CISTER
Research Centre in
Real-Time & Embedded
Computing Systems

Journal Paper

Resilience and Failure Analysis in Next-Generation Communication Networks: A Contemporary Survey

Siguo Bi

Xin Yuan

Shuyan Hu

Kai Li*

Wei Ni*

Ekram Hossain

Xin Wang

*CISTER Research Centre

CISTER-TR-251001

2025

Resilience and Failure Analysis in Next-Generation Communication Networks: A Contemporary Survey

Siguo Bi, Xin Yuan, Shuyan Hu, Kai Li*, Wei Ni*, Ekram Hossain, Xin Wang

*CISTER Research Centre

Polytechnic Institute of Porto (ISEP P.Porto)

Rua Dr. António Bernardino de Almeida, 431

4200-072 Porto

Portugal

Tel.: +351.22.8340509, Fax: +351.22.8321159

E-mail: fdbsg@fudan.edu.cn, xin.yuan@data61.csiro.au, syhu14@fudan.edu.cn, kai@isep.ipp.pt, wei.ni@cister-labs.pt, ekram.hossain@umanitoba.ca, xwang11@fudan.edu.cn

https://www.cister-labs.pt

Abstract

This paper provides a comprehensive exploration of network resilience in next-generation (xG) cellular communication infrastructures. It begins with an introduction to the network science framework and its relevance to modern communication systems, and then delves into the theoretical foundations of network resilience, including key concepts from graph theory, complex network analysis, and cascading failure models. A detailed examination of network failures in xG networks follows, employing graph-theoretic approaches to analyze failure propagation, identify critical nodes, and assess network vulnerabilities. The paper also outlines practical methodologies for enhancing resilience, such as adaptive topology design, failure prediction, and decentralized architectural frameworks. The paper further discusses future research directions, emphasizing emerging challenges and opportunities in network resilience. It also reviews ongoing standardization efforts aimed at integrating network science principles into communication infrastructure design. Lessons learned and open challenges are summarized that require further investigation, making it a valuable resource for researchers, engineers, and practitioners seeking to advance the resilience and adaptability of xG networks.

Resilience and Failure Analysis in Next-Generation Communication Networks: A Contemporary Survey

Siguo Bi, Xin Yuan, *Senior Member, IEEE,* Shuyan Hu, *Member, IEEE,* Kai Li*, *Senior Member, IEEE,* Wei Ni, *Fellow, IEEE,* Ekram Hossain, *Fellow, IEEE,* and Xin Wang*, *Fellow, IEEE*

***Abstract*—This paper provides a comprehensive exploration of network resilience in next-generation (xG) cellular communication infrastructures. It begins with an introduction to the network science framework and its relevance to modern communication systems, and then delves into the theoretical foundations of network resilience, including key concepts from graph theory, complex network analysis, and cascading failure models. A detailed examination of network failures in xG networks follows, employing graph-theoretic approaches to analyze failure propagation, identify critical nodes, and assess network vulnerabilities. The paper also outlines practical methodologies for enhancing resilience, such as adaptive topology design, failure prediction, and decentralized architectural frameworks. The paper further discusses future research directions, emphasizing emerging challenges and opportunities in network resilience. It also reviews ongoing standardization efforts aimed at integrating network science principles into communication infrastructure design. Lessons learned and open challenges are summarized that require further investigation, making it a valuable resource for researchers, engineers, and practitioners seeking to advance the resilience and adaptability of xG networks.**

***Index Terms*—Next-generation (xG) wireless communication network, cellular communication infrastructure, resilience, failure analysis, failure prevention.**

I. Introduction

Next-generation (xG) networks, including the sixth-generation (6G) and beyond 6G (B6G), represent highly complex, multi-layered, and interconnected systems essential for modern infrastructure. These networks resemble complex systems characterized by dynamic topologies, self-organizing behavior, and a high degree of interdependency. At the heart of this transformative wave is the central role of communication and network systems, which thread through essential sectors, including but not limited to telecommunications, power grids, banking and finance, transportation, water supply systems, supply chain, government services, and emergency services. In this impending epoch, xG cellular communication infrastructures are poised to ascend to a pivotal position, advancing beyond the achievements of their predecessors, including the fifth-generation (5G) communication systems.

The implementation of 5G, characterized by its unwavering focus on security, continuity, and availability, has already left an indelible mark on critical infrastructures. Not merely confined to incremental progress, 5G technology has orchestrated remarkable feats in diverse domains. In the area of smart grid management, the precision and efficacy of 5G have ushered in a new era of energy resource exploitation, demonstrating high flexibility [1] and stringent security measures [2]. The financial and banking sectors, driven by an insatiable demand for low-latency and high-security services, have found a reliable ally in 5G, ensuring efficient operations and robust governmental monitoring services [3]. The transportation and emergency services sectors, both inherently reliant on instantaneous and secure communication, have witnessed transformative benefits by empowering 5G technology [4], [5].

In networked systems, analyzing failures is pivotal for ensuring stability and reliability. Graph theory [6], percolation theory [7], and cascading failure models [8] serve as essential tools for dissecting failure propagation mechanisms. Graph theory, by representing networks as graphs of nodes and edges, elucidates the impact of node connections on system stability [6]. Percolation theory evaluates network resilience by examining the size of the largest connected component under stress [7]. Cascading failure models simulate the dynamic spread of failures from initial nodes throughout the network, offering insights into critical components and mitigation strategies [8], particularly in power systems where such failures can lead to widespread blackouts.

Network robustness metrics, including node degree distribution, clustering coefficients, betweenness centrality [9], and spectral gap analysis, are indispensable for identifying key nodes and vulnerabilities. Node degree distribution reflects connectivity, while betweenness centrality highlights node importance. These metrics assess network resilience against

Manuscript received May 1, 2025; revised August 18, 2025 and September 25, 2025; accepted October 6, 2025.

S. Bi and X. Wang are with Fudan University, Shanghai 200433, China (e-mail: {fdbsg,xwang11}@fudan.edu.cn).
X. Yuan is with Data61, Commonwealth Scientific and Industrial Research Organization (CSIRO), Sydney, NSW 2122, Australia, and the School of Computer Science and Engineering, University of New South Wales, Sydney, NSW 2052 (e-mail: xin.yuan@csiro.au).

W. Ni is with the School of Engineering, Edith Cowan University, Perth, WA 6027, and the School of Computer Science and Engineering, The University of New South Wales, Sydney, NSW 2052, Australia (e-mail: wei.ni@ieee.org).

S. Hu is with the College of Electronics and Information Engineering and the Shanghai Institute of Intelligent Science and Technology, Tongji University, Shanghai 201804, China (email: syhu@tongji.edu.cn).

K. Li is with the School of Electrical Engineering and Computer Science, TU Berlin, Germany, and also with Real-Time and Embedded Computing Systems Research Centre (CISTER), Porto 4249–015, Portugal (e-mail: kaili@ieee.org).

E. Hossain is with the Department of Electrical and Computer Engineering, University of Manitoba, Winnipeg, MB R3T 2N2, Canada (e-mail: ekram.hossain@umanitoba.ca).
**Corresponding authors: K. Li and X. Wang.*

List of acronyms and abbreviations

3GPP	3rd Generation Partnership Project
5G	The fifth-generation
6G	The sixth-generation
AI	Artificial intelligence
AKA	Authentication and key agreement
ATIS	Alliance for Telecommunications Industry Solutions
B6G	Beyond 6G
BBRv2	Bottleneck bandwidth and round-trip propagation time version 2
BPDC	Blockchain-based privacy-aware distributed collection
BS	Base station
CA	Certificate authority
CAV	Connected and autonomous vehicle
CNN	Convolutional neural network
CPS	Cyber-physical system
C-V2X	Cellular V2X
DAN	Decentralized autonomous network
D2D	Device-to-device
D-S	Dempster-shafer
DDoS	Distributed denial of service
DID	Decentralized identifier
DNN	Deep neural network
DNS	Domain name system
DRL	Deep reinforcement learning
DPA	Destructive physical analysis
DT	Digital twin
FL	Federated learning
FLISR	Fault location, isolation, and service recovery
FPGA	Field programmable gate array
FSO	Free-space optics
GA	Genetic algorithm
GNN	Graph neural network
GSM	Global system for mobile communications
GWO	Grey wolf optimization
IAB	Integrated access and backhaul
IDS	Intrusion detection system
IEG	Independent evaluation group
IIoT	Industrial Internet-of-Things
IL-GAN	Incremental learning generative adversarial network
IoT	Internet of Things
IoV	Internet of Vehicle
ISAC	Integrated sensing and communication
IT	Information technology
IQ	In-phase and quadrature
ITU	International Telecommunications Union
JEEC	Joint encryption and error-control
KGC	Key generation center
KPI	Key performance indicator
LEO	Low Earth orbit
LLM	Large language model
LoS	Line-of-sight
LSTM	Long short-term memory
LTE	Long term evolution
mMIMO	Massive MIMO
mmWave	Millimeter-wave
MAC	Medium access control
MDA	Management data analytics
MEC	Multi-access edge computing
ML	Machine learning
MFH	Mobile fronthaul
NF	Network function
NFV	Network function virtualization
NGMN	Next Generation Mobile Networks
NIST	National Institute of Standards and Technology
NR	New Radio
OBC	Onboard charging
O-RAN	Open RAN
P2P	Peer-to-peer
PAC	Protection, automation and control
PathGNN	Path-based graph neural network
PCRF	Policy and charging rules function
PD	Partial discharge
PoA	Proof-of-authority
PSO	Particle swarm optimization
PTP	Precision time protocol
QKD	Quantum key distribution
QSDC	Quantum secure direct communication
QoS	Quality of service
RAN	Radio access network
RF	Radio frequency
RIS	Reconfigurable intelligent surface
RSSI	Received signal strength indicator
RTO	Retransmission time
RTT	Round-trip time
SAGSIN	Space-air-ground-sea integrated network
SDN	Software-defined networking
SF	Service function
SFC	Service function chain
SFF	Service function forwarder
SMPB	Smart mobile power bank
SVM	Support vector machine
TCP	Transmission control protocol
TCP-PEP	TCP performance enhancing proxy
THz	Terahertz
UAV	Unmanned aerial vehicle
UDN	Ultra-dense network
UE	User equipment
URLLC	Ultra-reliable and low-latency communications
UWB	Ultra-wide band
V2G	Vehicle-to-grid
V2X	Vehicle-to-everything
VANET	Vehicular ad-hoc network
VLC	Visible light communication
VNF	Virtual network function
vSDN	Virtualized software-defined network
WLAN	Wireless local area network
WWRF	Wireless World Research Forum
XAI	Explainable AI
xG	Next-generation
ZSM	Zero touch management

random failures or targeted attacks. Integrating these theories and metrics provides a comprehensive analysis of network fragility and risks, enabling the formulation of targeted strategies to enhance overall system stability, ensuring *resilience, adaptability, and robustness* [10]–[13].

A. Notable Recent Failures in Communication Infrastructures

One notable case is Hurricane Katrina, which struck the Gulf Coast of the United States in 2005. The hurricane resulted in widespread destruction, flooding, and a breakdown of critical infrastructure, highlighting the essential role of communication systems in emergency response and recovery [14].

In 2020, a European Union (EU) annual report on telecom security incidents highlighted that 40% of time loss, that is, 346 million hours, was attributed to telecom failures caused by faulty software changes or updates [15]. In February 2021, a severe snowstorm in the central United States caused power outages, causing communication service failures and affecting millions of people [16]. June 2021 witnessed a catastrophic outage that affected critical websites and applications worldwide, spanning the Americas, Europe, Asia, and South Africa. The incident resulted from a network software failure triggered by an inappropriate software update [17]. An incidental outage in the same month damaged an international information technology (IT) organization's edge domain name system (DNS) service. Airlines, subways, banks, and international companies were affected [18]. Telecommunications and power systems in the United States were threatened by devastating floods [19].

In July 2022, serious service failures in data centers in London, UK, led to operational disruptions for major IT companies like Google and Oracle. The core reason behind the failure was the extreme weather that affected the normal operation of the cooling system [20]. Concurrently, millions of users in Japan faced disconnections caused by equipment failure, affecting finance and transportation [21]. November 2022 witnessed a security failure resulting from a hacker attack, leading to severe information leakage for millions of T-Mobile customers [22]. There were extensive breakdowns in Macau, China, in December 2022 due to an incidental hardware failure in the Hong Kong cooling system [23].

August 2023 brought severe telecom service failures to Maui, USA, due to wildfires causing power failures in telecom service infrastructures [24]. In the same month, many Haitian users experienced severe service failures due to fiber optic cable damage [25]. The data communication system for national bank statements in Japan failed in October 2023, affecting banks and financial institutions. The initial report suggested that the failure was possibly due to the update process of the relay processor reaching its operational limit [26]. In November 2023, Optus, the second largest network provider in Australia, failed to connect to phone and Internet services, with the cause not immediately identified [27].

Most recently, in February 2024, a network upgrade error caused a nationwide service disruption in the USA, leaving users with only SOS mode [28]. In August 2024, a network outage in Australia led to failed emergency calls due to delayed reporting to authorities [29]. In May 2025, a sudden telecom failure left over 130,000 users without access to mobile services across Quebec and Ontario in Canada [30]. In the same month, potential cases, including aging infrastructures and software faults, caused repeated radar and communication failures, disrupting flight operations at the Newark Liberty International Airport in the USA. Hundreds of flights were therefore delayed or canceled [31].

Many existing failures of the above-mentioned are anticipated not only to persist but also potentially worsen in severity in future systems, due to the increased scale and speed of operations. For example, security vulnerabilities currently experienced in 5G networks [32], e.g., subscriber privacy vulnerability [33], may become more critical in 6G, where higher data rates and broader connectivity could amplify the impact of breaches [34]. The reliance on massive Internet of Things (IoT) deployments could lead to frequent and severe service disruptions if devices are not adequately protected against cyber threats.

New failures or risks are likely to arise from new technologies and frequency bands that will be used in xG systems. For instance, the integration of advanced technologies, e.g., artificial intelligence (AI) and machine learning (ML) in network management, brings forth unique challenges [35], [36], including susceptibility to adversarial attacks or data poisoning. The adoption of terahertz (THz) bands [37], which promise greater bandwidth, also comes with new vulnerabilities, including a higher sensitivity to weather conditions that can severely impact signal propagation and network reliability. Moreover, the deployment of complex reconfigurable intelligent surfaces (RISs) and massive MIMO (mMIMO) systems increases the risks of hardware and system failures [38], [39].

B. Motivation

As communication network systems grapple with increasingly complex and dynamic risks, including cyberattacks, environmental disturbances, and systemic overloads, comprehensive risk management frameworks and internationally coordinated response protocols are imperative. Modeling such risks involves not only assessing static vulnerabilities but also understanding the temporal dynamics of failure propagation, feedback loops, and recovery mechanisms that are particularly critical in time-sensitive domains, such as emergency response and autonomous mobility.

As a rigorous engineering discipline, failure analysis uncovers and traces the underlying mechanisms of failures, thereby generating actionable insights to strengthen system robustness and prevent cascading consequences. Although significant progress has been made in investigating failure scenarios in xG systems, the escalating complexity of these systems has driven researchers to explore increasingly sophisticated analytical approaches. A growing body of literature has emerged, proposing diverse methodologies and solutions for effective failure analysis and offering perspectives to enhance the reliability and resilience of xG systems and applications.

Several emerging failure analysis and network technologies hold significant promise for enhancing the resilience of communication infrastructures to failures. For instance, decentralized autonomous networks (DANs) represent a paradigm shift from traditional centralized architectures to distributed, fault-tolerant systems [40]. By removing single points of failure and enabling localized decision-making, DANs support fault detection and response without reliance on central authorities. Moreover, advances in quantum communications, e.g., quantum key distribution (QKD) [41], introduce unprecedented security capabilities against unauthorized access and data tampering. By offering instant detection of breaches and enabling secure key exchange, QKD and related quantum techniques can provide a critical security layer that contributes to failure management and mitigates cyber-related failures.

C. Contribution

This survey enriches the discourse on failures, failure analysis, and countermeasures in xG cellular communication infrastructures, with the following contributions:

- We explore the critical role of failure analysis in supporting network resilience for xG systems, particularly by identifying network vulnerabilities and providing insights for resilience design and assessment. We highlight how failure analysis, as a foundational component of network resilience frameworks, contributes to the robustness of xG networks in the face of disruptions.
- We delve into a comprehensive review of representative works by categorizing failures in 5G/6G systems and applications, many of which are associated with new frequency bands and techniques likely to be adopted in xG. We also summarize constructive countermeasures

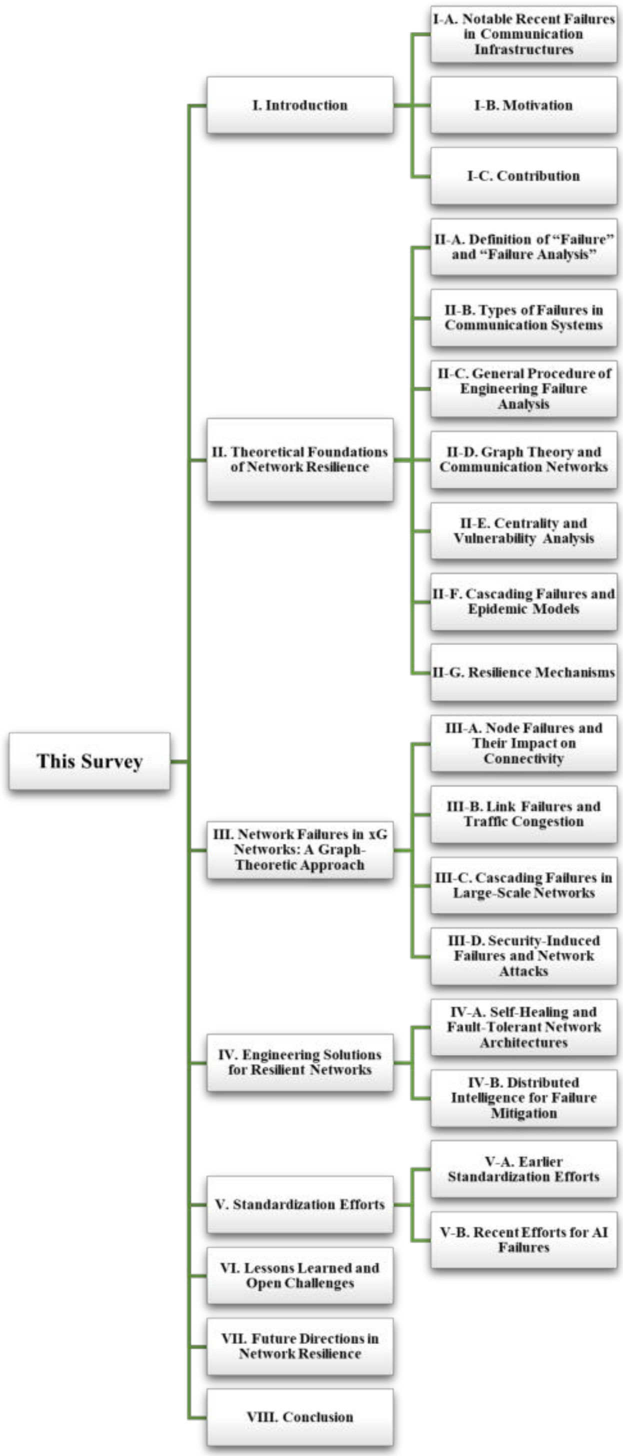

Fig. 1: The structure of this survey.

tailored to address these failures, contributing to xG network resilience, failure analysis, and prevention.

- We identify challenges and outline research directions, including concurrent failures, distributed and/or cross-domain authentication, self-modeling and healing, failure dataset standardization, and distributed data recovery.

As depicted in Fig. 1, the structure of this survey is as follows. Section II explores the theoretical foundations of network resilience and failure analysis. Section III reviews network failures in xG networks from a graph-theoretic perspective. Section IV provides engineering solutions for resilient networks. In Section V, we discuss efforts to standardize and mitigate failures in xG communications and closely related AI systems. Section VI summarizes the lessons learned, challenges, and open issues, followed by promising future directions in network resilience in Section VII. The survey is concluded in Section VIII.

II. Theoretical Foundations of Network Resilience

Network resilience is a multifaceted concept grounded in diverse theoretical foundations, including failure analysis, network science, system dynamics, and reliability engineering. These theories collectively form the framework for understanding and enhancing network resilience.

A. Definition of "Failure" and "Failure Analysis"

1) Failure: The notion of failure can be illustrated when one system, product, device, or component malfunctions due to the deterioration of the exterior appearance or interior structure, depriving its original declared function. Appearance deformation can significantly impact the mechanical integrity of communication equipment, leading to failures that cascade into broader network issues. Bent antennas, for instance, can suffer from misaligned directional patterns, reducing signal strength and coverage. Deformed circuit boards may experience short circuits or broken traces, disrupting electrical connections and causing intermittent or complete signal loss [42]. Loose components, such as connectors or capacitors, can introduce noise or intermittent failures, further degrading signal quality. In addition, these physical deformations can compromise the equipment's thermal management, leading to overheating and reduced performance. The product, device, or component can be considered under failure once it is in accordance with being under any of the three states [43]; see Fig. 2.

2) Failure Analysis: As an efficient countermeasure to failures, failure analysis is a crucial scientific subject specifically used for identifying the cause of failure, the underlying failure mechanism based on the failure mode [44]. Failure analysis is widely acknowledged as a rigorous and formal scientific process that relies on multidimensional data collected from various sectors of production and operation. This process involves conducting comprehensive analyses to trace the in-depth mechanisms and root causes leading to failures.

B. Types of Failures in Communication Systems

Table I provides a comprehensive overview of various critical issues affecting the robustness and reliability of xG cellular infrastructures. The identified failure types encompass transmission failure, service failure, network failure, power failure, component failure, authentication failure, task integrity failure, and physical security failure. Table II compares the severity levels of the different failures.

