Advanced International Journal for Research (AIJFR)
E-ISSN: 3048-7641 ● Website: www.aijfr.com ● Email: editor@aijfr.com

Comprehensive Analysis of Network Resilience for 6G Communication

Dr. Ashish Mishra

Assistant Professor
Department of Electronics and Communication Engineering, RKDF University, Bhopal

Abstract

Network resilience, a critical attribute of modern communication systems, embodies the capacity of a network to maintain acceptable levels of service in the face of disruptions, failures, and attacks. This research paper provides a comprehensive examination of network resilience, a critical attribute for modern digital infrastructures. It defines network resilience in contrast to related concepts such as reliability, availability, robustness, and fault tolerance, emphasizing its proactive and adaptive dimensions. The paper categorizes the diverse causes of network disruptions, including cyberattacks, hardware and software failures, human error, and natural disasters, highlighting the increasing complexity introduced by supply chain vulnerabilities and critical infrastructure interdependencies. Real-world incidents and case studies illustrate the profound impact of network failures across various sectors. Finally, the paper investigates emerging technologies like Artificial Intelligence, Machine Learning, and quantum networking, and their implications for future resilience strategies, advocating for a fundamental shift towards a "resilience-by-design" paradigm.

1. Introduction

1.1. Overview and Context of Network Resilience

Network resilience represents a fundamental capability for contemporary digital infrastructures, signifying a system's capacity to withstand, adapt to, and recover from various forms of adversity with minimal disruption to essential services. At its core, network resilience means being able to endure or rapidly recover from service degradation and complete outages, thereby minimizing business interruption. This involves maintaining continuous operations, even in a degraded state, and ensuring swift restoration of functionality after a failure, while also possessing the inherent ability to scale in response to fluctuating demands. The concept of network resilience has garnered significant attention due to the increasing reliance on networks in various aspects of modern life, ranging from critical infrastructure to social interactions [1]. The popularity of resilience has led to it being examined from multiple disciplinary perspectives [2]. The ability of an organization to withstand disruptions and maintain a competitive edge hinges on network resilience in today's interconnected world [3].The origin of resilience can be traced to the work of Holling, who studied ecology and ecosystems, and is defined as the ability to recover or "jump back" [4]. The term "resilience" itself has roots in the Latin word "resilire"[5].

Network resilience can be seen as having different meanings: the ability to recover quickly from trauma and return to a stable state, robustness, graceful extensibility when unexpected challenges arise, and network architectures that can adapt to future surprises [6]. Resilient networks are characterized by their ability to self-diagnose, self-configure, self-protect, and self-heal, ensuring continuous operation and minimizing downtime [7].

The National Institute of Standards and Technology (NIST) provides a foundational perspective, defining network resilience as a computing infrastructure designed for continuous business operation. Such an infrastructure is characterized by high resistance to disruption, the capacity to function in a compromised mode if damaged, and the ability to recover quickly from incidents, alongside inherent scalability. NIST extends this concept to "cyber resilience," which encompasses the broader ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems reliant on cyber resources. This expanded definition underscores a strategic shift towards proactive measures and continuous adaptation, moving beyond mere reactive responses. Ultimately, network resilience is understood as a holistic practice that involves preparing for an unpredictable future, safeguarding against potential impacts, and ensuring a rapid rebound from any network event, whether anticipated or unforeseen. It serves as the foundational element for a robust and enduring IT infrastructure.

1.2. Importance of Network Resilience in Modern Infrastructure

In an increasingly digitized and interconnected global landscape, network resilience is not merely a technical advantage but a strategic imperative for critical business continuity. It empowers organizations to sustain operations even when confronted with circumstances that would otherwise lead to costly disruptions or even threaten their very viability. The profound consequences of network failures, which include substantial financial losses, diminished productivity, elevated security risks, customer dissatisfaction, and potential data loss, underscore the critical necessity for resilient network architectures.

The pervasive integration of the Internet into nearly every facet of modern society means that any disruption carries increasingly severe ramifications. This reality makes enhancing the resilience and survivability of both current and future networks an urgent priority. Beyond commercial implications, cyber resilience plays a vital role in ensuring the uninterrupted delivery of essential services, such as electricity, water, data, goods, and financial transactions, especially during emergencies. The capacity to resist or recover from cyberattacks can have direct implications for public safety and even human life.

