMALAMARRI received the Ph.D. degree from the University of Technology Sydney (UTS), Australia. She is currently a Researcher with the National Telecommunication Resilience Centre (NTRC), UTS. Her research interests include software-defined networking, network automation, network intelligence, and network resilience.



MAHROKH ABDOLLAHI (Member, IEEE) received the M.S. and Ph.D. degrees in electrical and data engineering from the University of Technology Sydney (UTS), Australia, in 2016 and 2022, respectively. From 2006 to 2014, she worked as a Computer Engineer on various networking projects. Prior to her current role, she was with CSIRO's Data61 for two years, contributing to research in O-RAN and privacy-enhancing technologies. She is currently a Post-Doctoral Fellow with the National Telecom Resilience Centre (NTRC), UTS. Her research interests include telecommunications resilience, O-RAN, 5G/6G wireless networks, ML/AI applications, software-defined networking, privacy, and cybersecurity.

ADAM BRYANT (Member, IEEE) received the Bachelor of Science degrees in computer science and mathematics from the School of Engineering, Tulane University. He has more than 30 years of experience in the telecommunications industry, focusing on mission-critical network technologies and implementations across mobile and fixed-line broadband and associated IT and cybersecurity areas. He has held various roles in research and development, architecture, operations, and executive leadership. Currently, he is the Director of the NTRC Controlled Test Facility and an Industry Advisor to the Telecommunications Research Unit, University of Technology Sydney (UTS). He is also an independent consultant providing detailed subject matter expertise in investigations of network outages. He holds two U.S. patents.

MEHRAN ABOLHASAN (Senior Member, IEEE) received the B.E. degree in computer engineering and the Ph.D. degree in telecommunications from the University of Wollongong in 1999 and 2003, respectively. He has over 20 years of experience in research and development and working in various research leadership roles. Some of these previous roles include working as the Director of Research Programs with the Faculty of Engineering and IT and the Deputy Head of the School for Research with the School of Electrical and Data Engineering, University of Technology Sydney, where he is currently the Leader of the Intelligent Networks and Applications Laboratory, Faculty of Engineering and IT. He has authored over 200 international publications and through his sustained track record of industry engagement, creation of new research ideas, and directions; he has successfully secured several research and development projects worth over eight million dollars. This includes external grants, such as ARC, CRC, industry, and government funded research projects. His current research interests include 5G/6G wireless networks, the Internet of Things, cybersecurity, software defined networking, intelligent transportation systems (ITS), urban greening, and digital agriculture.

RAYMOND OWEN (Member, IEEE) received the Bachelor of Engineering degree in electrical and electronic from the King's College London in 1992 and the Ph.D. degree in electrical and electronic engineering from the University of Birmingham, U.K., in 1995. His doctoral research focused on the modeling of high-frequency acoustic scattering from a rough surface with the University of Birmingham. Currently, he works as an Industry Professor with the Faculty of Engineering and IT, University of Technology Sydney (UTS). In addition to his academic role, he is also a Partner at Tech Audit Partners, an U.S.-based consultancy specializing in resilience. He also provides high-level consultancy on network outages, their causes, and recovery strategies for major management consulting firms. His research and commercial interests include telecommunications resilience, digital modeling, fixed-line telecoms, network protocols, and wireless networking, particularly focusing on propagation.