TABLE I: Comparative summary of failure types

Failure Type	Definition	Main Causes
Service Failure	Disruptions in core services like cloud, edge, storage, computation, and virtualization.	Inefficient management of dynamic requirements, imbalanced service allocation, inadequacies in managing service demand.
Network Failure	Congestion, blockage, conflicts, and collisions; cascading failure; traffic reliability issues in network components.	Incidental disruptions, inappropriate traffic management, improper virtual network placement, and resource conflicts.
Power Failure	Malfunction in communication networks within power grids.	Connectivity and energy consumption issues, incidental equipment damage, and unreliability of Device-to-Device connections.
Component Failure	Malfunction or fault of critical components or modules in critical infrastructure.	Electromagnetic device deterioration, aging, and fracture, incidental disruption from natural disasters, and environmental corrosion.
Authentication Failure	Mistaken granting or denial of permissions; critical in xG's dynamic, AI-driven environment.	Complexity in dynamic xG environments, decentralized nature, and traditional authorization mechanisms may struggle.
Task Integrity Failure	Compromised or altered tasks are crucial for maintaining trustworthiness in xG systems.	Advanced cyberattacks, interference in interconnected devices, and internal system errors.
Physical Security Failure	Unauthorized interference or tampering with physical components in xG systems.	Device theft, tampering, sabotage of critical infrastructure nodes, and compromising localized networks.

TABLE II: Characteristics of different communication failures

Failure Type	Occurrence Time	Recovery and Detection Difficulty	Severity Level
Service failure	During operation	Medium	High
Network failure	During data transmission	Medium	High
Power failure	During operation	High	High
Component failure	During communication	Medium	Medium
Authentication failure	During data access	Medium	Medium
Task integrity failure	During mission execution	High	High

Fig. 2: Three categories of failure states: the orange box denotes devices or systems requiring replacement for recovery; the blue box indicates devices or systems that fail to satisfy operational reliability requirements; and the green box represents devices or systems that do not meet specified performance indicators.

1) Service Failure: Service failures primarily pertain to disruptions in operating services critical for supporting core system and application functions. These services, which encompass cloud services, edge services, resource storage services, computation services, and virtualization-based services, cease to operate normally or consistently, impacting their ability to fulfill designated functions [45]. The key contributors to service failures are inefficient management of dynamic requirements, imbalanced service allocation, and inadequacies in managing service demand.

2) Network Failure: Network failures are characterized by congestion, blockage, conflicts, and collisions within the network, primarily stemming from inefficient management of network traffic resources [46]–[48]. Network failures manifest as traffic reliability issues in backhaul, software-defined networking (SDN), multi-access edge computing (MEC), radio access network (RAN), and network slices. The key factors contributing to network failures include incidental disruptions, inappropriate dynamic traffic management, improper dynamic placement of virtual networks, inadequate orchestration, insufficient base station (BS) management, and resource conflicts. For example, the typical cascading failures are initiated by a small subset of malfunctioning nodes in a communication network [8], [49], [50]. In many cases, redistributed data flows could exceed the capacity of some links and routers, resulting in network failures.

3) Power Failure: In communication networks dependent on power grids, power failures, originating from grid outages, can lead to substantial disruptions [51]. The primary causes of power failures include connectivity and energy consumption issues, incidental equipment damage, and the unreliability of device-to-device (D2D) connections. For example, a power delivery failure often starts with component failures in one or several branches, leading to power delivery redistribution due to the physical laws of circuit theory. The resulting compensatory power flows can overload other branches, potentially triggering power failures.

4) Component Failure: A component failure can be defined as a situation where a malfunction or fault occurs in critical components or modules that are integral to the critical communication infrastructure. Then, xG is envisioned to play a versatile role. The main causes of component failure are electromagnetic device deterioration, device aging, device fracture, incidental disruption from natural disasters, and environmental corrosion at the location for deployment [52]. For example, the ever-increasing communication service needs in future xG systems could push up the power flow delivery in many

BSs. The integrated circuits would experience heating and temperature rise, causing possible damage to components.

5) Authentication Failure: An authorization failure represents a critical flaw where a device or application is mistakenly granted or denied permission to access resources, execute tasks, or perform actions within the network. Such failures could arise from complexities introduced by the highly dynamic, AI-driven [53], and decentralized nature of xG cellular infrastructures, where traditional centralized authorization mechanisms may struggle to keep pace [54]. For instance, the promising Internet of Drones for critical tasks is in need of efficient scheduling from the central control server. Then, a malicious drone can launch attacks to affect the cross-domain authentication, resulting in potential authentication failures.

6) Task Integrity Failure: In xG, a task integrity failure denotes a scenario where a task, including its data transmission, processing, or any network operation, is compromised or altered, either maliciously or inadvertently. This integrity breach could result from advanced cyberattacks targeting AI functions, interference in the vast web of interconnected user devices, or internal system errors. Given that xG promises operations at unparalleled scales and speeds, even minor task alterations can cascade into significant disruptions, ensuring task integrity is crucial. Take an unmanned aerial vehicle (UAV) network as an example. A small set of malfunctioning UAVs could severely impede the normal cooperation of the UAV swarm, e.g., in a collaborative task like disaster rescue, resulting in significant task integrity failures [55].

7) Physical Security Failure: xG systems are envisioned to converge intricate digital infrastructures and the proliferation of physical devices, including IoT sensors, edge servers, and radio transmitters. From device theft and tampering to sabotage of critical infrastructure nodes, physical security breaches can introduce catastrophic vulnerabilities. Integrating robust physical safeguarding measures is paramount, complementing the advanced digital security protocols they uphold. Some examples of physical attacks are eavesdropping and sabotage to BSs and sensors in communication networks [56]. They can lead to severe privacy breaches and loss of sensitive information. Inefficient management of physical attacks could further cascade down into system-wide physical security failures.

C. General Procedure of Engineering Failure Analysis

Given the inherent complexity of xG, a direct application of general procedural principles to the distinctive context of xG is deemed unrealistic, and hence, a more tailored approach is imperative. Table III gives a comprehensive exploration encompassing hardware failure, software failure [57], and system/network failure, and considering the unique challenges posed by xG.

1) Hardware Failure Analysis: When a physical entity fails to fulfill its original purpose, there is a hardware failure. Hardware is essential for critical infrastructure. Here, hardware refers to key devices, modules, and components crucial for emerging technologies. In THz communication, holographic beamforming, RIS, digital baseband processing units, radio frequency (RF) transceivers, and array antennas are indispensable. Specific hardware failures result from physical damage, defect, or aging of devices, modules, or components.

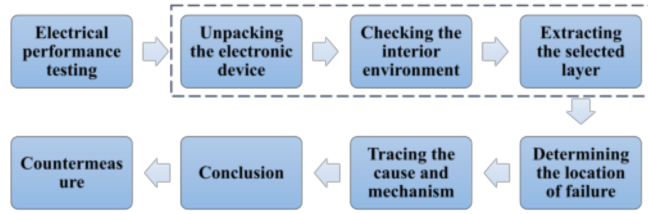

Fig. 3: The general failure analysis procedures for xG hardware, where the principle for this procedure is to timely, efficiently, and effectively identify and locate a failure and to trace further the very cause inducing the failure. The part of the procedure within the dashed block is also called DPA, which can be replaced by other non-destructive solutions.

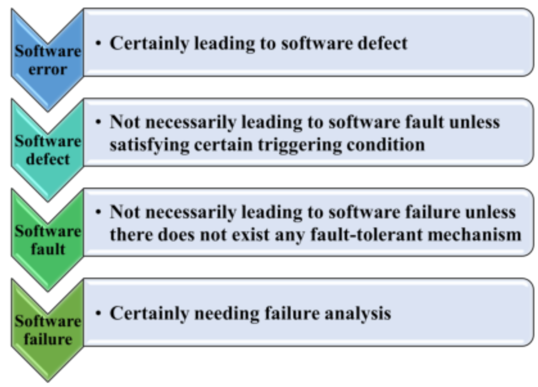

Fig. 4: The relationship among the four critical concepts of software failure.

The majority of hardware failures are due to electrical or electronic issues, e.g., open circuits, short circuits, abnormal leakage currents, and electrical breakdowns. The failure analysis process for xG hardware can generally be outlined sequentially, as illustrated in Fig. 3. The procedure within the dashed block of Fig. 3 is called destructive physical analysis (DPA), used for determining the defective devices potentially leading to severe consequences [58].

In critical components like quantum cascade lasers [59] and sealed relays [60], DPA has been used as a crucial method to boost the reliability of communication equipment. In particular, it can be used to provide structural failure analysis reports of degraded quantum cascade lasers, and to identify the internal abnormality of sealed relays. By accurately pinpointing failure modes and investigating internal flaws, DPA facilitates the refinement of design and manufacturing techniques, ultimately bolstering the stability and longevity of devices [59], [60]. In general scenarios, DPA can be flexibly replaced by resorting to flaw-detection tools, e.g., X-ray or ultrasonic waves, especially considering the powerful AI specialized in processing imaging [61].

2) Software Failure Analysis: Software errors, software defects, or software faults often cause software failures, as shown in Fig. 4. Software errors are unintentional defects in code

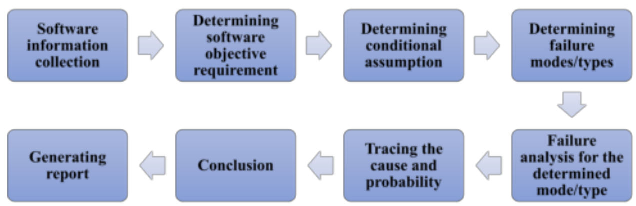

Fig. 5: The general procedure of failure analysis for xG software, whose principle is to timely, efficiently, and effectively identify software errors, software defects, software faults, and software failures, trace the very cause potentially resulting in failures, and verify whether code meets the specific objective stated in the requirements.

or script introduced by software developers. Errors can occur at each stage of a software life cycle, including requirement analysis, and designs at different levels [62]. Software errors do not necessarily result in software failures. Software defects are errors or bugs in software. Software defects pose a serious risk if they are not addressed appropriately, even if they seem normal. In the event that the defective software at risk continues to operate, it may progress to a state of software fault. However, the existence of a fault-tolerant mechanism does not guarantee that a software fault leads to software failure. Different software faults can result from the same software defect under specific conditions.

In xG, software primarily refers to emerging technologies, e.g., virtualization, AI, digital twin (DT), etc. All these software-based technologies are typical characteristics of general software, relying on data and predefined instructions to conduct training, computation, and operation; see Fig. 5.

3) System Failure Analysis: System failure emerges as a challenge in xG, constituting a highly sophisticated and interconnected system amalgamating hardware and software. The system failure of xG is not merely a conventional breakdown but a multifaceted challenge [12], [63]–[65] that demands a holistic understanding of the interplay between hardware and software. As technology continues to evolve and unfold, it is critical to comprehend and address the system failures contributing to the resilience and reliability of xG.

AI-based approaches, e.g., ML-based failure management [66], [67], excel at handling complex, data-rich failures through rapid pattern recognition and predictive analytics [67]. Yet, classical methods, e.g., quantitative network failure analysis [68], are vital for explainability and human-centric factors. The optimal strategy for failure analysis can be a hybrid approach to ensure speed and precision, where AI offers real-time detection and prioritization, while classical techniques provide root-cause validation and compliance [69], [70].

These traditional failure analysis solutions rely heavily on the expertise from multidisciplinary backgrounds to provide designated step-by-step rules for identifying potential communication failures. This could be inefficient in the face of versatile scenarios and requirements in xG cellular communication infrastructures. In contrast, AI/ML-based solutions could utilize all available types of data, e.g., historical/real-time numerical, textual, and graphic data, to comprehensively probe, analyze, and identify the very causes inducing failures, including those overlooked by human experts.

To quickly diagnose and identify specific failure types in xG network systems, a multi-faceted approach leveraging both traditional failure analysis [68] and advanced AI-based techniques [67] is essential.

- For network hardware failures, initial assessments should focus on common electrical issues, while non-destructive imaging tools (e.g., X-ray and ultrasonic waves) combined with AI [61] can efficiently detect defects.
- For network software failures, focus can be on identifying errors, defects, and faults, especially in emerging technologies, e.g., virtualization, AI, and DT [71].
- For network system-level failures, a holistic approach integrating interdisciplinary expertise and AI/ML-based data analysis is crucial [57], [72], [73].

By utilizing these tailored strategies, xG network systems are anticipated to achieve faster and more accurate failure diagnosis, enhancing overall resilience and reliability.

D. Graph Theory and Communication Networks

Modeling xG infrastructures as graphs involves representing the components of the infrastructure as nodes and links. Specifically, the nodes can be BSs or edge devices, while the links represent the wireless connections between them. Firyaguna et al. [6] proposed a proactive graph-based handover method to address the challenges of frequent and high-latency handovers in 6G integrated terrestrial and non-terrestrial networks for aircraft communications. Gharib and Ibnkahla [74] proposed a user-aware clustering method with security resource allocation using Graph Convolution Networks (GCNs) to optimize energy consumption and enhance user security satisfaction in IoT networks.

E. Centrality and Vulnerability Analysis

To identify critical nodes and weak links in the network, various network metrics such as betweenness centrality and eigenvector centrality are employed. These metrics help pinpoint the most important nodes that act as bridges in the network, as well as the links prone to failure or low reliability.

1) Identifying critical nodes and weak links using betweenness centrality: Ozaki et al. [9] proposed a multi-source multicast service chaining model that guarantees network service reliability by using betweenness centrality-based virtual network function (VNF) placement and heuristic algorithms to optimize resource allocation and minimize total cost.

2) Identifying critical nodes and weak links using eigenvector centrality: Kas et al. [75] demonstrated that using Eigenvector centrality to identify and better protect central nodes in peer-to-peer (P2P) networks can effectively prevent the catastrophic spreading of malicious content, leveraging social centrality metrics to enhance resilience against cyberattacks.

TABLE III: Interplay among software, hardware, and system failures in xG

Component	Possible Failures	Interplay and Impact
Hardware	• Malfunctioning BS • Antenna Damage • Network Component Failure • Server Breakdown	• BS failure impacting communication • Antenna issues affecting network connectivity • Network component failure causing data processing disruptions • Server breakdown leading to system downtime
Software	• Virtualization Software Errors • AI Algorithm Deficiencies • DT Inaccuracies	• Virtualization errors affecting system functions • AI algorithm issues impacting network management • DT inaccuracies affecting data processing
System Functions	• Disruptions in Communication Protocols • Network Downtime • Data Processing Errors	• Communication protocols affected by hardware failure • Network downtime due to software errors • Data processing errors resulting from system failures

F. Cascading Failures and Epidemic Models

Percolation theory and epidemic spreading models are utilized to predict how failures propagate through xG networks. These theories and models provide valuable insights into the potential pathways and extent of failure propagation, helping to enhance the resilience and reliability of the networks.

1) Using percolation theory to predict how failures propagate through xG networks: Chattopadhyay et al. [7] utilized percolation theory-based system equations to design optimal interlink patterns that maximize the robustness of interdependent networks against cascading failures triggered by randomized attacks.

2) Using epidemic spreading models to predict how failures propagate through xG networks: Li and Saad [76] utilized a dynamic message-passing method and optimal control to develop an effective optimization algorithm for mitigating network failures caused by infection-induced cascading failures in unidirectionally dependent networks.

G. Resilience Mechanisms

The most salient distinction in resilience between the current 5G and the future xG networks (including 6G) is rooted in their underlying architectural paradigms. Specifically, 5G networks predominantly depend on terrestrial infrastructures that are susceptible to localized disruptions. They address incidental failures via regular software updates and strict testing [77], [78]. In contrast, xG networks will integrate satellites, aerial platforms, and terrestrial systems into a cohesive space-air-ground architecture [79]. For this reason, xG needs to tackle more complex issues by incorporating adaptive self-healing [80], DT-based predictive maintenance [71], and modular designs for flexible upgrades [66], [67], [73], [81].

Implementing multi-path routing and adaptive topologies is an effective strategy to enhance failure tolerance in networks. These approaches allow for alternative paths and dynamic adjustments of network structures, thereby reducing the impact of failures and improving overall network reliability.

- *Multi-Path Routing for Failure Tolerance:* Madani et al. [82] proposed an adaptive multi-path routing method to enhance disaster resiliency for service function chains (SFCs) in network function virtualization (NFV) environments, reducing bandwidth and processing resource consumption compared to traditional methods.
- *Adaptive Topologies for Failure Tolerance:* Chen et al. [83] proposed an adaptive topology-aware Siamese network to address the limitations of graph convolutional networks in cross-domain fault diagnosis with small numbers of samples, effectively extracting domain-invariant features and enhancing diagnosis accuracy even with limited training data.

The multi-domain framework of xG eliminates single points of failure, enabling xG to maintain global coverage, including oceans and remote areas, and to reroute traffic adaptively during disasters through AI-driven self-healing mechanisms [80]. This represents a significant advancement of xG over 5G networks, which are geographically constrained and require manual recovery. The anticipated distributed intelligence of xG ensures continuous operations, transforming resilience from a reactive to an intrinsic and proactive capability, even in the face of catastrophic ground infrastructure failures [6].

III. Network Failures in xG Networks: A Graph-Theoretic Approach

A graph-theoretic perspective offers powerful tools to model, analyze, and predict such failures, especially within ultra-dense and heterogeneous networks. This section outlines three major categories of failures in xG networks, i.e., resource-related, security-oriented, and incidental/systemic, that are particularly relevant to this approach.

a) Resource-Related Failures: Resource exhaustion remains a critical issue in 5G and is projected to worsen in 6G. The exponential growth in data volume and service heterogeneity introduces intricate dependencies between network nodes (e.g., BS and edge servers) and links (e.g., millimeter-Wave (mmWave) and THz), which can be naturally modeled using graphs [84]–[87]. The integration of high-capacity technologies like visible light communication (VLC), mmWave, and THz further complicates dynamic resource allocation and scheduling. These technologies, while enabling high-throughput links, also increase susceptibility to failures under load or interference, particularly where scheduling conflicts or resource bottlenecks arise [88]–[90]. In a graph-theoretic view, bottlenecks can be studied through node/link centrality, congestion modeling, or flow-based optimization [91]. The challenge is heightened by 6G's intelligent and automated resource management mechanisms, which introduce complexity and new sources of failure [92], [93].

b) Security-Oriented Failures: Graph-based models also facilitate understanding of attack propagation, vulnerability surfaces, and resilience pathways. In 5G, security failures such as weak authentication protocols and physical layer

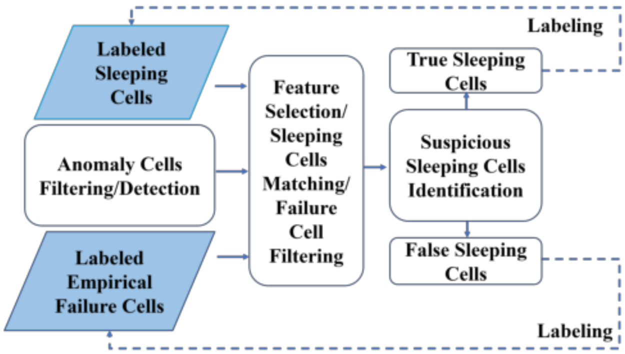

Fig. 6: The semi-supervised learning framework developed in [100] for sleeping cell detection. This frame is a multi-step framework combining anomaly detection, feature selection, classification, and clustering for sleeping cell detection. The framework uniquely utilizes unlabeled key performance indicator (KPI) data for clustering after each detection period, enriching training data for failure detection.

threats like pilot contamination attacks have already revealed structural weaknesses [94]. In 6G, the deployment of network slicing, multi-party services, and virtualized network functions expands the attack surface dramatically. Slices, modeled as subnetworks or partitions in a graph, may suffer from inter-slice leakage or isolation failures, which can be mapped to compromised nodes or bridge links [95]. Understanding these complex interdependencies requires tools from graph connectivity, community detection, and resilience metrics.

c) Incidental and Systemic Failures: Incidental failures—due to hardware aging, manufacturing flaws, or software bugs—become increasingly difficult to detect and localize as networks grow in density and complexity. In 6G systems, massive MIMO, RISs, and AI-driven orchestration add layers of opacity and coupling [96]–[99]. Hardware components may silently degrade or fail due to environmental stress, while software modules, especially AI/ML-driven components may malfunction due to data quality issues, poor model generalization, or implementation bugs [57], [72], [73], [81]. These faults may propagate across service chains or control loops, forming fault cascades that can be traced via failure propagation graphs.

Among these, node failures, whether due to hardware degradation, software faults, or targeted attacks, are particularly critical, as they can significantly disrupt network functionality. In the context of graph-theoretic modeling, nodes typically represent key elements, e.g., BSs, edge servers, or control units, whose failure may fragment the network, increase latency, or isolate users from essential services.

A. Node Failures and Their Impact on Connectivity

In xG networks, node failures, whether physical, logical, or software-driven, can severely disrupt connectivity. Nodes represent critical components, e.g., BSs, edge servers, and central controllers. When these nodes fail, the structure of the network changes, often leading to fragmented connectivity, increased delays, and degraded service quality. In this section, we explore different types of node failures and their graph-theoretic implications for network resilience; see Table IV.

1) Base Station Failures: When BSs fail due to power outages, hardware faults, or environmental conditions, the connectivity of nearby users is lost, splitting the network into disconnected segments. For instance, handover failures in satellite and terrestrial networks, e.g., those affecting high-speed rail systems, can interrupt connectivity. "Sleeping cell" failures, i.e., operational but unresponsive nodes, can go undetected without intelligent monitoring mechanisms. ML-based detection systems have been proposed to address this issue [100]; see Fig. 6. In ultra-dense networks (UDNs), the high density of BSs creates interference zones and increases the chances of fault propagation. From a graph view, more nodes and edges increase both capacity and vulnerability, especially when heterogeneous technologies, e.g., global system for mobile communications (GSM), long term evolution (LTE), wireless local area network (WLAN), are integrated [104].

2) Edge Computing Failures: Edge nodes, e.g., MEC servers, are modeled as processing hubs in network graphs. If an edge node fails, it can cause delays, data loss, or service outages, especially for time-sensitive applications like autonomous driving or remote surgery. Failures at the edge may result from hardware malfunctions, communication errors, or overloads. Ray et al. [101] introduced a dual-tiered fault recovery strategy that prioritizes applications. For critical applications, a local recovery strategy uses formal methods, in particular, stochastic multi-player games to model the interactions within the MEC environment. Probabilistic alternating-time temporal logic and a probabilistic model checker are utilized to formulate recovery strategies that encompass potential execution outcomes. In contrast, a global recovery strategy was applied to less critical applications, employing a heuristic that takes into account the likelihood of server failures to determine the optimal server for redeployment.