Recent global incidents, including widespread power outages, sophisticated cyberattacks, and devastating natural disasters, have starkly exposed the inherent vulnerabilities within modern communication networks. These events highlight the deep interdependencies between communication networks and other critical sectors, such as energy, transportation, and healthcare. Disruptions in one sector can trigger cascading ripple effects across others, impacting economic stability, eroding public trust, and potentially compromising national security. As organizations continue their digital transformation journeys, the demand for networks capable of efficiently managing escalating traffic

volumes, robustly safeguarding data, and maintaining operational excellence intensifies, solidifying network resilience as a non-negotiable strategic priority. This urgency is further amplified by the evolving demands placed on mobile networks, particularly with the advent of 6G, as these networks assume an increasingly central role in public safety and crisis response efforts.

The increasing societal and economic reliance on interconnected digital infrastructure elevates network resilience from a purely technical IT concern to a critical national security, public safety, and governance imperative, necessitating policy-level attention and cross-sectoral collaboration. Early discussions of network disruptions often focused on their business and economic consequences, such as financial losses and reduced productivity. However, the scope of concern has rapidly expanded. Evidence demonstrates that cyber resilience is now essential for the continuity of critical services like electricity and water, and the ability to recover from cyberattacks can literally be a matter of life and death. Furthermore, communication networks are deeply intertwined with other vital sectors, including energy, transport, and healthcare, meaning that disruptions can trigger cascading effects across multiple domains, impacting economic activity, public trust, and national security. The growing reliance on mobile networks for public safety and crisis response further underscores this critical dependency. This chain of events illustrates that as more critical societal functions become reliant on and interconnected through digital networks, the failure of these networks leads to consequences far beyond mere financial inconvenience. This necessitates a strategic, national-level approach to resilience, involving governments, policymakers, and inter-agency cooperation, rather than being confined solely to the purview of individual IT departments.

2. Literature Review On Network Resilience

As communication systems evolve toward the sixth generation (6G), ensuring **network resilience** has emerged as a key research priority. 6G is expected to support **ultra-reliable low-latency communications (URLLC)**, **massive machine-type communications (mMTC)**, and **extreme capacity and connectivity**, making the robustness and adaptability of networks critical. Resilience in this context encompasses **fault tolerance**, **self-healing**, **security**, and **adaptive recovery** mechanisms under both physical and cyber disruptions.

a) **Sterbenz et al. (2010)** defined network resilience as “the ability of the network to provide and maintain an acceptable level of service in the face of faults and challenges.”
b) Resilience is multifaceted, involving **robustness**, **survivability**, **disruption tolerance**, **traffic engineering**, and **security**.
c) Studies in **5G (Zhang et al., 2019; Li et al., 2020)** focus on software-defined networking (SDN), network function virtualization (NFV), and self-organizing networks (SONs) as tools to enhance adaptability and fault management.
d) Existing works lay the foundation for fault detection, anomaly mitigation, and secure routing using **AI and machine learning (ML)**.
e) **Reinforcement Learning (RL)** for routing and load balancing (e.g., He et al., 2021)
f) **Federated Learning (FL)** to enable distributed and privacy-preserving resilience mechanisms

g) **Anomaly detection** using deep learning (CNNs, GANs) for attack mitigation and fault prediction
h) Used for **decentralized authentication** and **data integrity** in distributed networks (e.g., smart cities, IoT)
i) Studies (Kumar et al., 2022) explore **smart contract-based fault detection**

3. Defining Network Resilience and Related Concepts

3.1. Core Definition of Network Resilience

Network resilience, at its fundamental level, describes a network's ability to withstand or recover from adversity, service degradation, and complete outages with minimal business disruption. This definition emphasizes the continuity of operations even when faced with significant challenges. The National Institute of Standards and Technology (NIST) provides a more detailed framework, defining network resilience as a computing infrastructure that ensures continuous business operation, possesses high resistance to disruption, can operate effectively even in a degraded mode if damaged, and facilitates rapid recovery from failures, while also being capable of scaling to meet evolving demands.

NIST further refines this concept in the context of information systems, characterizing resilience as the capacity to continue functioning while under attack, even if in a debilitated state, and to swiftly restore essential operational capabilities after a successful attack. The broader term "cyber resilience," as articulated by NIST, encompasses the comprehensive ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises affecting systems that utilize or are enabled by cyber resources. This definition highlights the proactive elements of planning and continuous adaptation as integral components of resilience. In essence, network resilience forms the bedrock of a robust IT infrastructure, ensuring uninterrupted operations, rapid recovery, and adaptability to unpredictable shifts in demand.

3.2. Distinguishing Network Resilience from Reliability, Availability, Robustness, and Fault Tolerance

While often used interchangeably, network resilience is a distinct and overarching concept that integrates and extends other critical system properties. Understanding these distinctions is crucial for effective network design and management.

- **Availability:** This concept is primarily concerned with ensuring that a system is consistently ready and operational. It is often quantified as the percentage of time a network or service is accessible and functioning. For instance, Tier 1 operators often target 99.999 percent or higher core network availability.
- **Reliability:** Reliability quantifies the dependability of the service delivered by a system. It is a measure of how consistently a system performs its intended function over a specified period, often assessed using metrics like Mean Time Between Failures (MTBF).
- **Robustness:** Robustness focuses on a system's ability to handle unexpected situations without crashing or producing incorrect results. It describes how well a network performs under uncertain

conditions or a range of scenarios. Robustness metrics can be structural (e.g., node degree, edge connectivity), centrality-based (e.g., betweenness centrality), or functional (e.g., packet loss, throughput).

- **Fault Tolerance:** This involves designing a system to continue functioning despite the failure of one or more of its components. High availability (HA) systems are a form of fault tolerance that accepts that failures will occur and provides mechanisms for automatic recovery by removing single points of failure, such as using load balancers with auto-scaling groups or primary/secondary database replication. In contrast, systems designed for absolute fault tolerance aim to completely avoid system crashes, performance degradation, and data loss by employing full, parallel copies of the entire system.
- **Scalability:** This refers to a network's capacity to expand and smoothly manage increased demand without sacrificing speed or dependability. A truly effective network must embody both scalability and resilience; a scalable but non-resilient network might accommodate more users but collapse under pressure or cyber threats, whereas a resilient but non-scalable network could remain operational during failures but falter when demand surpasses its limits.

A resilient network is considered a broader concept than mere redundancy or survivability, integrating these elements as components within a comprehensive strategy. Resilience goes beyond robustness by emphasizing the swift recuperation of services to minimize downtime and customer impact. Survivability, a related concept, is defined as the ability to maintain a tolerable quality of service and meet essential requirements when network failures occur.

Table 1 provides a concise comparison of these interconnected concepts.

Table 1: Network Resilience vs. Related Concepts

Concept	Primary Focus	Key Characteristic	Relationship to Resilience
Network Resilience	Adapting to and recovering from disruptions, maintaining service continuity	Anticipate, Withstand, Recover, Adapt	Overarching goal, encompasses others
Availability	Ensuring the system is operational and ready for use	Uptime percentage	A component of resilience; resilience ensures availability during disruptions
Reliability	Consistent and dependable performance over time	Mean Time Between Failures (MTBF)	A prerequisite for resilience; a reliable system is easier to make resilient
Robustness	Handling unexpected situations without crashing or incorrect results	Resistance to perturbation	A quality that contributes to resilience; resilience adds recovery and adaptation
Fault Tolerance	Continuing to function despite component failures	Redundant components, failover	A mechanism for achieving resilience, particularly in

Concept	Primary Focus	Key Characteristic	Relationship to Resilience
			preventing total collapse
Scalability	Ability to expand and manage increased demand	Performance consistency under load	Essential for resilience; a non-scalable resilient network may still fail under high demand

Network resilience functions as an overarching paradigm that integrates and extends traditional concepts like reliability, availability, robustness, and fault tolerance, emphasizing dynamic adaptation and rapid recovery over static prevention or mere uptime. Traditional concepts such as availability and reliability primarily focus on continuous operation and dependability under normal or expected conditions. Fault tolerance, while crucial, is fundamentally about preventing failure through redundancy. Robustness, similarly, centers on handling unexpected inputs without a system crash. These approaches, while valuable, often represent static or reactive measures. In contrast, resilience, as defined by NIST, explicitly incorporates "anticipate" and "adapt" and places significant emphasis on "rapid recovery" and the ability to operate in a "degraded mode". This emphasis on swift recuperation signifies a profound shift from a purely preventative mindset—"build it strong enough not to break"—to a dynamic understanding that acknowledges the inevitability of disruption. The new focus becomes: "it will break, how fast can it recover and adapt?" Resilience, therefore, acknowledges that complete prevention of all failures is unrealistic and instead prioritizes the system's ability to absorb disruptions, degrade gracefully, and self-heal. Fault tolerance might be a crucial component of a resilient system, but resilience represents the broader strategic objective of ensuring continuous service delivery despite the occurrence of disruptions.