3) Centralized Control Failures: Centralized controllers, such as SDN controllers and core network nodes, manage network orchestration and resource allocation. The failure of these high-centrality nodes may cause widespread disruptions to network operations. For instance, Abdulqadde et al. [103] focused on distributed denial of service (DDoS) attacks targeting SDN infrastructures. They proposed a hybrid classifier combining fuzzy logic and artificial neural networks to effectively distinguish malicious packets from normal traffic.

In the network layer, 5G achieves flexible resource allocation and management through network slicing, SDN, and NFV [102], [105], [106], but still encounters resource bottlenecks when handling massive IoT device connections [107]. On the other hand, 6G utilizes space-air-ground-sea integrated network (SAGSIN) and DT technology [108] to achieve global seamless coverage [79] and enhance network resilience and reliability through intelligent management and self-healing capabilities [80]. In addition, 6G employs intent-based communication technology [109], [110] to dynamically adjust network configurations based on user needs, further improving network adaptability and reliability [80], [111]. Basu et al. [102] indicated that long-distance communication links pose a significant challenge to the resilience of 5G. There is a risk of disruption in the quality index of network latency, resulting in potential failures. In response to these vulnerabil-

TABLE IV: Different types of node failures for network resilience

Failure Type	5G/6G Technology	Cause for Failure
Base station failures	Ultra-dense small cell deployments	Operational but unresponsive BSs going into undetected sleeping states [100]
Edge computing failures	MEC environment, MEC connectivity	Dynamic and unpredictable network environment, user mobility and volatile MEC environments [101]
Centralized control failures	Network resource management, SDN infrastructures, CPS in 5G/6G networks	DDoS attacks, long-distance communication links [102], [103]

ities, SDNs enabled by virtualized software-defined networks (vSDNs) were deployed. Controller and hypervisor instances were strategically deployed to enhance reliability and security. With the advent of 6G, ensuring reliable power is crucial for achieving inherent intelligence. This necessitates the deep integration of numerous power devices to support complex scenarios [112].

A significant focus was placed on identifying and securing vulnerability nodes in power networks [113]. Chandwani *et al.* [114] investigated the effects of data integrity attacks on power electronic hardware in electric vehicle chargers. These attacks, targeting the logic and data of field programmable gate array (FPGA)-based main charger controllers, pose risks to electric vehicles and their onboard charging (OBC) systems, compromising battery functionality. 6G core networks are vulnerable to failure due to the exponential growth in their size and complexity. This substantially challenges the quality of service (QoS) and overall reliability [67], [72]. For accidental failures resulting from unstable network structures in xG networks, Li et al. [72] proposed a robust belief-weighting framework for few-shot failure prevention, leveraging abductive learning and belief rule-based structures. A similar failure data analysis for 6G core networks can be found in [67].

4) Graph Theory Application: Node failures can significantly impact network connectivity, as even a single failure may disrupt the flow of information and degrade overall performance. To address this issue, graph-theoretic means, such as identifying critical nodes using centrality measures like degree centrality and eigenvector centrality, have been employed [75], [91]. Degree centrality measures the number of direct connections a node has, while eigenvector centrality considers the influence of a node based on its connections to other high-scoring nodes. These measures help in understanding the importance of nodes within the network and can guide strategies to enhance network resilience against failures.

B. Link Failures and Traffic Congestion

Backhaul and fronthaul failures, such as fiber cuts and microwave link failures, can severely disrupt network connectivity due to physical damage, natural disasters, or other external factors. Also, load balancing and congestion collapse caused by traffic spikes and bottlenecks are critical issues that degrade performance and require effective traffic optimization strategies. Routing failures in heterogeneous networks, often due to interoperability issues, further complicate network management. To address these challenges, graph theory applications such as shortest path resilience and dynamic link adaptation via network flow optimization are employed to enhance network stability and performance; see Table V.

1) Backhaul Failures: Physical security failure encompasses various threats, including eavesdropping attacks, where malicious actors intercept data transmission, leading to severe privacy breaches and loss of sensitive information [122]. This is particularly concerning in 6G due to its anticipated high-speed, high-volume data transfer and pervasive connectivity. In addition, physical attacks [123], for instance, tampering or destruction of infrastructure, such as BSs and sensors, pose a significant threat and cause system-wide failures.

For 5G wireless backhaul, WiGig protocols, e.g., IEEE 802.11ad and 802.11ay, are considered. The susceptibility of the mmWave band to high propagation loss [124], necessitates the use of directional antennas. Yaghoubi et al. [115] emphasized the importance of considering the correlation among link failures. Overlooking this aspect may lead to failed topology designs under correlated scenarios. For coverage and capacity, 5G network operators are exploring small cells. It was found in [116] that a challenge is cost-effectively backhauling the traffic from many BSs to the core network. This small cell backhauling dilemma can be addressed with integrated access and backhaul (IAB) using 5G new radio (NR), but densifying the network raises concerns about network reliability.

2) Fronthaul Failures: In 5G, the utilization of free-space optics (FSO) within mobile fronthaul (MFH) networks presents unique risks of signal failure due to atmospheric disturbances, including turbulence and adverse weather conditions, such as cloud, fog, and rain, which can lead to significant signal attenuation and reduced communication quality [117]. The susceptibility to obstruction compounds the reliability concerns in FSO-based MFH networks. Potential prevention strategies to mitigate these risks involve integrating wireless communication as a complementary approach to enhance resilience and adopting advanced Delta-sigma modulation [125]. These strategies improve the stability of FSO links and MFH network operations.

3) Overloading Failures: Overloading failures, which can be caused by traffic spikes or excessive load on network components, are a significant concern as they may lead to degraded performance and service disruptions. In [118], a hybrid deep learning model that combines a convolutional neural network (CNN) and long short-term memory (LSTM) was proposed to address network management challenges in 5G and 6G networks. LSTM managed statistical information related to network slices, such as load balancing and error rates, while CNN managed resource allocation, network reconfiguration, and slice selection. Different conditions were investigated for

TABLE V: Different types of link failures and traffic congestion

Failure Type	5G/6G Technology	Cause for Failure
Backhaul failures	Wireless backhaul networks, small cells	Correlated link failures, cost-effective backhauling challenges [115], [116]
Fronthaul failures	FSO in MFH	Atmospheric disturbances (turbulence, cloud, fog, rain), signal obstruction [117]
Overloading failures	Hybrid deep learning model (CNN + LSTM) for network management	Network slice failures, resource allocation challenges, unknown devices [118]
Congestion collapses	Network slice, TCP-PEP, BBRv2	Slice failures, and overloads, TCP's inability to differentiate errors from congestion, satellite network jitter [92], [119]
Routing failures in heterogeneous networks	NFV-based services, centralized mobility management	Data label imbalances, model interpretability issues, suboptimal routing, scalability challenges [84], [120], [121]
Link failures in in dynamic or failure-prone environments	V2G network, LEO network	Dynamic environment variation, unpredictable space environment [115], [116]

the applicability of the model, including unknown devices, slices failing, and overloading.

4) Congestion Collapses: Congestion collapses and bottlenecks can severely degrade network performance, leading to service disruptions and reduced efficiency. A congestion collapse refers to a severe network performance degradation caused by excessive traffic overwhelming resources, leading to service disruptions and inefficiencies [126]. A bottleneck is a point in the network, where performance limitations restrict data flow, causing delays and reduced throughput. Khan et al. [92] incorporated LSTM and support vector machine (SVM) in congestion control, with effectiveness demonstrated through simulations over one week in scenarios with multiple unknown devices, slice failures, and overloads.

The inability of transmission control protocol (TCP) to differentiate between transmission errors and congestion can often result in reduced transmission rates. The jitter in satellite networks further complicates TCP's congestion control [119]. To address these issues, variants such as the TCP performance enhancing proxy (TCP-PEP) [119] have been introduced to improve network performance by employing proxies to separate the space segment. However, TCP-PEP's connection splitting approach has limitations, particularly in supporting mobility. As a remedy, the bottleneck bandwidth and round-trip propagation time version 2 (BBRv2) [119], a model-based congestion control mechanism, has been proposed, which enhances link utilization by adjusting the transmission rate based on the measured available bottleneck bandwidth and minimum Round-Trip Time (RTT).

5) Routing Failures in Heterogeneous Networks: Routing failures in heterogeneous networks, often caused by interoperability issues, can lead to significant disruptions and inefficiencies in network operations. 5G networks still face notable shortcomings, such as data label imbalances, the need for enhanced model interpretability, and the necessity for adaptive design in NFV-based services to ensure robustness against diverse failures [84], [120]. Traditional centralized mobility management systems struggle with suboptimal routing and scalability issues, particularly when managing a large number of mobile devices [121]. Moreover, the current strategies prove insufficient in handling multiple concurrent failures, which is a common scenario during disasters [116].

For 6G, these challenges will be further amplified by the integration of VLC, mmWave, and THz, which require automated resource management and introduce new failures. Leveraging the security features and network slicing capabilities of 6G is essential to strengthen the resilience of critical systems against potential interruptions [127]. The integration of AI/ML with advanced control strategies is seen as a robust approach for 6G slicing and resource management [128].

The development of adaptive and resilient slicing strategies [128], dynamic virtual resource allocation mechanisms [129], and the utilization of intelligent power grids [130] will be fundamental in managing the complexity of heterogeneous components and failure propagation in 6G. It can also be interesting to create a failure knowledge graph to reveal the complex relationships between failure types and the prediction and management of failures in 6G systems, which will require innovative methods to address the uncertainty of retrieving visual information from RF signals and the impact of image quality on the accuracy of channel prediction [88], [89].

6) Graph Theory Application: Graph theory offers powerful tools for improving the efficiency, adaptability, and resilience of modern networks. Applications such as shortest path-based routing and network flow optimization play a central role in maintaining service quality and connectivity, especially in dynamic or failure-prone environments. For example, Wan et al. [131] introduced a network flow-based temporal-spatial model to optimize the routing and scheduling of smart mobile power banks (SMPBs) for mobile charging and vehicle-to-grid (V2G) services. Their approach enhances the utilization of mobile energy storage systems in power grids by balancing demand and mobility, ultimately maximizing operational profit and energy delivery.

In a different context, Zhang et al. [132] proposed a shortest path-based resilient routing algorithm, i.e., shortest path first directional routing (SPFDR), for managing multiple node or link failures in large inclined low Earth orbit (LEO) satellite constellations. Their method maintains 100% reachability even under k-failure conditions, with minimal path stretch and linear time complexity, making it highly scalable for real-time communication scenarios. These examples demonstrate how graph-theoretic techniques can support both resilience and optimization, offering adaptable solutions for the evolving challenges of xG networks and beyond.

TABLE VI: Different types of cascading failures in large-scale networks

Failure Type	5G/6G Technology	Cause for Failure
Power Grid Dependencies	Power optical communication networks, smart grids, UWB antennas	Power failures related to connectivity and energy consumption, PD monitoring, outage failures in smart critical infrastructures, packet traffic model for power flow failures [133]–[137]
DDoS Attacks	Hierarchical communication systems	Network vulnerabilities, malicious traffic [138]
Cross-layer Disruptions	Radio backhaul systems, multipath routing, intelligent active phased array communication blocks, non-terrestrial networks, femtocell deployments	Physical obstructions, rain-induced link failures, link failures in dense deployments, rare and extreme network behaviors [96], [97], [115], [124], [139], [140]

C. Cascading Failures in Large-Scale Networks

Cascading failures in large-scale networks pose significant challenges due to their potential to cause widespread disruptions. These failures can be triggered by power grid dependencies, DDoS attacks, and cross-layer disruptions. To mitigate these risks, percolation theory is applied to model and predict critical thresholds beyond which the entire network may collapse; see Table VI.

1) Power Grid Dependencies: Power grid dependencies can significantly impact cellular networks, as both systems are interdependent. For example, communication networks require power to operate, while the power grid relies on communication networks for control and monitoring.

A power optical communication network is a specialized network that caters to power grids, and its survival is crucial for their secure and steady functioning. The analysis in [133] focused on the dependability of communication networks and calculated a collection of risk links that can identify the likelihood of power failures. The set of probabilistic risk management links resulted in three distinct shared development path solutions. Ad-hoc systems operate without infrastructure. User equipment (UE) establishes quick networking, but cannot ensure the reliability of D2D connections. 5G offers a reliable network infrastructure, with which D2D enables visualized connections, such as power grids [141].

A critical issue in 5G is cascading failures. These failures are typically initiated by a small subset of network nodes. The redistributed data flow exceeds the capacity of other links and routers, resulting in a network outage [130]. As 6G approaches, data flows may be congested due to diverse demands on network resources.

For the sake of mitigating and preventing the risks of cascading failures, a myriad of cascading failure analysis solutions have been proposed, e.g., model-based re-enactment solutions [46], [48], [142], [143], isolation-based solutions [47], and resource scheduling-based solutions [144]. In [142], the authors focused on cascading failures and proposed an invulnerability communication model to realize an optimal overall metric concerning performance, cost, and reliability. In [47], the authors proposed a general model framework to identify certain subgraphs to isolate the spread of cascading failure. In [144], the authors proposed a novel communication network model to conduct congestion control for mitigating potential cascading failures.

The reliability of power is a fundamental concern essential for the smooth functioning of critical infrastructure. Despite the intelligent application of smart grid technologies to operate and control power delivery [145], persistent challenges threaten the reliability of power communication networks. A particularly pressing issue is the recurring cascading failure in power grid networks, demanding specific attention [127], [144], [146]–[149]. As previously discussed, component failures in one or several branches lead to power delivery redistribution due to the physical laws of circuit theory [130]. The compensatory power flow can overload other branches attempting to fulfill the function of the failed branch, potentially triggering a complete power grid outage.

In future 6G, the integration of smart grids is expected to introduce novel solutions for protection, automation, and control (PAC) in smart grids. Innovative fault location, isolation, and service recovery (FLISR) functions aim to enhance the responsiveness and coordination of grid defense mechanisms. Challenges, highlighted in [134], suggest potential risks of power failures related to connectivity and energy consumption. Effective protection assets require crucial communication with FLISR functions, catering to both best-effort and ultra-reliable and low-latency communications (URLLC) services.

IoT sensors are crucial in reporting the condition of power equipment, enabling preventive maintenance and repairs before failures occur. It was found in [135] that monitoring partial discharge (PD) in a power system continuously and non-intrusively is vital for improving QoS and preventing equipment damage. PD exhibits various measurable phenomena, with RF radiation being one of them. Meanwhile, Vargas et al. [136] investigated the outage failure of 5G arising in smart critical infrastructures.

To mitigate the recurrent cascading failure in power grids, mirrors that in communication networks, a myriad of model-based failure analysis solutions have been proposed [127], [137], [146], [147], [150], [151]. These works focus on the interdependence characteristic in smart grids to unveil the potential risks for cascading failure. In [137], the authors proposed a packet traffic model, comprehensively considering data packet network failures and power flow failures to investigate the interconnection between the two types of failures. Based on their proposed model, Gao et al. [137] utilized a routing strategy to optimize the dispatching procedure for mitigating power flow failures.

In [134], the authors presented an energy-efficient route scheduler and link scheduler for 5G mobile network traffic. The problem was formulated as an integer linear problem, and solved optimally. Ilahi et al. [135] concentrated on implementing a cost-effective and minimally intrusive method as a diagnostic tool for detecting Partial Discharge. Their innovative design solution introduces an ultra-wide band (UWB) antenna designed specifically for 6G-IoT-based smart grid monitoring, operating within the frequency range of 3.02 GHz to 11.17 GHz. The antenna, featuring a cavity with five rectangular slots, demonstrates remarkable performance metrics, including a fractional bandwidth of 112.97% and a maximum gain of 1.994 dB. The paper meticulously outlines the design parameters and presents simulation results, fostering a comprehensive discussion of its implications.

2) DDoS Attacks: DDoS attacks are a form of cascading failure in hierarchical communication systems. By overwhelming network infrastructure with malicious traffic, they can degrade performance or cause total outages. Liu et al. [138] proposed a threat assessment model using Dempster-Shafer (D-S) evidence theory to evaluate the impact of DDoS attacks. Their hierarchical model integrates data acquisition, metric extraction, and weighted analysis to reflect network vulnerabilities more accurately and support proactive defense.

3) Cross-Layer Disruptions: Cross-layer disruptions become increasingly significant in 5G and 6G networks, where failures in one layer can ripple across others, leading to widespread service degradation. These disruptions span the physical, medium access control (MAC), and transport layers, and often originate from environmental factors, hardware faults, or limitations in network design. Ferreira et al. [124] analyzed how short-term and long-term blockages affect each layer. Such disruptions can cascade into upper layers, impacting scheduling, data transport, and end-to-end reliability. To address environmental vulnerabilities, e.g., rain-induced link failures, Yaghoubi et al. [115] designed a cost-effective and resilient radio backhaul system. Their solution is particularly suited for correlated failure scenarios, where large-scale disturbances affect multiple links simultaneously. Yasin et al. [139] tackled recovery in the face of link failures by proposing an adaptive multipath routing method. Their approach adjusts the number of alternative paths based on the reliability of the primary path, combining shortest-distance and link-quality metrics to reduce recovery latency and overhead.

To model failures with limited data, Baldvinsson et al. [140] developed an incremental learning generative adversarial network (IL-GAN). This model learns rare and extreme network behaviors with minimal training data, making it particularly effective for scenarios like 5G factory automation, where unusual failure modes may emerge. Nielsen *et al.* [96] focused on examining the components' accidental failures within a 6G intelligent active phased array communication block; see Fig. 7. These failures extend beyond antenna elements and can manifest in front-end circuits, e.g., power amplifiers or phase shifters, presenting a complex multidimensional challenge for fault diagnosis. Maiwada *et al.* [97] studied accidental radio link failures in dense 6G femtocell deployments, which are prone to interference and localized outages.

Service-level disruptions represent a critical dimension of cross-layer failures, particularly in systems that rely on real-time connectivity and consistent network support. These failures often affect core services such as cloud computing, edge processing, virtualization, and storage, all of which are essential to the operation of modern communication infrastructures [152]. For example, Taniguchi et al. [153] studied a counseling robot designed to support users through spoken

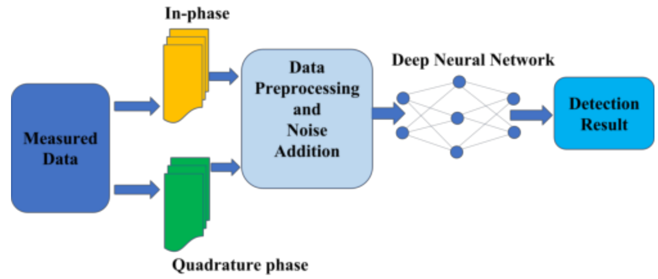

Fig. 7: Illustration of the APA Diagnosis in [96], where mathematical estimators use measured electric fields and antenna patterns, and a deep neural network (DNN)-based approach uses in-phase and quadrature (IQ) baseband signals. DNN training includes IQ signal acquisition, preprocessing, noise addition for robustness testing, and detection outcomes like the confusion matrix.

interactions. Despite its potential, the system experienced significant limitations, including word omissions, lags, and intermittent connectivity. These issues hindered its ability to monitor and engage with users effectively, demonstrating how even small disruptions in service layers can degrade user-facing applications.

In high-mobility systems, connected and autonomous vehicles (CAVs) operate at mmWave frequencies, offering high bandwidth and data rates, but are highly susceptible to line-of-sight (LoS) blockage by physical obstacles. Linsalata et al. [154] addressed this challenge by proposing the use of relays to restore broken links. In dynamic environments, conventional relays that rely on static or outdated information struggle to respond effectively, highlighting the need for more intelligent, adaptive solutions.

Service failures often stem from poor resource management, including the inability to dynamically adapt to changing demands, imbalanced service allocation, or a lack of orchestration among multiple virtualized services. These challenges are magnified in vehicle networks, where mobility and fluctuating connectivity pose additional constraints. To address these issues, Zhang et al. [155] introduced greedy boundary stateless routing (GRVAD), a fuzzy logic-based routing protocol, to overcome the limitations of traditional greedy boundary stateless routing (GPSR) in vehicular ad-hoc networks (VANETs). Using an unscented Kalman filter for predicting neighbor node locations, GRVAD improves packet delivery reliability and reduces service interruptions in mobile environments.

4) Percolation Theory Application: To better understand and anticipate the behavior of cascading failures, percolation theory offers a powerful analytical framework. It allows researchers to model how failures spread across interconnected networks and to identify critical thresholds or points at which small disruptions can lead to large-scale collapse. Sun and Qing [156] proposed a robustness analysis method for coupled networks with multiple interdependent links spanning different clusters. By applying percolation theory, they were able to pinpoint the precise conditions under which systemic failure becomes inevitable. Their approach was validated through numerical simulations, offering valuable insights for designing more resilient infrastructures that can withstand cascading effects across both communication and power domains.

D. Security-Induced Failures and Network Attacks

Security-induced failures and network attacks pose significant threats to communication systems. For example, quantum computing risks can break current cryptographic methods, and AI poisoning attacks manipulate training data to compromise AI and ML models. Moreover, SDN vulnerabilities, e.g., weak authentication, enable various attack vectors that can disrupt network operations; see Table VII.

1) Quantum Computing Risks: Quantum computing presents a fundamental threat to current cryptographic schemes by potentially breaking widely used encryption algorithms based on classical computational assumptions. As a result, xG networks face increased risks in maintaining confidentiality, integrity, and authentication. To address these challenges, Xu et al. [157] presented quantum learning-based coding that enables encoding and decoding of multiuser pilot signals using distinct subcarrier activation patterns. This strengthens uplink access security by making it harder for attackers to inject uncertainties during pilot transmission.