4. Causes and Classification of Network Disruptions

Network disruptions, which interrupt the normal functioning of a network and lead to connectivity issues, delays, or complete outages, can arise from a diverse array of sources. These challenges span various domains, from malicious attacks to environmental phenomena, each demanding specific strategies for mitigation and recovery.

4.1. Cyberattacks

Cyber-attacks represent a significant and evolving threat landscape for network resilience, designed to compromise network stability, steal data, or disrupt operations. Common types include:

- **Malware:** Malicious software, encompassing viruses, worms, ransomware, and spyware, infiltrates systems to steal data, disrupt operations, or hold data hostage. Modern ransomware attacks, for instance, can spread at machine speed, incapacitating entire networks and often reinfecting backup data and rebuilt systems, significantly complicating recovery efforts.
- **Phishing:** These attacks involve deceptive emails or messages that trick users into revealing sensitive information or downloading malicious software, often disguised as legitimate communications. Human susceptibility to phishing remains a top security risk.

- **Distributed Denial of Service (DDoS) Attacks:** DDoS attacks overwhelm network resources by flooding them with excessive traffic, causing disruptions and rendering systems inaccessible. These can be mitigated by overprovisioning circuits with additional bandwidth.
- **Man-in-the-Middle (MITM) Attacks:** MITM attacks intercept communications between two parties, allowing attackers to eavesdrop, alter, or steal data without detection. Encrypting network traffic and securing connections are effective countermeasures.
- **Insider Threats:** These occur when employees or contractors misuse their access to compromise security, either intentionally (e.g., data theft) or accidentally (e.g., clicking malicious links). Limiting access to sensitive data and monitoring network activities are crucial mitigation strategies.

4.2. Hardware and Software Failures

Failures in physical components and software systems are common causes of network disruptions.

- **Hardware Failures:** Malfunctioning routers, switches, servers, power supply units (PSUs), motherboards, or network interface cards (NICs) can lead to connectivity problems or complete system shutdowns. For example, a single path design in an industrial network means any hardware failure will interrupt all communications.
- **Software Issues:** Bugs, outdated firmware, or misconfigured network settings can cause significant connectivity problems. Unpatched vulnerabilities in software code create gaps that attackers can exploit, leaving networks exposed to various threats, including zero-day vulnerabilities that are exploited before patches are available. The 2023 Cisco Viptela SD-WAN appliance failure due to an expired cryptographic certificate exemplifies how software issues can take down entire networks.

Table 2 provides a classification of these network threats and disruptions.

Table 2: Classification of Network Threats and Disruptions

Category	Description	Examples
Cyberattacks	Malicious actions targeting network systems and data.	Malware (Ransomware, Viruses), Phishing, DDoS, Man-in-the-Middle (MITM), Insider Threats
Hardware Failures	Malfunctions or breakdowns of physical network components.	Routers, Switches, Servers, Power Supply Units (PSUs), Motherboards, NICs
Software Failures	Issues arising from bugs, outdated code, or misconfigurations.	Bugs, Outdated Firmware, Misconfigured Settings, Unpatched Vulnerabilities, Expired Certificates
Human Errors	Mistakes made by individuals leading to network disruptions.	Incorrect Configuration, Accidental Cable Disconnections, Mismanagement, Phishing Susceptibility

Category	Description	Examples
Natural Disasters	Environmental events causing physical damage or widespread outages.	Hurricanes, Floods, Fires, Earthquakes, Extreme Temperatures, Tidal Forces
Supply Chain Vulnerabilities	Exploitation of weaknesses within the chain of IT products and services.	Faulty software updates from third-party vendors, compromised hardware components
Critical Infrastructure Interdependencies	Cascading failures due to reliance between different essential sectors.	Energy grid outage impacting telecommunications, transportation system disruption affecting data centers

Table 3 summarizes these key metrics.