There remains a need for solutions ensuring key freshness and security against sophisticated attacks. Time synchronization systems in 5G are particularly vulnerable to insider threats, necessitating robust measures to prevent timing-related failures in cyber-physical systems (CPS) or IoT [165]. Security risks in industrial IoT (IIoT) are exacerbated by quantum computing, calling for innovative, lightweight, and secure authentication methods [157]. Cross-domain authentication schemes for 5G-enabled drones face high transaction failure rates and latency issues due to smart contracts [166].

2) AI Poisoning Attacks: As AI becomes increasingly integral to network control, management, and security, poisoning attacks—where adversaries manipulate training data to subvert model behavior—pose a critical threat. To address single-point authentication failures, Garzon et al. [158] proposed an authentication framework to actualize distributed identity management within 6G. Instead of relying on a trusted third party, this framework relies on individual entities to validate credentials. Zhang et al. [159] introduced a blockchain-centric framework that incorporates proof-of-strategy into spectrum allocation, reducing vulnerabilities in broadband radio services. To address single-point attack-induced failures, Fang et al. [160] delineated collaborative authentication to detect malevolent attackers in 6G networks promptly, while Chai et al. [161] leveraged Byzantine fault tolerance to speed up consensus and secure 6G-enabled Internet of Vehicles (IoV). For broader network defense, Zainudin et al. [162] introduced a blockchain-aided federated learning (FL) intrusion detection system (IDS) for securing metaverse environments. Their design uses a proof-of-authority (PoA) consensus mechanism and a hybrid client selection algorithm to improve detection accuracy and resist poisoning attempts.

3) SDN Vulnerabilities: SDN and NFV, while improving flexibility and scalability, also introduce new attack surfaces due to their centralized control logic and abstraction layers. Weak authentication, misconfiguration, and insufficient isolation between virtual functions can expose the entire control plane to compromise. Studies [163], [164] highlight how attackers can exploit SDN protocols to manipulate flow tables or launch stealthy control attacks, potentially leading to system-wide service disruptions. Mitigating these vulnerabilities requires secure SDN architectures, redundancy in controller deployment, and real-time anomaly detection.

4) Game Theory Application: By modeling the interactions between attackers and defenders as strategic games, optimal policies can be designed to enhance resilience [167]. For instance, Nash equilibrium-based models can guide attack-prevention mechanisms by predicting stable states in adversarial interactions [168]. In heterogeneous networks, evolutionary game theory has been used to manage resource allocation and network access, helping avoid cascading misallocations [169]. These game-theoretic approaches help anticipate attack strategies and adapt network responses accordingly, ensuring more robust, self-adaptive security in xG systems.

IV. Engineering Solutions for Resilient Networks

To address the challenges of network resilience, engineering solutions such as self-healing and fault-tolerant network architectures are essential. Edge computing and distributed intelligence also play a crucial role in failure mitigation. Together, these solutions form a comprehensive approach to building resilient networks capable of withstanding various failures and maintaining reliable performance.

A. Self-Healing and Fault-Tolerant Network Architectures

Self-healing and fault-tolerant network architectures are crucial for enhancing network resilience. Redundant and adaptive topologies provide multiple paths for rerouting and self-organizing capabilities. Blockchain technology is used for decentralized failure detection, leveraging smart contracts to handle faults in a secure and transparent manner. Graph neural networks (GNNs) are employed for failure prediction and topology optimization. These technologies form a comprehensive approach to building networks that can withstand and recover from various failures, ensuring reliable and efficient performance; see Table VIII.

1) AI-Driven Network Self-Repair Mechanisms: AI-driven network self-repair mechanisms, such as reinforcement learning for dynamic path reconfiguration, are increasingly adopted to enhance network resilience. These mechanisms enable networks to autonomously detect faults, analyze issues in real-time, and dynamically adjust paths to maintain performance.

Researchers have developed solutions to deal with resource depletion failures in 5G and 6G networks. In 5G, the focus has been on optimizing resource allocation and improving self-healing capabilities using predictive ML models for dynamic radio resource allocation, as well as introducing backup mechanisms to counteract failures of the service function forwarder (SFF) within the NFV environment [128], [129], [170]. Model-based simulations and isolation strategies have also been proposed to mitigate cascading failures [47], [130]. In contrast, 6G solutions anticipate the intelligent and automated management of resources, with ML-based compensation mechanisms

TABLE VII: Different types of Security-Induced Failures and Network Attacks

Failure Type	5G/6G Technology	Cause for Failure
Quantum computing risks	Quantum learning-based coding scheme, IIoT authentication methods	IIoT Security risks exacerbated by quantum computing, vulnerabilities in multiuser pilot signals [157]
AI poisoning attacks	Distributed identity management, blockchain-centric framework, collaborative authentication scheme	Single-point authentication failures, vulnerabilities in broadband radio services, malicious attackers in distributed networks, consensus security in IoV, poisoning attempts in metaverse environments [158]–[162]
SDN vulnerabilities	Secure SDN architectures, redundant controller deployment, real-time anomaly detection	Exploitation of SDN protocols, flow table manipulation, stealthy control attacks, weak authentication, misconfiguration, insufficient isolation between virtual functions [163], [164]

TABLE VIII: Different types of Self-Healing and Fault-Tolerant Network Architectures

Architecture Type	Failure Types	5G/6G Technologies	Countermeasures for Failure
AI-driven Network Self-repair Mechanisms	Resource depletion, SFF failures, cascading failures	NFV, Predictive ML models	Optimized resource allocation, dynamic radio resource allocation, backup mechanisms [128], [129], [170]
Redundant and Adaptive Topologies	High costs of extensive redundancies	Redundant topologies	Failure rate evaluation [171]
Blockchain for Decentralized Failure Detection	6G network operational failures, privacy security risks, AI failures, IoV network vulnerabilities	Explainable AI, blockchain, 6G-enabled industrial applications, elastic vehicle-based cognitive radio architecture	Decentralized trust management, BPDC, moving-target defense, distributed data aggregation [114], [122], [123], [172]
Graph Neural Networks	Security-induced failures, heterogeneous data surveillance, traffic fluctuations, link failures	6G-enabled industrial automation, software-defined LEO mega-constellations, distributed traffic engineering	Comprehensive failure analysis, resilient routing, adaptive local routing decisions [173]–[175]

to address VLC color distortion and algorithms for high-frequency spectrum resource management [176].

A range of solutions has been developed to address the issue of incidental or age-related failures in 5G. On the software front, regular updates and patches are employed to rectify known vulnerabilities and bugs [77], while more stringent testing and verification procedures are adopted to ensure software/hardware stability [78]. For 6G, solutions need to tackle more complex failure patterns and meet higher performance demands. For example, 6G networks might incorporate adaptive and self-healing technologies [66], [73], [81], enabling the networks to automatically adjust configurations or reroute traffic upon detecting failures. 6G may leverage AI/ML to predict and preempt potential failures by analyzing historical and real-time monitoring data [66], [67]. Moreover, 6G networks are expected to emphasize modularity and flexibility to facilitate the quick replacement or upgrade of hardware/software in the event of failures [72], [73].

2) Redundant and Adaptive Topologies: Redundant and adaptive topologies, featuring multiple paths for rerouting and self-organizing capabilities, enhance network resilience. To balance reliability and cost efficiency, Xu et al. [171] explored the impact of network failure rates on overall performance and optimized redundancy configuration.

A promising avenue for future research in distributed cloud frameworks, e.g., O-Cloud [177], is the enhancement of failure recovery mechanisms, e.g., through advanced network coding techniques. Network coding can be designed to create resilient data transmission and storage schemes capable of withstanding network failures or faults. The aim is to design systems that can autonomously distribute, encode, and recover data across geographically dispersed nodes in the face of node or link failures. This involves exploring both linear and nonlinear coding strategies that introduce redundancy while optimizing data dispersion and recovery efficiency. Furthermore, integrating network coding with open RAN (O-RAN), VNF, and network slicing will enable dynamic, intelligent, and centralized management of data recovery processes.

3) Blockchain for Decentralized Failure Detection: Security and access control in 6G depend on a single authentication mechanism or process in single-point authentication failures. It is impossible to prevent an attacker from gaining full access if this single authenticating node is compromised, fails, or experiences a fault. Vehicle-to-everything (V2X) applications can be developed using the IoV, with authentication ensuring a reliable vehicular environment. Chai et al. [161] found that prevalent schemes predominantly rely on centralized systems involving third parties like certificate authorities (CAs) or key generation centers (KGCs). This centralized model is susceptible to threats like DDoS and single-point failure attacks. Hence, vehicle owners hesitate to store personal information on servers due to privacy concerns.

A joint authentication approach was studied in [160], where edge devices can assist the service provider in authentication by analyzing users' received signal strength indicators (RSSIs) and movement patterns. In [159], a distributed citizens broadband radio service-blockchain model with a unique consensus technique establishes a sound consensus mechanism and safeguards spectrum allocation from single-point failures. This can decrease the administrative costs associated with dynamic access systems.

Symmetric-key authentication and key agreement (AKA) protocols, such as those developed in [178], [179], underpin security architectures, relying on the exchange of failure messages for mutual authentication in 5G. However, vulnerabilities, particularly in location confidentiality, have been identified [180]. Recent research, exemplified by [181]–[184], harnesses blockchain technology to decentralize authentica-

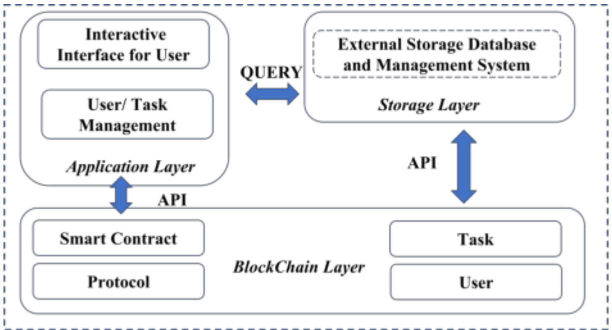

Fig. 8: The architecture of blockchain-based parallel distributed computing [122] has three layers: application layer, blockchain layer, and storage layer. Using smart contracts, the blockchain layer records tasks to prevent single-point failures. Users and tasks are managed through the application layer API.

tion in 5G NFV, IoT, and general cloud platforms. In 5G and beyond, FL within the zero touch management (ZSM) concept is vital. Nevertheless, FL faces construction failures due to poisoning attacks, posing a significant threat to slice management [185]–[187].

Despite the precision time protocol (PTP) role in achieving time synchronization in 5G, it remains susceptible to Byzantine failures from malicious insiders [165]. While recognizing the potential of 5G-enabled IoT, they noted a lack of in-depth exploration into specific failure mechanisms and called for comprehensive solutions to address reliability and security challenges. Wang et al. [172] surveyed the integration of explainable AI (XAI) in 6G networks to address the risks of opaque AI decision-making, exploring its applications and identifying key research challenges for "human-centric" network systems. While emphasizing XAI's role in enhancing transparency and addressing operational failures, the authors did not discuss the inherent risks of AI failures. Ghourab et al. [123] introduced an elastic vehicle-based cognitive radio architecture overseen by a blockchain framework that is responsive to varying circumstances. Moving-target defense technology enhances protection against cyberattacks and system failures. Blockchain technology was also integrated as part of a decentralized trust management system.

In [122], a blockchain-based privacy-aware distributed collection (BPDC) algorithm was developed for distributed data aggregation, aimed at safeguarding 6G-enabled industrial applications from internal collusion attacks while bolstering privacy security. Various attributes specify the security level of various tasks and the requisite credentials for task recipients. BPDC involved decomposing sensitive tasks and categorizing task receivers according to their security level requirements, as depicted in Fig. 8.

In a detailed exploration of attack-induced failure analysis on the IoV, Chandwani et al. [114] provided insights into potential vulnerabilities and failure scenarios. The study in [188] delved into attack-induced failure analysis in 6G-enabled IoV. As a result of attack-induced failures, rerouting was implemented, reducing response latency. In [113], a model was based on failure analysis to capture interdependence between a power network and a communication network, pinpointing the critical nodes that contributed to power communication network reliability and mitigating cascading failures.

4) Graph Neural Networks: GNNs are increasingly being used for failure prediction and topology optimization in networks. These models can effectively capture the complex relationships and dependencies within network structures, enabling more accurate failure prediction and facilitating the optimization of network topologies to enhance resilience.

For security-induced failure analysis in 6G-enabled heterogeneous data surveillance within Industrial 4.0, Mezair et al. [173] integrated LSTM, CNN, and GNN components for comprehensive failure analysis. This framework accommodates various types of heterogeneous data. Bai et al. [174] proposed a graph reinforcement learning-based resilient routing framework for software-defined LEO mega-constellations, using cascade failure theory and GNNs to enhance routing robustness and scalability, significantly improving path reliability and reducing link utilization in failure scenarios. Ye et al. [175] introduced a path-based graph neural network (PathGNN) to address performance degradation in distributed traffic engineering due to traffic fluctuations and link failures, leveraging GNN architecture for adaptive local routing decisions and improving load balancing and end-to-end delay under dynamic conditions.

B. Distributed Intelligence for Failure Mitigation

Technologies, e.g., edge computing, distributed intelligence, FL, and hybrid reinforcement learning, form a robust framework that ensures reliable network performance and minimizes the impact of failures; see Table IX.

1) MEC-Based Resource Balancing: MEC-based resource balancing enhances network efficiency by redistributing loads from over-utilized nodes to under-utilized ones. UAVs extend MEC capabilities by leveraging their mobility, cost-effectiveness, and LoS advantages. They can support UAV-mounted cloudlets [201], [202], facilitate data collection [203], and enable radio/video surveillance [204], making them a versatile solution for dynamic edge computing environments.

Complex vehicular applications demand low latency and substantial computational resources. Vehicular MEC systems address these challenges by enabling nearby vehicles and edge servers connected to BSs to share computing and storage resources [189]. However, implementing this approach is challenging due to the dynamic nature of network nodes, fluctuating computing and energy loads, and high mobility, which can lead to frequent network disruptions. By integrating MEC with cellular-V2X (C-V2X), delay-sensitive services can be efficiently delivered, mitigating the resource limitations of individual vehicles. Since MEC servers have inherent constraints in computing, storage, and communication resources, effective orchestration of multi-domain resources is essential to ensure seamless service delivery.

The study in [190] investigated training data generation for offloading decisions and evaluated the role of DTs in MEC, with a focus on minimizing download delays and service relocation costs. These systems utilize enhanced Actor-Critic learning and Lyapunov optimization to reduce offloading delays, failure rates, and operational migration overhead.

TABLE IX: Different types of Edge Computing and Distributed Intelligence Technologies for Failure Mitigation

Architecture Type	Failure Types	5G/6G Technologies	Countermeasures for Failure
MEC-based resource balancing	Resource limitations, frequent network disruptions, offloading delays, operational migration overhead, service failures	MEC, C-V2X, DT, NFV, SFC	Effective orchestration of multi-domain resources, optimized MEC offloading decisions, enhanced Actor-Critic learning, Lyapunov optimization, semi-Markov model for reliability assessment [77], [78], [189]–[191]
FL for predictive failure analysis	Privacy leakage failures, authentication failures	Network slicing, FL-empowered 5G networks	DRL framework, coordinated security orchestration architecture, proactive security measures [95], [186], [192]–[194]
Hybrid reinforcement learning for fault tolerance	Simulating rare events, cascading faults	Quantum learning, user-centric network, Industry 4.0	Efficient construction and migration of user-centric environment, dynamic knowledge graph construction, meta-heuristics, fuzzing, DRL [57], [123], [128], [140], [195]–[200]

The integration of MEC and NFV facilitates the execution of customized services structured as service functions (SFs). The study in [77] identified memory-related software aging in SFs as a critical threat that increases failure risks, significantly compromising MEC-SFC reliability. By leveraging MEC and network slicing, mobile networks can meet stringent QoS requirements while reducing the likelihood of service failures [78]. In 5G core networks, preventing service disruptions requires operators to strike a balance between cost and reliability [191]. Networks lacking redundancy may struggle to maintain consistent reliability, highlighting the need for strategic resource allocation.

The study in [77] developed a semi-Markov model to assess the transient availability and steady-state dependability of MEC-SFC services, considering complex aging, failure, and recovery dynamics. Similarly, Chantre et al. [78] explored efficient MEC and slice placement in 5G networks under a $1:N:K$ protection scheme, striving for an optimal balance between high reliability, low latency, and cost efficiency.

2) Federated Learning for Predictive Failure Analysis: FL enables decentralized AI-driven network monitoring by allowing clients to collaboratively train models without sharing raw data [205]. In AI-driven networks, personalized FL (pFL) bolsters privacy safeguards by employing differential privacy (DP) techniques [206]. These techniques introduce noise into model updates to offer customized privacy levels for each user. User-centric DP-based FL methods enable individuals to define their own privacy settings [207]–[210]. This allows for the optimization of model performance while striking a balance between privacy requirements and model utility/accuracy.

As a feature of 5G, network slicing allows multiple virtual networks to operate on a single physical infrastructure tailored to different services or customer needs [192], [193]. This granularity introduces security concerns. The existing works on FL-empowered 5G network issues investigate privacy leakage failures [194]. The joint research on FL and network slicing [95] investigated privacy leakage failures.

To address authentication failures in FL, a new approach was presented in [186], where a deep reinforcement learning (DRL) framework dynamically selects a trusted participant and employs unsupervised learning to identify malicious participants, enhancing security. In [95], coordinated security orchestration was developed based on FL to manage security operations within a slicing ecosystem centrally. This architecture preserves data privacy while enabling proactive security measures. It enhances a steady security level independent of the slicing strategy.

3) Hybrid Reinforcement Learning for Fault Tolerance: Hybrid reinforcement learning enables self-adaptive traffic rerouting, allowing networks to dynamically adjust traffic paths in response to failures and maintain connectivity and service continuity. New architectures, algorithms, and the integration of technologies, e.g., quantum learning and DTs, are interesting [123]. Creating a user-centric environment that adapts to the dynamic nature of a network of networks is crucial for connectivity and service continuity [195].

The demands of Industry 4.0 place stringent criteria on 5G systems, necessitating high reliability, availability, and low latency. However, it was noted in [140] that training reinforcement learning algorithms and simulating rare events require access to diverse failure data. A key component of cellular core networks is the control plane. The reliability of end-user applications is directly affected by the time required for cellular control plane operation [196].

Enhancing knowledge graphs with fault attributes and rule-based patterns increases their semantic expressiveness and inferential reasoning capabilities [197], [198]. Constructing and updating multi-tiered knowledge graphs involves continuously extracting fault risk information from communication data. Identifying and localizing cascading faults within the graph may use accumulated knowledge, patterns, and rules, and employ meta-heuristics, e.g., fuzzing [57], [199] or DRL [128], [200], to deduce typical structures and anomalies.

V. Standardization Efforts

This section encompasses the global initiatives to mitigate failures in 6G. Organizations like the International Telecommunications Union (ITU), Alliance for Telecommunications Industry Solutions (ATIS), and 3rd Generation Partnership Project (3GPP) have been developing standards tailored to address 6G network diagnostics and energy efficiency. The IEEE and Next Generation Mobile Networks (NGMN) Alliance have contributed to communication reliability and radio link failure, respectively. Table X compares the standardizations on failure analysis and prevention.

A. Earlier Standardization Efforts

1) ITU: In January 2020, ITU-T released standards on intelligent network analytics and diagnostics, delving into

TABLE X: Comparison of standardization activities on failure analysis and prevention

Org.	Key Contributions	Noteworthy Standards
ITU	• Standards on intelligent network analytics and diagnostics. • Mobile network energy efficiency assessment. • Common equipment management function requirements.	ITU-T standards on network failure analysis, mobile network energy efficiency, and equipment management.
ATIS	• Examination of resilience against equipment failures. • Report on “Trust, Security, and Resilience for 6G Systems.”	Resilience against equipment failures on trust, security, and resilience for 6G.
3GPP	• Standardized NF Service and User Plane Path Failures. • Release-17 with failure prediction and data analytics. • Standards on digital cellular telecommunications, NG-RAN, UE conformance, and radio transmission.	3GPP standards addressing various aspects of network failures, including Release-15, Release-16, and ongoing efforts in Release-17.
IEEE	• Standards on failure analysis for maintenance, reliability, predictions, and assessment. • Organized Asian Test Symposium and the International Symposium on Physical and Failure Analysis of Integrated Circuits.	IEEE standards covering failure analysis and significant conferences on related topics.
NGMN	• Testing framework for 5G pre-commercial networks. • Standard on 5G trust, incl. service trustworthiness failure.	NGMN contributions include a testing framework for 5G networks and a standard on 5G trust.
WWRF	• Published an outlook report on a simulation tool for mobile communication system reliability.	WWRF’s outlook report on a simulation tool for reliability in mobile communication systems.
One6G	• Publications discussing mechanisms against server failures, drawbacks of single-point failures, and the role of failure tolerance.	One6G publications on mechanisms against server failures and the role of failure tolerance in 6G.

network failure analysis. By September 2020, ITU-T standardized mobile network energy efficiency assessment, discussing failures like handover and coverage issues, and computational solution failure rates. October 2020 saw ITU-T standardize equipment management function requirements, focusing on hardware failures, e.g., transmission and link issues, and failure localization and detection strategies.

Transitioning from ITU’s efforts, the ATIS also contributed significantly. On March 22, 2022, ATIS examined resilience against equipment failures due to unintentional disruptions in critical infrastructure like power grids, telecommunications, and finance systems. On August 18, 2022, ATIS released a report on “Trust, Security, and Resilience for 6G Systems,” targeting the mitigation of single-point failures in 6G systems.

2) 3GPP: The 3GPP’s Release-15 standardized network function (NF) Service and User Plane Path Failures for enhanced detection and prevention [211]. A work item for Release-16, issued in 2018, agreed on radio link failure issues to reduce connection interruption delays [212]. Release-17, published in 2021, specified that failure prediction is a key feature of management data analytics (MDA). 3GPP TS 28.532 version 17.5.2 Release 17 standardized failure reasons, statuses, and types for generic management service configuration [213].

July 2023 saw 3GPP release standards on digital cellular telecommunications and mobile station conformance, detailing failures like initialization, tunnel, handover, synchronization, and TCP issues [214]. In January 2023, 3GPP standardized NG-RAN, focusing on positioning measurement and activation failures [215]. In the same month, standards on UE conformance were released, addressing link, handover, and connection establishment failures [216]. Another standardization covered radio transmission, reception, and resource management test cases, focusing on beam failure and recovery [217]. Release-17 work plan included policy and charging rules function (PCRF) failure and restoration. The recovery of beam failure for supporting NR sidelink CA operation was reported to be included in the upcoming Release-18 [218].

3) IEEE: The IEEE has published standards on failure analysis for maintenance, reliability, predictions, and assessment in communication support layers [219]. They have also organized significant conferences like the Asian Test Symposium (ATS) and the International Symposium on Physical and Failure Analysis of Integrated Circuits (IPFA) to discuss these issues.

4) NGMN: The NGMN Alliance has also been actively involved in addressing network failures. In July 2019, NGMN released a testing framework for 5G pre-commercial networks, discussing radio link failure in NR service connectivity. On July 26, 2021, NGMN released a standard on 5G trust, focusing on service trustworthiness failure [220].

5) Other Standardization Activities: In February 2022, the Wireless World Research Forum (WWRF) published an outlook report, mentioning their independent evaluation group (IEG)’s design of a simulation tool for mobile communication system reliability, addressing link-level and system-level failures [221]. In addition, One6G’s publications in June and November 2022 and June 2023 discussed mechanisms against server failures in 6G Vertical Use Cases, the drawbacks of single-point failures in centralized architectures, and the critical role of failure tolerance in communication systems for 6G and robotics [222]–[224].

B. Recent Efforts for AI Failures

The endogenous intelligent architecture and derivative AI-empowered, advanced solutions, e.g., semantic communication [225], are envisioned to be pervasively deployed in 6G. Countries have initiated regulatory frameworks to responsibly oversee AI development and application; see Table XI.

1) USA: In the United States, the U.S. National Institute of Standards and Technology (NIST) released a framework in January 2023 for Artificial Intelligence Risk Management to prevent various types of AI failures [35]. This initiative represents a significant step by the U.S. Department of Commerce in addressing AI risks.

2) EU: The EU has been proactive in this regard. In February 2020, the EU released a white paper on AI to standardize AI requirements and address its risks, promoting harmonized AI development [226]. By April 2021, the EU proposed regulations to harmonize AI development, focusing on privacy, security, and safety in managing critical infrastructure [36]. On June 14, 2023, the European Parliament adopted the AI Act, moving towards a consensus among EU countries [227].

3) UK: In the United Kingdom, a pro-innovation approach to AI regulation was presented to Parliament in March 2023 [228]. The UK's policy balances AI's risks and opportunities, emphasizing safety, security, robustness, accountability, governance, fairness, and contestability.

4) Canada: Canada has also been actively involved in ensuring the ethical and responsible use of AI. Since March 2019, the Canadian government has released several proposals and directives, including the Directive on Automated Decision-Making in March 2019 [229] and the Guide on the use of Generative Artificial Intelligence in September 2023 [230].

VI. Lessons Learned and Open Challenges

This section summarizes the failure analysis and mitigation lessons learned and challenges present; see Table XII.

1) Network Failures and Resilience in Interwoven Heterogeneous Networks: 6G technology is transcending the boundaries of traditional communication fields and integrating with power networks, social networks, logistics networks [231]–[234], and more to form a complex heterogeneous super-network. The high reliability and low-latency requirements of power networks drive 6G to enable precise control and rapid response in smart grids, enhancing the stability and efficiency of power systems. The diverse application scenarios of social networks demand that 6G support massive device connectivity and data interaction, prompting more flexible and scalable network architectures. Meanwhile, the real-time data transmission needs of logistics networks rely on 6G to optimize supply chain management and improve logistics efficiency and transparency. This deep integration poses significant challenges, such as network compatibility, data consistency, and resource allocation, which must be addressed through innovative research.

2) Agent-Based Approaches for Communication Network Resilience and Failure Identification: Although large language models (LLMs) hold significant application value in communication network failure identification [235] and network resilience, they still face numerous challenges in the future. On the one hand, data quality, privacy, and security issues are prominent. Communication network data is complex and voluminous, with problems such as noise, incompleteness, and inaccuracy, which affect the diagnostic accuracy of the models. On the other hand, there are shortcomings in model performance, such as model hallucination, false alarms, and lack of explainability, which make it difficult to gain user trust. In network resilience assessment, there is a lack of unified standards, and long-term effect assessment is difficult.

3) Establishing Standardized Procedure for xG Failure Analysis and Prevention: Current works often tailor solutions to specific failures within distinct application scenarios [89], [146], [236], [237]. However, there is a critical need for a comprehensive failure analysis and prevention procedure that can be universally applied across various scenarios. Tailoring these procedures to different application contexts remains a crucial open issue that needs to be addressed to ensure the reliability and efficiency of advanced communication systems.

4) Establishing xG Failure Datasets and Specifications: Establishing failure datasets and specifications is crucial for ensuring the reliability, efficiency, and security of advanced communication systems [236]. Leveraging AI in this process enhances the ability to identify, predict, and mitigate potential issues. Imbalance in available data for training, validating, and testing significantly affects AI performance in failure analysis, particularly in xG networks [238]. Negative-label (failure) data is substantially insufficient compared to positive-label (normal) operation data, creating a skewed dataset that challenges AI models to accurately detect and predict failures [239]. While recent AI approaches such as few-shot learning [240], zero-shot learning [241], and meta-learning [242] attempt to address minor unimodal sample deficiencies, deploying these methods in the complex and pluralistic 6G environment remains a formidable challenge.

5) Developing Effective Approaches for Heterogeneous Failure Data: The widespread interconnection of IoT devices in xG results in vast amounts of multi-modal and heterogeneous data, presenting significant challenges for failure detection and prevention [243]. Effective failure analysis in xG networks requires handling diverse data types from various sources, e.g., UEs, BSs, and network servers. Real-time analytics platforms must scale to handle massive data volumes and provide actionable insights for network optimization and failure mitigation. Developing comprehensive frameworks that unify these approaches will be key to maintaining the high standards of reliability and performance required for xG.

6) Complicated Cascading or Concurrent Failures: In the evolution towards xG networks, managing cascading and/or concurrent failures, e.g., within more diverse and immersive SAGSINs, is increasingly complex. Developing a failure knowledge graph for SAGSINs is essential. This can involve creating a multi-tiered graph structure representing satellite, aerial, terrestrial, and maritime networks [244], [245]. Nodes represent entities like satellites, aircraft, BSs, routers, and ocean buoys, with edges illustrating both intra- and inter-stratum connectivity.

Enhancing the knowledge graph with fault attributes and rule-based patterns increases its semantic expressiveness and inferential reasoning capabilities [197], [198]. Constructing and updating the multi-tiered knowledge graph dynamically involves continuously extracting fault risk information from communication data using techniques, such as fuzzing [57], [199] or DRL [128], [200].

7) Decentralized Failure Detection and Mitigation: Networks are anticipated to be highly distributed [238]. A critical focus area is the advancement of decentralized failure detection and mitigation mechanisms, which must operate autonomously across distributed networks to efficiently identify and diagnose failures in real time. The integration of blockchain maintains an immutable record of system states and events, essential for reliable post-mortem analysis and real-time failure identification [182]. This decentralized approach

TABLE XI: Comparison of global initiatives on AI risk management

Country/Region	Initiatives on AI Risk Management	Key Regulations and Actions
USA	NIST released a framework in January 2023 for AI Risk Management [35].	Significant step by the U.S. Department of Commerce in addressing AI risks.
EU	Released a white paper in February 2020 on AI to standardize AI requirements and address its risks [226]. Proposed regulations in April 2021 focusing on privacy, security, and safety [36]. Adopted the AI Act in June 2023 [227].	Proactive initiatives to harmonize AI development and regulate its risks, especially in managing critical infrastructure.
UK	Presented a pro-innovation approach to AI regulation to Parliament in March 2023 [228].	Safety, security, robustness, accountability, governance, fairness, contestability, and redress.
Canada	Released several proposals and directives, including the Directive on Automated Decision-Making [229] and the Guide on the use of Generative Artificial Intelligence [230].	Actively involved in ensuring the ethical and responsible use of AI, and managing AI-related risks.
Other	Global efforts with a growing awareness and proactive stance in managing AI's unique risks.	Acknowledges the importance of responsible AI development and application globally.

aligns with the distributed nature of 6G and beyond and enhances resilience against a single point of failure.

The development of lightweight algorithms and swift consensus mechanisms is crucial to ensure system efficiency and security, even under adverse network conditions [99]. These algorithms must be capable of rapidly processing vast amounts of heterogeneous data generated by IoT devices, UEs, BSs, and network servers in parallel, transforming it into actionable insights for proactive maintenance [246], [247].

8) Data Recovery in Distributed Cloud Network Failure: A promising avenue for future research in distributed cloud frameworks, e.g., O-Cloud [177], is the enhancement of failure recovery mechanisms, e.g., through advanced network coding. The aim is to design systems that can autonomously distribute, encode, and recover data across geographically dispersed nodes in the face of node/link failures.

A significant challenge will be the development of scalable and robust coding algorithms that can handle the increasing complexity and heterogeneity of distributed cloud environments. This includes addressing issues such as varying network topologies, diverse data types, and real-time processing requirements. In addition, ensuring security and privacy during the recovery process will be critical, necessitating the creation of secure coding and transmission protocols.

9) Inter-Intra Operator Authentication Collaboration: A critical challenge lies in developing a cross-carrier security center that ensures seamless data handover, service continuity during carrier transitions, and rigorous protection of user privacy. Central to this effort is a federated identity authentication system that dynamically and securely manages user identities across different network operators. New protocols must handle identity verification and authentication across multiple carriers, ensuring mutual trust and secure interactions between different network operators. Advanced cryptographic primitives such as homomorphic encryption [248], zero-knowledge proofs [249], and secure multi-party computation [250] are essential, allowing for decentralized identifiers (DIDs) [251] and verifiable credentials [252] without exposing sensitive information during cross-carrier handovers. Lattice-based cryptography [253] can offer quantum-resistant security.

10) Heightened Risks from Emerging Technologies: Emerging technologies, such as O-RAN, RISs, integrated sensing and communication (ISAC) [254], and quantum communication [255], can be prone to the risks of failure due to their complex nature. For instance, the disaggregated architecture of O-RAN increases the complexity of interoperability, raising concerns about software bugs and compatibility across multi-vendor components [177]. Hardware malfunctions, such as defects in the meta-material elements and phase shifters, can arise from environmental stressors or manufacturing flaws [38]. Control system failures might occur due to software bugs or algorithmic errors, leading to incorrect phase adjustments and suboptimal signal reflections [38].

Summary. To address these challenges, research efforts should prioritize several key directions. New physics-oriented modeling (e.g., for RISs), DT, real-time monitoring systems, and analytics tools can provide comprehensive visibility into system health and performance metrics across diverse operational environments. Adaptive fault-tolerant strategies (e.g., resilient architecture with redundancy strategies and failover mechanisms) and self-healing mechanisms can autonomously recover from failures. Furthermore, advancing quantum error correction techniques and optimizing quantum hardware reliability are imperative for the successful deployment of quantum communication technologies.

VII. Future Directions in Network Resilience

Future network resilience research is advancing through several key areas aiming to greatly improve the resilience, adaptability, and security of future network infrastructures.

A. Failure Analysis for Future 6G

Failure analysis in future 6G is anticipated to leverage AI-driven predictive models, e.g., DT-based dynamic monitoring approaches [38], [71], to address emerging challenges, such as RIS errors [38] and open RAN security vulnerabilities [256]. Cross-domain analysis will be critical for managing interdependencies between photonic, RF, and thermal systems in terahertz communications. Yet, new frameworks of failure analysis are needed for standardization and to address new semiconductor failures, e.g., GaN-based device failure [257], [258]. This multidisciplinary approach will be essential to

TABLE XII: Summary of challenges in xG failure analysis

Challenge	Current Limitations	Potential Solutions	Impacted Areas
Complex Heterogeneous Network Integration	Existing architecture limitations and security/privacy issues	Architecture innovation, AI integration, and multi-source coordinated control	Communication networks, power networks, social networks, logistics networks
Agent-Based Approaches for Network Resilience	Data quality, privacy, security, model performance, agent collaboration, and resilience assessment	Data management, model optimization, and assessment standards	Communication network failure identification, network resilience
Standardized Procedures	A lack of a comprehensive guide for xG failure analysis	The development of a step-by-step standardized procedure	Implementation, procedure design
Failure Datasets	Imbalanced data for specific failures that hamper proposed solution evaluation	The creation of standardized data sets for each xG failure scenario; exploration of few-shot learning for imbalanced data	Data collection, evaluation, AI, data balance
Heterogeneous Data	A lack of lightweight models for diverse data sources	The investigation and development of lightweight AI models for diverse data handling	Data handling, AI model design
Complicated Multiple Failures	Coordinated failures in xG that require efficient identification	The development of a specific failure knowledge graph to identify and distinguish complex failures	System coordination, failure discrimination
Decentralized Failure Detection and Mitigation	To identify and diagnose single points of failure in real-time across distributed networks; incapable of rapidly processing vast amounts of heterogeneous data	The integration of blockchain technology, the development of lightweight algorithms, and swift consensus mechanisms	Proactive maintenance
Data Recovery in Distributed Cloud Network Failure	Incapable of transacting data across geographically dispersed nodes in the face of node or link failures	The development of scalable and robust network coding algorithms	Network topology, transmission protocols
Inter-Intra Operator Authentication and Collaboration	A lack of a cross-carrier security center that ensures seamless data handover, service continuity during carrier transitions, and protection of user privacy	The creation of a federated identity authentication system and advanced cryptographic algorithms development	Authentication protocols
Risks Arising from Emerging Technologies	A lack of handling risks of failure due to the complex and innovative nature of emerging technologies	Physics-oriented modeling, adaptive fault-tolerant strategies, and advancing quantum error correction techniques	Network architecture, operational environments

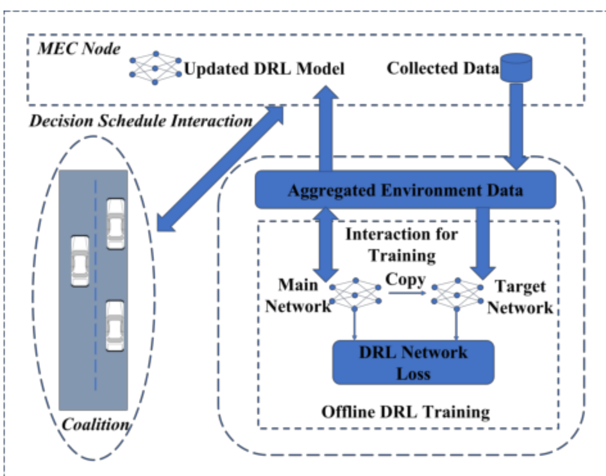

Fig. 9: Illustration of V2X channel scheduling [71]. A branch-lane vehicle is modeled as a DRL agent, which learns from environmental data obtained via a simulator. The DRL agent's state indicates traffic flow in ramps, action dictates vehicle merging decisions, and the reward is a weighted sum of average traffic speeds. The training process involves an experience replay buffer, a target network, and an evaluate network. The DRL output guides vehicles in the ramp area for efficient merging.

maintain the ultra-reliable performance of future 6G systems amid growing requirements on terabit speed and sub-millisecond latency in AI-native communication networks.

B. Resilient Digital Twin for 6G

DTs create high-fidelity virtual replicas of physical network components, and facilitate risk-free testing of emerging 6G technologies, e.g., RISs, adapting to evolving conditions while maintaining performance and reliability. While RISs offer unprecedented control over wireless environments, their deployment depends on hardware reliability. Due to their sub-wavelength metasurface structures, RISs are vulnerable to environmental factors (e.g., temperature, humidity, and mechanical stress), which can induce hardware impairments and degrade performance over time. DTs can model these vulnerabilities by mirroring the real-time state of RIS elements, using statistical or physics-based approaches.

DT integration faces two challenges: identifying applicable DT capabilities and translating them into tangible performance gains [71]. To address these, Cai et al. [71] proposed a DT and MEC-synergized architecture supporting human-machine interaction, vehicle failure detection, and traffic pattern analysis, as shown in Fig. 9. 6G is expected to enhance security through distributed identity management [158], blockchain-enabled dynamic network reconfiguration [123], and DT-based predictive failure analysis [71]. The transformative integration of AI in 6G raises security concerns; defense mechanisms against adversarial attacks are needed to ensure secure AI operations [112], [172], [259].

Robust security solutions are crucial for 6G's cross-industry deployment. Addressing sophisticated attacks, such as poisoning in FL [186], requires predictive DT capabilities combined with advanced detection algorithms [100]. Optimal model aggregation for secure network slicing [95] and health monitoring with strong authentication [260] will be essential to prevent service disruptions in Industry 4.0.

C. Quantum-Secure Networks

Quantum communication faces challenges that can lead to its failure [261]. Quantum secure direct communication (QSDC) allows for direct and confidential exchanges over a quantum channel without the need for a key agreement channel, as required in QKD protocols [41]. However, the practical implementation of QSDC is hindered by its dependence on quantum memory, the risk of immediate communication interruption due to eavesdropping, and low transmission reliability caused by significant qubit losses [41].

A recent QSDC protocol, termed Quantum-Memory-Free DL04 QSDC (QMF-DL04 QSDC) [41], incorporates dynamic joint encryption and error-control (JEEC) coding to achieve a high-accuracy secrecy capacity estimate. It enhances the robustness of the original DL04 QSDC, with improved secure information rate and communication distance. The integration of quantum sampling-based entropic uncertainty relations further fortifies the security of quantum cryptographic systems, offering a promising approach for deriving proofs of security across a variety of quantum communication scenarios [262].

Quantum communication faces challenges, such as quantum bit errors [41], decoherence [263], and environmental sensitivities [264], necessitating robust error correction mechanisms and resilient hardware designs. To address these challenges, advancing quantum error correction techniques and optimizing quantum hardware reliability are imperative for the successful deployment of quantum communication technologies [255].

D. Bio-Inspired Resilience

Biological systems, such as neural circuits and ecological networks, exhibit high resilience and adaptability through mechanisms of decentralized control, local information exchange, and emergent behavior. By translating these principles into engineered systems, network architectures can achieve improved scalability, fault tolerance, and operational efficiency. Such bio-inspired designs enable dynamic reconfiguration in response to environmental variations and system perturbations, facilitating autonomous recovery and sustained performance on complex and uncertain conditions. Wang et al. [265] introduced the artificial rabbits optimization algorithm, inspired by rabbits' survival strategies, to solve engineering optimization problems, demonstrating superior performance in benchmark functions and real-world applications like fault diagnosis. Soundarayaa and Balasubramanian [266] proposed a Komodo Mlipir algorithm-based optimal route determination mechanism to enhance QoS in VANETs by optimizing routing paths and minimizing communication overhead and latency. Dixit and Kumar Singh [267] developed a hybrid bio-inspired model called BMUDF for fault-aware UAV routing, using a combination of particle swarm optimization (PSO), genetic algorithm (GA), and grey wolf optimization (GWO) to optimize routing paths and improve QoS metrics like delay, energy consumption, and throughput.

E. Human-Centric Network Resilience

Human-centric network resilience emphasizes the adaptation to socio-technical disruptions by aligning network performance with user needs and expectations. This approach prioritizes the design of fail-safe mechanisms that preserve essential functionalities under adverse conditions, thereby enhancing system reliability, user trust, and overall quality of experience. Xu and Zhang [268] conducted a statistical analysis of China's air traffic data to investigate the resilience of air transport networks, proposing a resilience metric and analyzing the causal relationships in delay propagation networks using the Granger causality test to understand the system's recovery patterns and resilience loss. Charitoudi and Blyth [269] proposed an agent-based socio-technical approach for assessing the impact of cyber attacks on critical information infrastructures, integrating responsibilities and dependencies across supply chains into a socio-technical model to provide situational awareness and enhance cyber defense capabilities.

VIII. Conclusion

To build resilient xG infrastructures, we advocate for a network science-driven approach that integrates graph theory, AI, and decentralized architectures. Graph theory provides a foundation for modeling complex network structures and analyzing their properties, such as connectivity, robustness, and scalability, while AI, particularly ML and GNNs, enables dynamic optimization and real-time decision-making, allowing systems to adapt to changing conditions and recover quickly from failures. Decentralized architectures further enhance resilience by eliminating single points of failure and enabling distributed coordination and control, which is critical for maintaining functionality during large-scale disruptions.

Future research must focus on three key areas: failure prediction, adaptive topologies, and cyber-physical resilience. This includes developing advanced AI models to predict failures by identifying patterns in network data, designing adaptive topologies that dynamically reconfigure themselves in response to disruptions, and integrating network science with control theory to ensure the stability of physical infrastructure and cyber systems during cascading failures. By combining these approaches, we can create xG infrastructures that are resilient, adaptable, and scalable for future challenges.

Acknowledgements

This work was supported by national funds through FCT/MECI (Portuguese Foundation for Science and Technology), within the CISTER Research Unit (UIDP/UIDB/04234/2020) and under the project Intelligent Systems Associate Laboratory - LASI (LA/P/0104/2020).

References

[1] X. Chen, S. Chen, W. Ni, X. Wang, S. Zhang, S. Zhang, Y. Sun, S. Xu, and A. Jamalipour, "Optimal two-timescale configuration of mobile edge computing with mixed energy supply," *IEEE Trans. Smart Grid*, vol. 15, no. 5, pp. 4765–4778, 2024.

[2] S. Shi, J. Wang, Q. Yu *et al.*, "Research of hybrid integrated energy station based on gas turbine," in *Proc. ACPEE*, 2021.

[3] G. O. Boateng, D. Ayepah-Mensah, D. M. Doe *et al.*, "Blockchain-enabled resource trading and deep reinforcement learning-based autonomous RAN slicing in 5G," *IEEE Trans. Netw. Serv. Manag.*, vol. 19, no. 1, pp. 216–227, 2022.

[4] X. Wang, S. Garg, H. Lin *et al.*, "Heterogeneous blockchain and AI-driven hierarchical trust evaluation for 5G-enabled intelligent transportation systems," *IEEE Trans. Intell. Transp. Syst.*, vol. 24, no. 2, pp. 2074–2083, 2023.

[5] Z. Yao, W. Cheng, W. Zhang *et al.*, "Resource allocation for 5G-UAV-based emergency wireless communications," *IEEE J. Sel. Areas Commun.*, vol. 39, no. 11, pp. 3395–3410, 2021.

[6] F. Firyaguna, C.-K. Lin, H. Alshaer, and P. Harris, "Graph-based handover for future aeronautical 6g integrated terrestrial and non-terrestrial networks," in *AIAA/IEEE Digital Avionics Systems Conference*, 2024.

[7] S. Chattopadhyay, H. Dai, D. Y. Eun, and S. Hosseinalipour, "Designing optimal interlink patterns to maximize robustness of interdependent networks against cascading failures," *IEEE Transactions on Communications*, vol. 65, no. 9, p. 3847 – 3862, 2017.

[8] J. Wu, Z. Chen, Y. Zhang, Y. Xia, and X. Chen, "Sequential recovery of complex networks suffering from cascading failure blackouts," *IEEE Trans. Netw. Sci. Eng.*, vol. 7, no. 4, pp. 2997–3007, 2020.

[9] S. Ozaki, T. Sato, and E. Oki, "Multi-source multicast service chaining model guaranteeing reliability of network services," *Computer Networks*, vol. 241, 2024.

[10] C.-L. Chen, Q. P. Zheng, A. Veremyev, E. L. Pasiliao, and V. Boginski, "Failure mitigation and restoration in interdependent networks via mixed-integer optimization," *IEEE Trans. Netw. Sci. Eng.*, vol. 8, no. 2, pp. 1293–1304, 2021.

[11] J.-B. Liu, X. Zhang, J. Cao, and L. Chen, "Mean first-passage time and robustness of complex cellular mobile communication network," *IEEE Trans. Netw. Sci. Eng.*, vol. 11, no. 3, p. 3066 – 3076, 2024.

[12] L. Zhang, Y. Du, and Z. Sun, "Modeling and analysis of cascading failures in leo satellite networks," *IEEE Trans. Netw. Sci. Eng.*, vol. 11, no. 1, p. 807 – 822, 2024.

[13] A. Ghasemi and H. De Meer, "Robustness of interdependent power grid and communication networks to cascading failures," *IEEE Trans. Netw. Sci. Eng.*, vol. 10, no. 4, p. 1919 – 1930, 2023.

[14] "Katrina response: A failure to communicate," 2015. [Online]. Available: https://veoci.com/blog/katrina-response-a-failure-to-communicate/

[15] "Telecom and trust services incidents in 2020: System failures on the rise," 2021. [Online]. Available: https://www.enisa.europa.eu/news/enisa-news/telecom-trust-services-incidents-in-2020-system-failures-on-the-rise.

[16] "The power outages and telecommunication failure caused by the extreme snowstorm in the central United States," 2021. [Online]. Available: https://www.americanoversight.org/investigation/the-february-2021-texas-power-outage

[17] "Massive internet outage: Websites and apps around the world go dark," 2021. [Online]. Available: https://edition.cnn.com/2021/06/08/tech/internet-outage-fastly/index.html

[18] "The internet outage that took down several major websites seems to be fixed," 2021. [Online]. Available: https://www.cnbc.com/2021/07/22/several-major-websites-go-down-in-widespread-internet-outage.html

[19] "25% of all critical infrastructure in the us is at risk of failure due to flooding, new report finds," 2021. [Online]. Available: https://edition.cnn.com/2021/10/11/weather/infrastructure-flood-risk-climate-first-street/index.html

[20] "Google's London data center outage during heatwave caused by simultaneous failure of multiple, redundant cooling systems," 2022. [Online]. Available: https://www.datacenterdynamics.com/en/news/googles-london-data-center-outage-during-heatwave-caused-by-simultaneous-failure-of-multiple-redundant-cooling-systems/

[21] "The communication outages caused by equipment failure in Japan," 2022. [Online]. Available: https://www.theregister.com/2022/07/04/massive_telecom_outage_in_japan/

[22] "37 million T-mobile customers were hacked," 2023. [Online]. Available: https://edition.cnn.com/2023/01/19/tech/tmobile-hack/index.html

[23] "The failure for server room in Hong Kong," 2022. [Online]. Available: https://new.qq.com/rain/a/20221226A02X7200

[24] "Why cell phone service is down in Maui — and when it could be restored," 2023. [Online]. Available: https://edition.cnn.com/2023/08/09/tech/cell-service-outages-maui-fires/index.html

[25] "Telecom companies in Haiti report severed fiber optic cables," 2023. [Online]. Available: https://apnews.com/article/haiti-digicel-gangs-cables-cut-fcce6d69803d59d6b19ea02f98f5e296

[26] "The failure for nationwide bank data communication system in Japan," 2023. [Online]. Available: https://new.qq.com/rain/a/20231010A07D8500.html

[27] "Optus outage affects millions of Australians, phone and internet connections still down," 2023. [Online]. Available: https://edition.cnn.com/2023/11/07/tech/australia-optus-network-outage-intl-hnk/index.html

[28] "Breaking news! the networks of multiple us carriers have been interrupted on a large scale," 2024. [Online]. Available: https://www.cww.net.cn/article?from=timeline&id=587475

[29] "Telco tpg cops warning for triple-zero code breach," 2024. [Online]. Available: https://www.canberratimes.com.au/story/9003758/telco-tpg-cops-warning-for-triple-zero-code-breach/

[30] "Bell canada outage 'fully resolved' after widespread disruption," 2025. [Online]. Available: https://www.ctvnews.ca/business/article/bell-canada-outage-fully-resolved-after-widespread-disruption/

[31] "Why are there so many loopholes at newark airport when flights are delayed and the control tower cannot find the plane?" 2025. [Online]. Available: http://usa.people.com.cn/n1/2025/0513/c241376-40478687.html

[32] D. Basin, J. Dreier, L. Hirschi, S. Radomirovic, R. Sasse, and V. Stettler, "A formal analysis of 5G authentication," in *Proc. ACM SIGSAC*, ser. CCS '18, 2018, p. 1383–1396.

[33] A. Koutsos, "The 5G-AKA authentication protocol privacy," in *Proc. EuroS&P*, 2019, pp. 464–479.

[34] Y. Wang, Z. Zhang, and Y. Xie, "Privacy-preserving and standard-compatible AKA protocol for 5G," in *Proc. USENIX*. USENIX Association, Aug. 2021, pp. 3595–3612.

[35] "*Artificial Intelligence Risk Management Framework*, NIST AI 100-1," 2023.

[36] "*Laying down harmonised rules on artificial intelligence (artificial intelligence act) and amending certain union legislative acts*, Regulation of the European Parliament and of the Council COM (2021) 206 final," 2023.

[37] Y. Ahn, J. Kim, S. Kim, and B. Shim, "Computer vision-aided proactive mobility management for 6G terahertz communications," in *Proc. GLOBECOM*, 2023, pp. 1513–1518.

[38] A. Mondal, K. Singh, and S. Biswas, "A digital twin framework for dynamic monitoring of hardware impairment in RIS-aided networks," in *Proc. GLOBECOM*, 2023, pp. 68–73.

[39] U. Gustavsson, C. Sanchez-Pérez, T. Eriksson, F. Athley, G. Durisi, P. Landin, K. Hausmair, C. Fager, and L. Svensson, "On the impact of hardware impairments on massive MIMO," *arXiv preprint arXiv:1411.7197*, 2014, accessed: 2024-06-12.

[40] M. Wang, L. Rui, Y. Yang, Z. Gao, and X. Chen, "A blockchain-based multi-CA cross-domain authentication scheme in decentralized autonomous network," *IEEE Trans. Netw. Serv. Manag.*, vol. 19, no. 3, pp. 2664–2676, 2022.

[41] Z. Sun, L. Song, Q. Huang, L. Yin, G. Long, J. Lu, and L. Hanzo, "Toward practical quantum secure direct communication: A quantum-memory-free protocol and code design," *IEEE Trans. Commun.*, vol. 68, no. 9, pp. 5778–5792, 2020.

[42] P. Eureka, "Common fieldbus communication errors and how to fix them," 2025. [Online]. Available: https://eureka.patsnap.com/article/common-fieldbus-communication-errors-and-how-to-fix-them

[43] B. A. Miller, R. J. Shipley, R. J. Parrington *et al.*, *Failure Analysis and Prevention*. ASM International, 2021.

[44] "What is failure mode? Definition and examples." [Online]. Available: https://marketbusinessnews.com/financial-glossary/failure-mode

[45] N. Shahriar, R. Ahmed, S. R. Chowdhury, A. Khan, R. Boutaba, and J. Mitra, "Generalized recovery from node failure in virtual network embedding," *IEEE Trans. Netw. Serv. Manag.*, vol. 14, no. 2, pp. 261–274, 2017.

[46] C. Zhang, X. Xu, and H. Dui, "Analysis of network cascading failure based on the cluster aggregation in cyber-physical systems," *Reliab. Eng. Syst. Saf.*, vol. 202, p. 106963, 2020.

[47] F. Kaiser, V. Latora, and D. Witthaut, "Network isolators inhibit failure spreading in complex networks," *Nat. Commun.*, vol. 12, no. 1, p. 3143, 2021.

[48] A. Prakash and S. Kar, "Network failure assessment based on graph signal processing," in *Proc. ANTS*, 2020, pp. 1–6.

[49] I. Lin, O. Yağan, and C. Joe-Wong, "Dynamic coupling strategy for interdependent network systems against cascading failures," *IEEE Trans. Netw. Sci. Eng.*, vol. 10, no. 4, pp. 2265–2282, 2023.

[50] A. Sturaro, S. Silvestri, M. Conti, and S. Das, "A realistic model for failure propagation in interdependent cyber-physical systems," *IEEE Trans. Netw. Sci. Eng.*, vol. 7, no. 2, pp. 817–831, 2018.

[51] L. Chen, S. Gorbachev, D. Yue, C. Dou, X. Xie, S. Li, N. Zhao, and T. Zhang, "Impact of cascading failure on power distribution and data transmission in cyber-physical power systems," *IEEE Trans. Netw. Sci. Eng.*, vol. 11, no. 2, p. 1580 – 1590, 2024.

[52] S. N. Edib, Y. Lin, V. M. Vokkarane, and X. Fan, "A cross-domain optimization framework of pmu and communication placement for multidomain resiliency and cost reduction," *IEEE Internet Things J.*, vol. 10, no. 9, pp. 7490–7504, 2023.

[53] L. U. Khan, W. Saad, D. Niyato *et al.*, "Digital-twin-enabled 6G: Vision, architectural trends, and future directions," *IEEE Commun. Mag.*, vol. 60, no. 1, pp. 74–80, 2022.

[54] Q. Cui, Z. Zhu, W. Ni *et al.*, "Edge-intelligence-empowered, unified authentication and trust evaluation for heterogeneous beyond 5G systems," *IEEE Wirel. Commun.*, vol. 28, no. 2, pp. 78–85, 2021.

[55] S. Bi, K. Li, S. Hu, W. Ni, C. Wang, and X. Wang, "Detection and mitigation of position spoofing attacks on cooperative uav swarm formations," *IEEE Trans. Info. Forensics Secur.*, vol. 19, pp. 1883–1895, 2024.

[56] W. Son, M. Oh, H. Yu, and B. C. Jung, "Physical-layer security in MU-MISO downlink networks against potential eavesdroppers," *Digit. Commu. Netw.*, vol. 11, no. 2, pp. 424–431, 2025.

[57] S. Gupta, A. Mishra, and M. Chawla, "Analysis and recommendation of common fault and failure in software development systems," in *Proc. SCOPES*, 2016, pp. 1730–1734.

[58] Z. Shuai, W. Zhangzhao, Q. Baojun *et al.*, "Destructive physical analysis methods of flip chip packaging devices for high reliability," in *Proc. ICEPT*, 2021.

[59] Y. Sin, Z. Lingley, M. Brodie, N. Presser, S. Moss, J. Kirch, C. Chang, C. Boyle, L. Mawst, D. Botez, D. Lindberg, and T. Earles, "Destructive physical analysis of degraded quantum cascade lasers," vol. 9382, 2015.

[60] D. Lin, "Application of three-dimensional x-ray microscopy in failure analysis for sealed relay," in *Proc. ICEPT*, 2018, pp. 1351–1354.

[61] Y. Zhao, M. Xiao, H. Lv *et al.*, "Research on scanning acoustic image defects detection of integrated circuits based on YOLOX," in *Proc. ICEPT*, 2022.

[62] H. K. Apat and B. Sahoo, "LESP: A fault-aware Internet of Things service placement in fog computing," *Sustain. Comput.*, vol. 46, p. 101097, 2025.

[63] W. Zhu and J. V. Milanović, "Cyber-physical system failure analysis based on complex network theory," in *Proc. EUROCON*, 2017, pp. 571–575.

[64] S. Fei, Z. Yan, H. Xie, and G. Liu, "Sec-e2e: End-to-end communication security in ls-hetnets based on blockchain," *IEEE Trans. Netw. Sci. Eng.*, vol. 11, no. 1, p. 761 – 778, 2024.

[65] Z. Jia, Y. Cao, L. He, G. Li, F. Zhou, Q. Wu, and Z. Han, "Nfv-enabled service recovery in space–air–ground integrated networks: A matching game-based approach," *IEEE Trans. Netw. Sci. Eng.*, vol. 12, no. 3, p. 1732 – 1744, 2025.

[66] F. B. Mismar and J. Hoydis, "Unsupervised learning in next-generation networks: Real-time performance self-diagnosis," *IEEE Commun. Lett.*, vol. 25, no. 10, pp. 3330–3334, 2021.

[67] Y. Wang, Y. Ruan, and Y. Tang, "Intelligent fault diagnosis method for mobile cellular networks," in *Proc. IEEE Globecom Workshops*, 2021.

[68] D. Hongyan, Z. Chi, and X. Xin, "Failure analysis of network nodes and edges in scale-free networks," *Commun. Stat. - Theor. M.*, vol. 49, no. 15, p. 3635 – 3649, 2020.

[69] M. Mokhtarzadeh, J. Rodríguez-Echeverría, I. Semanjski, and S. Gautama, "Hybrid intelligence failure analysis for industry 4.0: A literature review and future prospective," *J. Intell. Manuf.*, vol. 36, no. 4, pp. 2309–2334, 2025.

[70] N. Dolle, "Comparison of classical and AI-based decision-making methodologies," in *Proc. Reliability and Statistics in Transportation and Communication*, 2024.

[71] G. Cai, B. Fan, Y. Dong, T. Li, Y. Wu, and Y. Zhang, "Task-efficiency oriented V2X communications: Digital twin meets mobile edge computing," *IEEE Wireless Commun.*, vol. 31, no. 2, pp. 149–155, 2024.

[72] J. Li, K. Zhu, and Y. Zhang, "Knowledge-assisted few-shot fault diagnosis in cellular networks," in *Proc. IEEE GLOBECOM*, 2022.

[73] A. Shaghaghi, A. Zakeri, N. Mokari *et al.*, "Proactive and AoI-aware failure recovery for stateful NFV-enabled zero-touch 6G networks: Model-free DRL approach," *IEEE Trans. Netw. Serv. Manag.*, vol. 19, no. 1, pp. 437–451, 2022.

[74] A. Gharib and M. Ibnkahla, "User security-oriented information-centric iot nodes clustering with graph convolution networks," *IEEE Internet of Things Journal*, vol. 11, no. 5, p. 8311 – 8326, 2024.

[75] M. Kas, L. Richard Carley, and K. M. Carley, "Monitoring social centrality for peer-to-peer network protection," *IEEE Communications Magazine*, vol. 51, no. 12, p. 155 – 161, 2013.

[76] B. Li and D. Saad, "Infection-induced cascading failures – impact and mitigation," *Communications Physics*, vol. 7, no. 1, 2024.

[77] J. Bai, X. Chang, F. Machida *et al.*, "Impact of service function aging on the dependability for MEC service function chain," *IEEE Trans. Dependable Secure Comput.*, vol. 20, no. 4, pp. 2811–2824, 2023.

[78] H. D. Chantre and N. L. S. D. Fonseca, "Design of 5G MEC-based networks with 1:N:K protection scheme," *IEEE Trans. Netw. Serv. Manag.*, vol. 19, no. 3, pp. 2478–2491, 2022.

[79] M. Matracia, N. Saeed, M. A. Kishk, and M.-S. Alouini, "Post-disaster communications: Enabling technologies, architectures, and open challenges," *IEEE Open Journal of the Communications Society*, vol. 3, p. 1177 – 1205, 2022.

[80] L. Velasco, M. Signorelli, O. G. De Dios, C. Papagianni, R. Bifulco, J. J. V. Olmos, S. Pryor, G. Carrozzo, J. Schulz-Zander, M. Bennis, R. Martinez, F. Cugini, C. Salvadori, V. Lefebvre, L. Valcarenghi, and M. Ruiz, "End-to-end intent-based networking," *IEEE Communications Magazine*, vol. 59, no. 10, p. 106 – 112, 2021.

[81] B. Shayesteh, C. Fu, A. Ebrahimzadeh *et al.*, "Auto-adaptive fault prediction system for edge cloud environments in the presence of concept drift," in *Proc. IEEE IC2E*, 2021.

[82] M. A. Madani, F. Zhou, and A. Meddahi, "Deploying disaster-resilient service function chains using adaptive multi-path routing," *IEEE Trans. Netw. Serv. Manag.*, 2024.

[83] Z. Chen, J. Ji, K. Chen, Q. Ni, X. Ding, and W. Yu, "Adaptive topology-aware siamese network for cross-domain fault diagnosis with small samples," *IEEE Sensors Journal*, vol. 24, no. 15, p. 24438 – 24451, 2024.

[84] M. A. Islam, H. Siddique, W. Zhang *et al.*, "A deep neural network-based communication failure prediction scheme in 5G RAN," *IEEE Trans. Netw. Serv. Manag.*, vol. 20, no. 2, pp. 1140–1152, 2023.

[85] H. H. Esmat, B. Lorenzo, and W. Shi, "Toward resilient network slicing for satellite-terrestrial edge computing IoT," *IEEE Internet Things J.*, vol. 10, no. 16, pp. 14 621–14 645, 2023.

[86] E. E. Haber, H. A. Alameddine, C. Assi *et al.*, "UAV-aided ultra-reliable low-latency computation offloading in future IoT networks," *IEEE Trans. Commun.*, vol. 69, no. 10, pp. 6838–6851, 2021.

[87] G. Abbas, A. U. Khan, Z. H. Abbas *et al.*, "FMCPR: Flexible multiparameter-based channel prediction and ranking for CR-enabled massive IoT," *IEEE Internet Things J.*, vol. 9, no. 10, pp. 7151–7165, 2022.

[88] M. Choi, T. Kim, J. p. Lee *et al.*, "An empirical study on root cause analysis and prediction of network failure using deep learning," in *Proc. ICTC*, 2021, pp. 741–746.

[89] T. Nishio, Y. Koda, J. Park *et al.*, "When wireless communications meet computer vision in beyond 5G," *IEEE Communications Standards Magazine*, vol. 5, no. 2, pp. 76–83, 2021.

[90] G. Manogaran, T. Baabdullah, D. B. Rawat *et al.*, "AI-assisted service virtualization and flow management framework for 6G-enabled cloud-software-defined network-based IoT," *IEEE Internet Things J.*, vol. 9, no. 16, pp. 14 644–14 654, 2022.

[91] L. Wang, Z. Li, C. Wang, J. Li, M. Hu, W. Liu, and K. Peng, "Obstacle-aware multicast routing algorithm for large-scale leo constellations," *IEEE Trans. Netw. Sci. Eng.*, vol. 11, no. 5, p. 4551 – 4563, 2024.

[92] S. Khan, A. Hussain, S. Nazir *et al.*, "Efficient and reliable hybrid deep learning-enabled model for congestion control in 5G/6G networks," *Comput. Commun.*, vol. 182, pp. 31–40, 2022.

[93] S. Majumdar, R. Trivisonno, and G. Carle, "Scalability of distributed intelligence architecture for 6G network automation," in *Proc. IEEE ICC*, 2022, pp. 2321–2326.

[94] C. Shahriar, M. La Pan, M. Lichtman *et al.*, "Phy-layer resiliency in ofdm communications: A tutorial," *IEEE Commun. Surv. Tut.*, vol. 17, no. 1, pp. 292–314, 2014.
[95] S. Wijethilaka and M. Liyanage, "A federated learning approach for improving security in network slicing," in *Proc. IEEE GLOBECOM*, 2022.
[96] M. H. Nielsen, Y. Zhang, C. Xue *et al.*, "Robust and efficient fault diagnosis of mm-Wave active phased arrays using baseband signal," *IEEE Trans. Antennas Propagat.*, vol. 70, no. 7, pp. 5044–5053, 2022.
[97] U. D. Maiwada, K. Usman Danyaro, and A. B. Sarlan, "An improved mobility state detection mechanism for femtocells in LTE networks," in *Proc. DASA*, 2022.
[98] A. L. P. Fernandes, D. D. Souza, D. B. Da Costa *et al.*, "Cell-free massive MIMO with segmented fronthaul: Reliability and protection aspects," *IEEE Wireless Commun. Lett.*, vol. 11, no. 8, pp. 1580–1584, 2022.
[99] L. Shi, C. Wang, X. Cai *et al.*, "GaAs RF Amplifier Field Failure Analysis and Reliability Prediction in 5G AAU System," in *Proc. IPFA*, 2022.
[100] Z. Ming, X. Li, C. Sun *et al.*, "Sleeping cell detection for resiliency enhancements in 5G/B5G mobile edge-cloud computing networks," *ACM Trans. Sens. Netw.*, vol. 18, no. 3, 2022.
[101] K. Ray and A. Banerjee, "Prioritized fault recovery strategies for multi-access edge computing using probabilistic model checking," *IEEE Trans. Dependable Secure Comput.*, vol. 20, no. 1, pp. 797–812, 2023.
[102] D. Basu, A. Jain, U. Ghosh *et al.*, "A reverse path-flow mechanism for latency aware controller placement in vSDN enabled 5G network," *IEEE Trans. Ind. Informat.*, vol. 17, no. 10, pp. 6885–6893, 2021.
[103] I. H. Abdulqadder, D. Zou, I. T. Aziz *et al.*, "Deployment of robust security scheme in SDN based 5G network over NFV enabled cloud environment," *IEEE Trans. Emerg. Topics Comput.*, vol. 9, no. 2, pp. 866–877, 2021.
[104] W. Tang, J. Zhao, J. Xue, T. Ma, and H. Zhou, "A grasshopper optimization algorithm for fault diagnosis in ultra-dense LEO satellite networks," in *Proc. ICCC*, 2022, pp. 1080–1084.
[105] Q. Zhang, O. Ayoub, J. Wu, F. Musumeci, G. Li, and M. Tornatore, "Progressive slice recovery with guaranteed slice connectivity after massive failures," *IEEE/ACM Transactions on Networking*, vol. 30, no. 2, p. 826 – 839, 2022.
[106] R. Jhaveri, S. Ramani, G. Srivastava, T. Gadekallu, and V. Aggarwal, "Fault-resilience for bandwidth management in industrial software-defined networks," *IEEE Trans. Netw. Sci. Eng.*, vol. 8, no. 4, pp. 3129–3139, 2021.
[107] L. De Simone, M. Di Mauro, R. Natella, and F. Postiglione, "Performance and availability challenges in designing resilient 5G architectures," *IEEE Trans. Netw. Serv. Manag.*, vol. 21, no. 5, p. 5291 – 5303, 2024.
[108] A. Schosser, F. Burmeister, P. Schulz, M. D. Khursheed, S. Ma, and G. Fettweis, "Advancing spectrum anomaly detection through digital twins," *IEEE Commun. Mag.*, 2024.
[109] S. Zou, M. Liwang, B. Wu, W. Wu, Y. Sun, and W. Ni, "Intent-oriented network slicing with hypergraphs," *IEEE Netw.*, vol. 39, no. 4, pp. 202–210, 2025.
[110] D. Wang, S. Zou, M. Liwang, W. Ni, and X. Wang, "Intent-driven cognitive xDFC bridge in endogenous intelligent IIoT: A systematic review and S^2 croft architecture with Bayesian-CRO-fuzzy synergy," *IEEE Trans. Netw. Sci. Engi.*, pp. 1–17, 2025, early access.
[111] M. Farhoudi, M. Shokrnezhad, T. Taleb, R. Li, and J. Song, "Discovery of 6G services and resources in edge-cloud-continuum," *IEEE Network*, p. 1–1, 2024.
[112] Y. Wang, C. Feng, Y. Li *et al.*, "Expected failure method and its analysis for safety evaluation in a cyber-physical power system," *IEEE Access*, vol. 10, pp. 133 348–133 356, 2022.
[113] R. Atat, M. Ismail, S. S. Refaat *et al.*, "Cascading failure vulnerability analysis in interdependent power communication networks," *IEEE Syst. J.*, vol. 16, no. 3, pp. 3500–3511, 2022.
[114] A. Chandwani, S. Dey, and A. Mallik, "Cybersecurity of onboard charging systems for electric vehicles-review, challenges and countermeasures," *IEEE Access*, vol. 8, pp. 226 982–226 998, 2020.
[115] F. Yaghoubi, M. Furdek, A. Rostami *et al.*, "Design and reliability performance of wireless backhaul networks under weather-induced correlated failures," *IEEE Trans. Rel.*, vol. 71, no. 2, pp. 616–629, 2022.
[116] M. Y. Selim and A. E. Kamal, "Self-backhauling failure mitigation using 5G new radio," *Comput. Netw.*, vol. 217, 2022.
[117] K. K. Soumya and J. Zacharias, "FSO challenges and solutions at 5G networks - a review," in *Proc. ICCC*, 2023, pp. 1–5.
[118] S. Khan, S. Khan, Y. Ali *et al.*, "Highly accurate and reliable wireless network slicing in 5th generation networks: A hybrid deep learning approach," *J. Netw. Comput. Appl.*, vol. 30, no. 2, 2022.
[119] H. He, Y. Hou, J. Yang, X. Jiang, S. Chen, and L. Hanzo, "Towards reliable space-ground integrated networks: From system-level design to implementation," *IEEE Netw.*, vol. 37, no. 5, pp. 154–161, 2023.
[120] D. Zheng, G. Shen, Y. Li *et al.*, "Service function chaining and embedding with heterogeneous fault tolerance in edge networks," *IEEE Trans. Netw. Serv. Manag.*, vol. 20, no. 3, pp. 2157–2171, 2022.
[121] M. K. Hasan, S. Islam, I. Memon *et al.*, "A novel resource oriented DMA framework for internet of medical things devices in 5G network," *IEEE Trans. Ind. Informat.*, vol. 18, no. 12, pp. 8895–8904, 2022.
[122] H. Lin, S. Garg, J. Hu *et al.*, "A blockchain-based secure data aggregation strategy using sixth generation enabled Network-in-Box for industrial applications," *IEEE Trans. Ind. Informat.*, vol. 17, no. 10, pp. 7204–7212, 2021.
[123] E. M. Ghourab, L. Bariah, S. Muhaidat *et al.*, "Blockchain-enabled moving target defense for secure CR networks," in *Proc. ITC*, 2022.
[124] T. Ferreira, A. Figueiredo, D. Raposo *et al.*, "Millimeter-wave feasibility in 5G backhaul: A cross-layer analysis of blockage impact," *IEEE Access*, vol. 11, pp. 5178–5192, 2023.
[125] X. Ao, Q. Fan, L. Zhong, T. Mei, Y. Wang, Q. Yang, X. Dai, C. Liu, M. Cheng, L. Deng, and D. Liu, "Real-time experimental demonstration of hybrid FSO/wireless transmission based on coherent detection and Delta-Sigma modulation," *IEEE Photonics J.*, vol. 14, no. 6, pp. 1–8, 2022.
[126] T. Zhu, X. Yang, Z. Ma, J. Gao, and J. Wu, "Can a bottleneck capacity enhancement policy postpone infrastructure network collapse?" *Transport Policy*, vol. 163, pp. 1–13, 2025.
[127] Y. Wang, G. Bai, Y.-A. Zhang *et al.*, "Cascading failure analysis and robustness assessment of the operational system and electric power system based on dependent network," in *Proc. PHM*, 2022, pp. 1–8.
[128] G. Dandachi, S. Cerf, Y. Hadjadj-Aoul *et al.*, "A robust control-theory-based exploration strategy in deep reinforcement learning for virtual network embedding," *Comput. Netw.*, vol. 218, 2022.
[129] H. Cao, H. Zhao, D. X. Luo *et al.*, "Dynamic virtual resource allocation mechanism for survivable services in emerging NFV-enabled vehicular networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 11, pp. 22 492–22 504, 2022.
[130] M. Z. Islam, Y. Lin, V. M. Vokkarane *et al.*, "Cyber-physical cascading failure and resilience of power grid: A comprehensive review," *Frontiers in Energy Research*, vol. 11, 2023.
[131] Y. Wan, Y. Hu, X. Liu, Q. Zhou, N. Wang, Y. Wang, and Z. Chen, "Routing and scheduling of smart mobile power banks for mobile charging and vehicle-to-grid services," *IEEE Transactions on Transportation Electrification*, 2025.
[132] Y. Zhang, K. Zhao, and W. Li, "A resilient routing algorithm for handling k-link/node failure in inclined LEO megaconstellations," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 60, no. 4, p. 4876 – 4886, 2024.
[133] R. Wu, X. Liu, W. Huang *et al.*, "Calculation and analysis of communication network survivability in SCADA communication system," in *Proc. IEEE IMCEC*, 2022.
[134] M. O. Nait Belaid, V. Audebert, B. Deneuville *et al.*, "SD-RAN based approach for smart grid critical traffic routing and scheduling in 5G mobile networks," in *Proc. IEEE GLOBECOM*, 2022.
[135] F. Ilahi, S. Dutta, M. M. Hasan *et al.*, "Development of a novel UWB antenna for 6G-IoT based smart grid device monitoring system," in *Proc. GECOST*, 2021.
[136] P. Vargas and I. Tien, "Impacts of 5G on cyber-physical risks for interdependent connected smart critical infrastructure systems," *Int. J. Crit. Infrastruct. Prot.*, vol. 42, 2023.
[137] X. Gao, M. Peng, and C. K. Tse, "Cascading failure analysis of cyber–physical power systems considering routing strategy," *IEEE Trans. Circuits Syst. II Express Briefs*, vol. 70, no. 1, pp. 136–140, 2023.
[138] L. Zihao, Z. Bin, Z. Ning, and L. Lixun, "Hierarchical network threat situation assessment method for DDoS based on d-s evidence theory," in *2017 IEEE International Conference on Intelligence and Security Informatics: Security and Big Data, ISI 2017*, 2017, p. 49 – 53.
[139] Q. Yasin, Z. Iqbal, M. A. Khan *et al.*, "Reliable multipath flow for link failure recovery in 5G networks using SDN paradigm," *Inf. Technol. Control.*, vol. 51, no. 1, pp. 5–17, 2022.
[140] J. R. Baldvinsson, M. Ganjalizadeh, A. Alabbasi *et al.*, "IL-GAN: Rare sample generation via incremental learning in GANs," in *Proc. IEEE GLOBECOM*, 2022.

[141] X. Xu, X. Deng, B. Li *et al.*, "An analysis of 5G D2D network in power grids' automation," in *Proc. ICCIS*, 2022.
[142] Y. Qu, M. Gao, Y. Chen *et al.*, "An analysis of the invulnerability for communication networks based on cascading failure model," in *Proc. ICRIS*, 2020, pp. 154–157.
[143] S. Gao, X. Ma, F. Ma *et al.*, "Cascading failure analysis of uniform double-layer hyper-networks based on the couple map lattice model," in *Proc. IEEE HPCC/DSS/SmartCity/DependSys*, 2022, pp. 1449–1456.
[144] X. Li and T. S. Cheng, "Cascading failure analysis of cyber-physical power systems under communication congestion," in *Proc. ICCSI*, 2021, pp. 1–6.
[145] X. Chen, H. Wen, W. Ni *et al.*, "Distributed online optimization of edge computing with mixed power supply of renewable energy and smart grid," *IEEE Trans. Commun.*, vol. 70, no. 1, pp. 389–403, 2022.
[146] A. Salehpour, I. Al-Anbagi, K.-C. Yow *et al.*, "A realistic failure propagation model for smart grid networks," in *Proc. icSmartGrid*, 2022, pp. 66–71.
[147] Y. Chen, Y. Li, W. Li *et al.*, "Cascading failure analysis of cyber physical power system with multiple interdependency and control threshold," *IEEE Access*, vol. 6, pp. 39 353–39 362, 2018.
[148] Q. Lin and H. Wu, "Interconnect reliability modeling and index failure analysis for power amplifier," in *Proc. ITNEC*, 2017, pp. 1188–1191.
[149] W. Zhu and J. V. Milanović, "Cyber-physical system failure analysis based on complex network theory," in *Proc. IEEE EUROCON ST*, 2017, pp. 571–575.
[150] J. Huang, Q. Wang, Z. Sang *et al.*, "The dc power flow model based analysis on failure of power grid communication network," in *Proc. IFEEA*, 2022, pp. 683–686.
[151] A. Salehpour, I. Al-Anbagi, K.-C. Yow *et al.*, "Modeling cascading failures in coupled smart grid networks," *IEEE Access*, vol. 10, pp. 81 054–81 070, 2022.
[152] L. Duan, H. Huang, C. Li, W. Ni, and B. Cheng, "A novel cross-chain hierarchical federated learning framework for enhancing service security and communication efficiency," *IEEE Trans. Serv. Comput.*, vol. 18, no. 3, pp. 1199–1212, 2025.
[153] Y. Taniguchi, Y. Ikegami, H. Fujikawa *et al.*, "Counseling (ro)bot as a use case for 5G/6G," *Complex and Intell. Syst.*, vol. 8, no. 5, pp. 3899–3917, 2022.
[154] F. Linsalata, S. Mura, M. Mizmizi *et al.*, "LoS-map construction for proactive relay of opportunity selection in 6G V2X systems," *IEEE Trans. Veh. Technol.*, vol. 72, no. 3, pp. 3864–3878, 2022.
[155] D.-G. Zhang, J.-X. Wang, J. Zhang, T. Zhang, C. Yang, and K.-W. Jiang, "A new method of fuzzy multicriteria routing in vehicle ad hoc network," *IEEE Transactions on Computational Social Systems*, vol. 10, no. 6, p. 3181 – 3193, 2023.
[156] N. Sun and T. Qing, "Robustness analysis of coupled networks with multiple dependent links from different clusters," *International Journal of Nonlinear Science*, vol. 37, no. 1, p. 42 – 46, 2024.
[157] D. Xu, K. Yu, and J. A. Ritcey, "Cross-layer device authentication with quantum encryption for 5G enabled IIoT in Industry 4.0," *IEEE Trans. Ind. Informat.*, vol. 18, no. 9, pp. 6368–6378, 2022.
[158] S. R. Garzon, H. Yildiz, and A. Kupper, "Towards decentralized identity management in multi-stakeholder 6G networks," in *Proc. 6GNet*, 2022.
[159] H. Zhang, S. Leng, and H. Chai, "A blockchain enhanced dynamic spectrum sharing model based on proof-of-strategy," in *Proc. IEEE ICC*, 2020.
[160] H. Fang, Z. Xiao, X. Wang *et al.*, "Collaborative authentication for 6G networks: An edge intelligence based autonomous approach," *IEEE Trans. Inf. Forensics Secur.*, vol. 18, pp. 2091–2103, 2023.
[161] H. Chai, S. Leng, J. He *et al.*, "CyberChain: Cybertwin empowered blockchain for lightweight and privacy-preserving authentication in internet of vehicles," *IEEE Trans. Veh. Technol.*, vol. 71, no. 5, pp. 4620–4631, 2022.
[162] A. Zainudin, M. A. P. Putra, R. N. Alief, R. Akter, D.-S. Kim, and J.-M. Lee, "Blockchain-inspired collaborative cyber-attacks detection for securing metaverse," *IEEE Internet of Things Journal*, vol. 11, no. 10, p. 18221 – 18236, 2024.
[163] F. Ezzeddine, O. Ayoub, D. Andreoletti *et al.*, "Vertical split learning-based identification and explainable deep learning-based localization of failures in multi-domain NFV systems," in *Proc. NFV-SDN*, 2023, pp. 46–52.
[164] Z. Jia, Y. Cao, L. He, G. Li, F. Zhou, Q. Wu, and Z. Han, "Nfv-enabled service recovery in space-air-ground integrated networks: A matching game based approach," *IEEE Trans. Netw. Sci. Eng.*, 2025.
[165] S. Shi, Y. Xiao, C. Du *et al.*, "MS-PTP: Protecting network timing from byzantine attacks," in *Proc. ACM WiSec*, 2023.
[166] C. Feng, B. Liu, Z. Guo *et al.*, "Blockchain-based cross-domain authentication for intelligent 5G-enabled internet of drones," *IEEE Internet Things J.*, vol. 9, no. 8, pp. 6224–6238, 2022.
[167] W. Tang, E. Liu, W. Ni, X. Qu, B. Huang, K. Li, D. Niyato, and A. Jamalipour, "Game-theoretic incentive mechanism for blockchain-based federated learning," *IEEE Trans. Mobile Comput.*, pp. 1–14, 2025, early access.
[168] Y. Wang, Y. Wang, J. Liu, Z. Huang, and P. Xie, "A survey of game theoretic methods for cyber security," in *2016 IEEE First International Conference on Data Science in Cyberspace (DSC)*, 2016, pp. 631–636.
[169] K. Fan, B. Feng, X. Zhang, and Q. Zhang, "Network selection based on evolutionary game and deep reinforcement learning in space-air-ground integrated network," *IEEE Trans. Netw. Sci. Eng.*, vol. 9, no. 3, p. 1802 – 1812, 2022.
[170] C. Peng, D. Zheng, Y. Zhong *et al.*, "Off-site protection against service function forwarder failures in NFV," *Comput. Netw.*, vol. 221, 2023.
[171] J. Xu, F. Luo, and H. Shao, "Failure rate analysis for time-sensitive networking," in *Proc. ICMIA*, 2016/11.
[172] S. Wang, M. Qureshi, L. Miralles-Pechuan, T. Huynh-The, T. Gadekallu, and M. Liyanage, "Explainable AI for 6G use cases: Technical aspects and research challenges," *IEEE Open J. Commun. Soc.*, vol. 5, pp. 2490–2540, 2024.
[173] T. Mezair, Y. Djenouri, A. Belhadi *et al.*, "A sustainable deep learning framework for fault detection in 6G Industry 4.0 heterogeneous data environments," *Comput. Commun.*, vol. 187, pp. 164–171, 2022.
[174] L. Bai, H. Ma, Y. Jiang, Z. Yin, H. Wan, and H. Wang, "GRL-RR: A graph reinforcement learning-based resilient routing framework for software-defined leo mega-constellations," *Computer Networks*, vol. 259, 2025.
[175] M. Ye, J. Zhang, Z. Guo, and H. Jonathan Chao, "Path-based graph neural network for robust and resilient routing in distributed traffic engineering," *IEEE Journal on Selected Areas in Communications*, 2025.
[176] A. U. Khan, G. Abbas, Z. H. Abbas *et al.*, "Reliability analysis of cognitive radio networks with reserved spectrum for 6G-IoT," *IEEE Trans. Netw. Serv. Manag.*, vol. 19, no. 3, pp. 2726–2737, 2022.
[177] J. Chen, X. Liang, J. Xue, Y. Sun, H. Zhou, and X. Shen, "Evolution of RAN architectures towards 6G: Motivation, development, and enabling technologies," *IEEE Commun. Surveys Tuts.*, vol. 26, no. 3, pp. 1950–1988, 2024.
[178] X. Zha, W. Ni, K. Zheng *et al.*, "Collaborative authentication in decentralized dense mobile networks with key predistribution," *IEEE Trans. Inf. Forensics Secur.*, vol. 12, no. 10, pp. 2261–2275, 2017.
[179] A. Braeken, "Symmetric key based 5G AKA authentication protocol satisfying anonymity and unlinkability," *Comput. Netw.*, vol. 181, p. 107424, 2020.
[180] J. Munilla, M. Burmester, and R. Barco, "An enhanced symmetric-key based 5G-AKA protocol," *Comput. Netw.*, vol. 198, 2021.
[181] S. K. Taskou, M. Rasti, and P. H. J. Nardelli, "Energy and cost efficient resource allocation for blockchain-enabled NFV," *IEEE Trans. Serv. Comput.*, vol. 15, no. 4, pp. 2328–2341, 2022.
[182] G. Yu, X. Zha, X. Wang *et al.*, "Enabling attribute revocation for fine-grained access control in blockchain-IoT systems," *IEEE Trans Eng. Manag.*, vol. 67, no. 4, pp. 1213–1230, 2020.
[183] G. Yu, L. Zhang, X. Wang *et al.*, "A novel dual-blockchained structure for contract-theoretic LoRa-based information systems," *Inf. Process. Manage.*, vol. 58, no. 3, may 2021.
[184] I. Makhdoom, M. Abolhasan, H. Abbas *et al.*, "Blockchain's adoption in IoT: The challenges, and a way forward," *J. Netw. Comput. Appl.*, vol. 125, pp. 251–279, 2019.
[185] J. Zheng, K. Li, E. Tovar *et al.*, "Federated learning for energy-balanced client selection in mobile edge computing," in *Proc. IWCMC*, 2021.
[186] S. Ben Saad, B. Brik, and A. Ksentini, "Toward securing federated learning against poisoning attacks in zero touch B5G networks," *IEEE Trans. Netw. Serv. Manag.*, vol. 20, no. 2, pp. 1612–1624, 2023.
[187] J. Zheng, K. Li, N. Mhaisen *et al.*, "Exploring deep-reinforcement-learning-assisted federated learning for online resource allocation in privacy-preserving EdgeIoT," *IEEE Internet Things J.*, vol. 9, no. 21, pp. 21 099–21 110, 2022.
[188] S. B. Prathiba, G. Raja, S. Anbalagan *et al.*, "SOSChain: Self optimizing streamchain for last-mile 6G UAV-truck networks," in *Proc. ACM MobiCom*, 2021.
[189] X. Lyu, W. Ni, H. Tian *et al.*, "Optimal schedule of mobile edge computing for Internet of Things using partial information," *IEEE J. Sel. Areas Commun.*, vol. 35, no. 11, pp. 2606–2615, 2017.

[190] Y. Cui, T. Lv, W. Ni *et al.*, "Digital twin-aided learning for managing reconfigurable intelligent surface-assisted, uplink, user-centric cell-free systems," *IEEE J. Sel. Areas Commun.*, vol. 41, no. 10, pp. 3175–3190, 2023.

[191] H. Zhu, J. Li, J. Hu *et al.*, "Failure-aware and automated disaster backup in the 5G core network," in *Proc. CECCC*, 2022.

[192] P. K. Thiruvasagam, A. Chakraborty, and C. S. R. Murthy, "Resilient and latency-aware orchestration of network slices using multi-connectivity in MEC-enabled 5G networks," *IEEE Trans. Netw. Serv. Manag.*, vol. 18, no. 3, pp. 2502–2514, 2021.

[193] P. K. Thiruvasagam, A. Chakraborty, A. Mathew *et al.*, "Reliable placement of service function chains and virtual monitoring functions with minimal cost in softwarized 5G networks," *IEEE Trans. Netw. Serv. Manag.*, vol. 18, no. 2, pp. 1491–1507, 2021.

[194] Y. Liu, J. Peng, J. Kang *et al.*, "A secure federated learning framework for 5G networks," *IEEE Wireless Commun.*, vol. 27, no. 4, pp. 24–31, 2020.

[195] A. Fernandez-Fernandez, E. Coronado, A. Erspamer *et al.*, "Unlocking the path toward intelligent telecom marketplaces for beyond 5G and 6G networks," *IEEE Commun. Mag.*, vol. 61, no. 3, pp. 28–34, 2023.

[196] M. Ahmad, S. M. N. Ali, M. T. Tariq *et al.*, "Neutrino: A fast and consistent edge-based cellular control plane," *IEEE/ACM Trans. Netw.*, vol. 31, no. 2, pp. 754–769, 2023.

[197] Y. Wu, F. Liu, L. Wan *et al.*, "Intelligent fault diagnostic model for industrial equipment based on multimodal knowledge graph," *IEEE Sensors J.*, pp. 1–1, 2023.

[198] Y. Ding, H. Li, F. Zhu *et al.*, "A semi-supervised failure knowledge graph construction method for decision support in operations and maintenance," *IEEE Trans. Ind. Informat.*, pp. 1–11, 2023.

[199] M. J. Nazar, A. Alhudhaif, K. N. Qureshi *et al.*, "Signature and flow statistics based anomaly detection system in software-defined networking for 6G internet of things network," *International Journal of System Assurance Engineering and Management*, vol. 14, no. 1, pp. 87–97, 2023. [Online]. Available: 6G-security-software-definednetworking

[200] A. Prado, F. Stockeler, F. Mehmeti *et al.*, "Enabling proportionally-fair mobility management with reinforcement learning in 5G networks," *IEEE J. Sel. Areas Commun.*, vol. 41, no. 6, pp. 1845–1858, 2023.

[201] K. Li, W. Ni, and F. Dressler, "Continuous maneuver control and data capture scheduling of autonomous drone in wireless sensor networks," *IEEE Trans. Mobile Comput.*, vol. 21, no. 8, pp. 2732–2744, 2021.

[202] C. Sun, W. Ni, and X. Wang, "Joint computation offloading and trajectory planning for UAV-assisted edge computing," *IEEE Trans. Wirel. Commun.*, vol. 20, no. 8, pp. 5343–5358, 2021.

[203] C. Sun, X. Xiong, Z. Zhai *et al.*, "Max–min fair 3D trajectory design and transmission scheduling for solar-powered fixed-wing UAV-assisted data collection," *IEEE Trans. Wirel. Commun.*, vol. 22, no. 12, pp. 8650–8665, 2023.

[204] A. V. Savkin, W. Ni, and M. Eskandari, "Effective UAV navigation for cellular-assisted radio sensing, imaging, and tracking," *IEEE Trans. Veh. Technol.*, vol. 72, no. 10, pp. 13 729–13 733, 2023.

[205] X. Zhao, Q. Cui, W. Li, W. Ni, E. Hossain, Q. Z. Sheng, X. Tao, and P. Zhang, "Convergence-privacy-fairness trade-off in personalized federated learning," *IEEE Trans. Machine Learn. Commun. Netw.*, vol. 3, pp. 246–262, 2025.

[206] X. Zhao, Q. Cui, Z. Du, W. Ni, W. Li, X. Yu, J. Zhang, X. Tao, and P. Zhang, "Enhancing convergence, privacy and fairness for wireless personalized federated learning: Quantization-assisted min-max fair scheduling," *IEEE Trans. Mobile Comput.*, pp. 1–16, 2025, early access.

[207] M. Shawkat, Z. H. Ali, M. Salem, and A. El-Desoky, "A robust and personalized privacy-preserving approach for adaptive clustered federated distillation," *Sci. Rep.*

[208] J. Zhou, Z. Su, J. Ni, Y. Wang, Y. Pan, and R. Xing, "Personalized privacy-preserving federated learning: Optimized trade-off between utility and privacy," in *Proc. GLOBECOM*, 2022, pp. 4872–4877.

[209] S. Li, Y. Liu, F. Feng, Y. Liu, X. Li, and Z. Liu, "Hierfed-pdp:hierarchical federated learning with personalized differential privacy," *J. Inf. Secur. Appl.*, vol. 86, p. 103890, 2024.

[210] W. Li, T. Lv, X. Zhao, X. Yuan, and W. Ni, "Free privacy protection for wireless federated learning: Enjoy it or suffer from it?" *IEEE Trans. Info. Forensics Secur.*, vol. 20, pp. 6263–6278, 2025.

[211] "*5G; 5G System; Restoration Procedures*, 3GPP TS 23.527 version 15.0.0 Release-15," 2018.

[212] "How to tackle fast recovery from radio link failure," 2020. [Online]. Available: https://www.ericsson.com/en/blog/2020/9/fast-recovery-from-radio-link-failure

[213] "*5G; Management and orchestration; Generic management services*, 3GPP TS 28.532 version 17.5.2 Release-17," 2023.

[214] "*Digital cellular telecommunications system (Phase 2+) (GSM); Mobile Station (MS) conformance specification; Part 2: Protocol Implementation Conformance Statement (PICS) proforma specification*, ETSI TS 151 010-2 v13.15.0," 2023.

[215] "*5G; NG-RAN; F1 Application Protocol (F1AP)*, 3GPP TS 38.473 version 17.3.0 Release 17," 2023.

[216] "*LTE; 5G; 5GS; User Equipment (UE) conformance specification; Part 3: Protocol Test Suites*, 3GPP TS 38.523-3 version 17.7.0 Release 17," 2023.

[217] "*5G; NR; User Equipment (UE) conformance specification; Applicability of radio transmission, radio reception and radio resource management test cases*, 3GPP TS 38.522 version 17.9.0 Release 17," 2023.

[218] "*5G-Advanced RAN Features*, 3GPP Rel-18," 2023.

[219] "IEEE topic on failure-analysis." [Online]. Available: https://technav.ieee.org/topic/failure-analysis

[220] "*Sustainable trust*, NGMN Alliance Security Competence Team V1.0," 2023.

[221] "*WWRF IEG Evaluation of IMT-2020 Candidate Technology EUHT Submission from NUFRONT*, WWRF OUTLOOK," 2022.

[222] "*6G Vertical Use Cases*, One6G White Paper," 2023.

[223] "*6G Technology Overview – Second Edition*, One6G White Paper," 2023.

[224] "*6G & Robotics*, One6G Position Paper," 2023.

[225] W. Yang, H. Du, Z. Q. Liew *et al.*, "Semantic communications for future internet: Fundamentals, applications, and challenges," *IEEE Commun. Surv. Tut.*, vol. 25, no. 1, pp. 213–250, 2023.

[226] "*On Artificial Intelligence - A European approach to excellence and trust*, European Union White Paper," 2023.

[227] "EU AI Act: First regulation on artificial intelligence," 2023. [Online]. Available: https://www.europarl.europa.eu/news/en/headlines/society/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence?Channel=Partner&Channel=Partner

[228] "AI regulation: A pro-innovation approach," 2023. [Online]. Available: https://www.gov.uk/government/publications/ai-regulation-a-pro-innovation-approach

[229] "Directive on automated decision-making," 2023. [Online]. Available: https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=32592

[230] "Guide on the use of Generative AI," 2023. [Online]. Available: https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/responsible-use-ai/guide-use-generative-ai.html

[231] A. K. Erenoğlu, I. Sengor, and O. Erdinç, "Power system resiliency: A comprehensive overview from implementation aspects and innovative concepts," *Energy Nexus*, vol. 15, p. 100311, 2024.

[232] L. Khaloopour, Y. Su, F. Raskob, T. Meuser, R. Bless, L. Janzen, K. Abedi, M. Andjelkovic, H. Chaari, P. Chakraborty, M. Kreutzer, M. Hollick, T. Strufe, N. Franchi, and V. Jamali, "Resilience-by-design in 6G networks: Literature review and novel enabling concepts," *IEEE Access*, vol. 12, pp. 155 666–155 695, 2024.

[233] T. Krueger, B. Mitra, T. Ozanski, and S. Pramanik, "Epidemic spreading on directed networks and twitter cascades," *IEEE Trans. Netw. Sci. Eng.*, vol. 11, no. 3, p. 2742 – 2756, 2024.

[234] H. Wang, X. Zhou, S. Wang, X. Zhao, X. Deng, and W. Gong, "Full-link delivery time prediction in logistics using federated heterogeneous graph transformer," *IEEE Internet Things J.*, vol. 12, no. 6, p. 6775 – 6789, 2025.

[235] C. Liu, X. Xie, X. Zhang, and Y. Cui, "Large language models for networking: Workflow, advances and challenges," *IEEE Network*, pp. 1–1, 2024.

[236] S. Bi, C. Wang, B. Wu *et al.*, "A comprehensive survey on applications of AI technologies to failure analysis of industrial systems," *Eng. Fail. Anal.*, vol. 148, p. 107172, 2023.

[237] F. Mogyorosi, P. Babarczi, J. Zerwas *et al.*, "Resilient control plane design for virtualized 6G core networks," *IEEE Trans. Netw. Serv. Manag.*, vol. 19, no. 3, pp. 2453–2467, 2022.

[238] S. Hu, X. Chen, W. Ni *et al.*, "Distributed machine learning for wireless communication networks: Techniques, architectures, and applications," *IEEE Commun. Surveys Tuts.*, vol. 23, no. 3, pp. 1458–1493, 3rd Quart., 2021.

[239] Y. Sun, T. Zhao, Z. Zou *et al.*, "Imbalanced data fault diagnosis of hydrogen sensors using deep convolutional generative adversarial network with convolutional neural network," *Rev. Sci. Instrum.*, vol. 92, no. 9, 2021.

[240] Y. Hu, R. Liu, X. Li *et al.*, "Task-sequencing meta learning for intelligent few-shot fault diagnosis with limited data," *IEEE Trans. Ind. Informat.*, vol. 18, no. 6, pp. 3894–3904, 2022.

[241] P. A. Traganitis and E. G. Strangas, "Perspectives of transfer learning on the diagnosis of faults in electrical machines, power electronics, and drives," in *Proc. IEEE SDEMPED*, 2023.

[242] Z. Zhao, R. Zhao, Y. Xu, and Y. Jiao, "Task-generalization-based graph convolutional network for fault diagnosis of rod-fastened rotor system," *IEEE Trans. Ind. Informat.*, vol. 20, no. 3, pp. 4616–4626, 2024.

[243] S. Bi, J. Cui, W. Ni *et al.*, "Three-dimensional cooperative positioning for Internet of Things provenance," *IEEE Internet Things J.*, vol. 9, no. 20, pp. 19 945–19 958, 2022.

[244] D. Pan, Y. Dong, M. Qi *et al.*, "Fault management platform based on knowledge graph in network slicing environment," in *Proc. IEEE BMSB*, 2023.

[245] Y. Sui, Y. Zhang, J. Sun *et al.*, "LogKG: Log failure diagnosis through knowledge graph," *IEEE Trans. Serv. Comput.*, vol. 16, no. 5, pp. 3493–3507, 2023.

[246] Z. Zhou, S. Yu, W. Chen *et al.*, "CE-IoT: Cost-effective cloud-edge resource provisioning for heterogeneous IoT applications," *IEEE Internet Things J.*, vol. 7, no. 9, pp. 8600–8614, 2020.

[247] T. Kim, H. Park, Y. Jin *et al.*, "Partition placement and resource allocation for multiple DNN-based applications in heterogeneous IoT environments," *IEEE Internet Things J.*, vol. 10, no. 11, pp. 9836–9848, 2023.

[248] F. Liu, Y. Li, H. Chen, L. Jiao, M. Luo, and M. Wang, "YuX: Finite field multiplication based block ciphers for efficient FHE evaluation," *IEEE Trans. Inf. Theory*, vol. 70, no. 5, p. 3729 – 3749, 2024.

[249] Z. Haddad, "Enhancing privacy and security in 5G networks with an anonymous handover protocol based on blockchain and zero knowledge proof," *Comput. Netw.*, vol. 250, 2024.

[250] D. Liu, G. Yu, Z. Zhong, and Y. Song, "Secure multi-party computation with secret sharing for real-time data aggregation in IIoT," *Comput. Commun.*, vol. 224, pp. 159–168, 2024.

[251] A. Feraudo, N. Romandini, C. Mazzocca, R. Montanari, and P. Bellavista, "DIVA: A DID-based reputation system for secure transmission in VANETs using IOTA," *Comput. Netw.*, vol. 244, 2024.

[252] B. Alzahrani, "An information-centric networking based registry for decentralized identifiers and verifiable credentials," *IEEE Access*, vol. 8, p. 137198 – 137208, 2020.

[253] X. Shen, X. Li, H. Yin, C. Cao, and L. Zhang, "Lattice-based multi-authority ciphertext-policy attribute-based searchable encryption with attribute revocation for cloud storage," *Comput. Netw.*, vol. 250, 2024.

[254] P. Zhu, W. Ni, and X. Wang, "Integrated sensing and communication with reconfigurable holographic surface," *IEEE Trans. Commun.*, pp. 1–1, 2025, early access.

[255] X. Zhou, A. Shen, S. Hu, W. Ni, X. Wang, and E. Hossain, "Towards quantum-native communication systems: State-of-the-art, trends, and challenges," *IEEE Commun. Surv. Tut.*, pp. 1–1, 2025, early access.

[256] F. Klement, W. Liu, and S. Katzenbeisser, "Toward securing the 6G transition: A comprehensive empirical method to analyze threats in O-RAN environments," *IEEE J. Select. Areas Commun.*, vol. 42, no. 2, p. 420 – 431, 2024.

[257] O. Latry, N. Moultif, E. Joubert *et al.*, "A time to failure evaluation of AlGaN/GaN HEMT transistors for RF applications," *e-Prime - Advances in Electrical Engineering, Electronics and Energy*, vol. 2, p. 100062, 2022.

[258] A. Avila, A. Garcia-Bediaga, F. Gonzalez, X. Jord, X. Perpi, and A. Rujas, "Thermal performance analysis of GaN-based high-power converters," in *Proc. ECCE*, 2018, pp. 1–10.

[259] M. Ganjalizadeh, H. S. Ghadikolaei, J. Haraldson *et al.*, "Interplay between distributed AI workflow and URLLC," in *Proc. IEEE GLOBECOM*, 2022.

[260] T. Hewa, A. Braeken, M. Liyanage *et al.*, "Fog computing and blockchain-based security service architecture for 5G industrial IoT-enabled cloud manufacturing," *IEEE Trans. Ind. Informat.*, vol. 18, no. 10, pp. 7174–7185, 2022.

[261] U. Pereg, C. Deppe, and H. Boche, "Communication with unreliable entanglement assistance," in *Proc. ISIT*, 2022, pp. 2231–2236.

[262] K. Yao, W. O. Krawec, and J. Zhu, "Quantum sampling for finite key rates in high dimensional quantum cryptography," *IEEE Trans. Inf. Theory*, vol. 68, no. 5, pp. 3144–3163, 2022.

[263] B. Vacchini, "Comparison of distances and entropic distinguishability quantifiers for the detection of memory effects," *Int. J. Quantum Inf.*, 2024.

[264] X. Feng, D. He, and L. Wei, "Robust phase metrology with hybrid quantum interferometers against particle losses," *Phys. Rev. A*, vol. 107, no. 6, 2023.

[265] L. Wang, Q. Cao, Z. Zhang, S. Mirjalili, and W. Zhao, "Artificial rabbits optimization: A new bio-inspired meta-heuristic algorithm for solving engineering optimization problems," *Engineering Applications of Artificial Intelligence*, vol. 114, 2022.

[266] R. Soundarayaa and C. Balasubramanian, "Komodo mlipir algorithm-based optimal route determination mechanism for improving quality of service in vehicular ad hoc network," *Sustainable Computing: Informatics and Systems*, vol. 42, 2024.

[267] A. Dixit and S. Kumar Singh, "BMUDF: Hybrid bio-inspired model for fault-aware uav routing using destination-aware fan shaped clustering," *Internet of Things (Netherlands)*, vol. 22, 2023.

[268] G. Xu and X. Zhang, "Statistical analysis of resilience in an air transport network," *Frontiers in Physics*, vol. 10, 2022.

[269] K. Charitoudi and A. J. C. Blyth, "An agent-based socio-technical approach to impact assessment for cyber defense," *Information Security Journal*, vol. 23, p. 125 – 136, 2014.

Siguo Bi received the Ph.D. degree in Electronic Science and Technology from Fudan University, Shanghai, China, in 2020. His research interests include failure analysis in communication networks, network security, practical applications of large language models, and knowledge management.

Xin Yuan (M'19-SM'24) received the B.E. degree from Taiyuan University of Technology, Shanxi, China, in 2013, and the dual Ph.D. degree from Beijing University of Posts and Telecommunications (BUPT), Beijing, China, and the University of Technology Sydney (UTS), Sydney, Australia, in 2019 and 2020, respectively. She is currently a Senior Research Scientist at CSIRO, Sydney, NSW, Australia. She is also an Adjunct Senior Lecturer at the University of New South Wales. Her research interests include machine learning and optimization, and their applications to intelligent systems.

Shuyan Hu (M'20) received the B.Eng. degree in Electrical Engineering from Tongji University, Shanghai, China, in 2014 and the Ph.D. degree in Electronic Science and Technology from Fudan University, Shanghai, China, in 2019. She is currently an Associate Professor with Tongji University. She was a Postdoctoral Research Fellow with Fudan University from 2019 to 2024. Her research interests include machine learning and convex optimizations and their applications to wireless communication, satellite-terrestrial networks, and intelligent and autonomous systems.

Kai Li (S'09–M'14–SM'20) received the B.E. degree from Shandong University, China, in 2009, the M.S. degree from The Hong Kong University of Science and Technology, Hong Kong, in 2010, and the Ph.D. degree in computer science from The University of New South Wales, Sydney, NSW, Australia, in 2014. Currently, he is a Visiting Research Scholar with the School of Electrical Engineering and Computer Science, TU Berlin, Germany, and a Senior Research Scientist with the CISTER Research Centre, Porto, Portugal. He is also a CMU-Portugal Research Fellow, jointly supported by Carnegie Mellon University (CMU), Pittsburgh, PA, USA, and the Foundation for Science and Technology (FCT), Lisbon, Portugal. From 2023 to 2024, he was a Visiting Research Scientist with the Division of Electrical Engineering, Department of Engineering, University of Cambridge, UK. In 2022, he was a Visiting Research Scholar with the CyLab Security and Privacy Institute, CMU. Prior to this, he was a Post-Doctoral Research Fellow with the SUTD-MIT International Design Centre, Singapore University of Technology and Design, Singapore, from 2014 to 2016. He has also held positions as a Visiting Research Assistant with the ICT Centre, CSIRO, Brisbane, QLD, Australia, from 2012 to 2013, and a full-time Research Assistant with the Mobile Technologies Centre, The Chinese University of Hong Kong, Hong Kong, from 2010 to 2011. He has been an Associate Editor of journals, such as *Internet of Things* (Elsevier) since 2024, *Nature Computer Science* (Springer) since 2023, *Computer Communications* (Elsevier) and *Ad Hoc Networks* (Elsevier) since 2021, and IEEE ACCESS from 2018 to 2024.

Wei Ni (M'09-SM'15-F'24) received the B.E. and Ph.D. degrees in Electronic Engineering from Fudan University, Shanghai, China, in 2000 and 2005, respectively. He is the Associate Dean (Research) in the School of Engineering, Edith Cowan University, Perth, and a Conjoint Professor at the University of New South Wales, Sydney, Australia. He is also a Technical Expert at Standards Australia with focus on the international standardization of Big Data and AI. He was a Deputy Project Manager at the Bell Labs, Alcatel/Alcatel-Lucent from 2005 to 2008; a Senior Research Engineer at Nokia from 2008 to 2009; and a Senior Principal Research Scientist and Group Leader at the Commonwealth Scientific and Industrial Research Organisation (CSIRO) from 2009 to 2025. He has been an Editor for IEEE Transactions on Wireless Communications since 2018, IEEE Transactions on Vehicular Technology since 2022, IEEE Transactions on Information Forensics and Security and IEEE Communication Surveys and Tutorials since 2024, and IEEE Transactions on Network Science and Engineering since 2025. He served as Secretary, Vice-Chair, and Chair of the IEEE VTS NSW Chapter from 2015 to 2022, Track Chair for VTC-Spring 2017, Track Co-chair for IEEE VTC-Spring 2016, Publication Chair for BodyNet 2015, and Student Travel Grant Chair for WPMC 2014.

Ekram Hossain (Fellow, IEEE) is a Professor and the Associate Head (Graduate Studies) of the Department of Electrical and Computer Engineering, University of Manitoba, Canada. He is a Member (Class of 2016) of the College of the Royal Society of Canada. He is also a Fellow of the Canadian Academy of Engineering and the Engineering Institute of Canada. He has won several research awards, including the 2017 IEEE Communications Society Best Survey Paper Award and the 2011 IEEE Communications Society Fred Ellersick Prize Paper Award. He was listed as a Clarivate Analytics Highly Cited Researcher in Computer Science in 2017-2025. Previously, he served as the Editor-in-Chief (EiC) for the IEEE Press (2018–2021) and the IEEE Communications Surveys and Tutorials (2012–2016). He was a Distinguished Lecturer of the IEEE Communications Society and the IEEE Vehicular Technology Society. He served as the Director of Magazines (2020-2021) and the Director of Online Content (2022-2023) for the IEEE Communications Society.

Xin Wang (SM'09-F'23) received the B.Sc. and M.Sc.degrees from Fudan University, Shanghai, China, in 1997 and 2000, respectively, and the Ph.D. degree from Auburn University, Auburn, AL, USA, in 2004, all in electrical engineering. From September 2004 to August 2006, he was a Postdoctoral Research Associate with the Department of Electrical and Computer Engineering, University of Minnesota, Minneapolis. In August 2006, he joined the Department of Electrical Engineering, Florida Atlantic University, Boca Raton, FL, USA, as an Assistant Professor, then was promoted to a tenured Associate Professor in 2010. He is currently a Professor with the College of Future Information Technology, Fudan University, China. His research interests include stochastic network optimization, wireless distributed learning, integrated sensing and communications, UAV communications, and signal processing for communications. He served as a Senior Area Editor for the IEEE Transactions on Signal Processing, as an Associate Editor for the IEEE Transactions on Signal Processing, as an Editor for the IEEE Transactions on Wireless Communications, as an Editor for the IEEE Transactions on Vehicular Technology, and as an Associate Editor for the IEEE Signal Processing Letters. He is a member of the Signal Processing for Communications and Networking Technical Committee of IEEE Signal Processing Society, and a Distinguished Speaker of the IEEE Vehicular Technology Society.