Table 3: Key Metrics for Network Resilience Measurement

Metric Category	Specific Metric	Description	Relevance to Resilience
Performance-Based	Uptime Percentage	Percentage of time the network is operational.	Directly indicates availability and operational continuity.
	Mean Time to Repair (MTTR)	Average time taken to restore service after an incident.	Measures recovery speed; lower MTTR means higher resilience.
	Mean Time Between Failures (MTBF)	Average time between system failures.	Indicates reliability and stability; higher MTBF means fewer disruptions.
	Recovery Time Objective (RTO)	Max tolerable downtime for a business process.	Defines recovery targets; meeting RTO is critical for business continuity.
Structural	Node Degree	Number of connections a node has.	Indicates connectivity; high-degree nodes are critical for network integrity.
	Edge Connectivity	Minimum edges whose removal disconnects the network.	Measures network robustness against link failures.
	Largest Connected Component Ratio	Proportion of network remaining connected after disruption.	Assesses overall network integrity post-attack/failure.
	Average Path Length	Average shortest path between nodes.	Reflects network efficiency and potential for rapid data flow.
Centrality	Betweenness	How often a node is on the	Identifies critical nodes whose

Metric Category	Specific Metric	Description	Relevance to Resilience
	Centrality	shortest path between others.	failure can severely impact network flow.
	Closeness Centrality	How close a node is to all other nodes.	Indicates efficiency of information dissemination from a node.
Functional	Failure Impact	Degree of disruption to performance or user experience.	Quantifies the severity of an incident's effect on service delivery.
	Blocked Connections	Number of connections unable to be established.	Measures service degradation under stress or failure conditions.

4.3. Qualitative Assessment Methods

Qualitative assessment methods are crucial when risks are difficult to quantify, data is lacking, or new, unprecedented risks emerge. These methods rely on expert judgment and available information to assess emerging threats.

- **Risk Analysis Frameworks:** Qualitative analysis helps create a framework for assessing risks that cannot be statistically expressed, such as reputational or legal risks.
- **Stakeholder Input:** Gathering input from diverse stakeholders helps understand all dimensions of resilience, ensures no major vulnerabilities are overlooked, and identifies a broader range of opportunities. This can involve workshops, interviews, and surveys.
- **Scenario Planning:** Envisioning future scenarios aids in identifying common ground among stakeholders and creating a positive vision for the future. This can involve stress testing, failover simulations, and security drills to evaluate network performance under high traffic, test backup systems, and assess response effectiveness to cyberattacks.

4.4. Resilience Evaluation Frameworks

Formal frameworks provide structured approaches to characterize and evaluate network resilience.

- **Service-Oriented Frameworks:** Some frameworks characterize network resilience by quantifying the operational state and expected service using functional metrics. This often formalizes resilience as transitions of network state in a two-dimensional space: one dimension representing network operation (normal, partially degraded, severely degraded) and the other representing service level (acceptable, impaired, unacceptable).
- **Systematic Approaches:** The "ResiliNets" strategy, for instance, proposes a D2R2+DR (Defend, Detect, Remediate, Recover, Diagnose, and Refine) approach, which includes both real-time control loops for dynamic adaptation and non-real-time loops for long-term system evolution and design improvement. This systematic view addresses the wide variety of challenges networks may face.

- **Integrated Assessment Systems:** Evaluation systems for network resilience can integrate economic, social, and structural dimensions. For example, research on urban networks evaluates resilience using metrics like average clustering coefficient, average degree, average path length, global efficiency, isolated nodes ratio, and largest connected component ratio. These frameworks often aim to provide actionable strategies for optimizing knowledge flows and mitigating systemic risks.
- **Industry Standards:** Standards like the Integrated Business Continuity and Resiliency (ICR) standard guide organizations in developing comprehensive programs to achieve continuous resilience across all levels—from core business functions to IT systems and cloud services—under all operating conditions. This standard emphasizes continuous monitoring, alert mechanisms, root cause analysis, and adaptive scaling.

5. Conclusion

Network resilience has evolved from a specialized technical concern to a strategic imperative for businesses, governments, and society at large. The increasing reliance on interconnected digital infrastructures for critical services, from emergency response to financial transactions, means that disruptions carry profound and cascading consequences, extending beyond financial losses to impact public trust and national security. The understanding of network resilience has matured from a focus on static prevention or mere uptime to a dynamic, holistic paradigm that emphasizes the ability to anticipate, withstand, recover from, and adapt to adversity.

The analysis presented in this paper underscores that achieving robust network resilience requires a comprehensive, multi-layered approach. This involves a deep understanding of the diverse threat landscape, encompassing sophisticated cyberattacks, inherent hardware and software vulnerabilities, pervasive human errors, unpredictable natural disasters, and the complex interdependencies within critical infrastructure supply chains. Effective architectural strategies, such as redundancy, diversity, fault tolerance, and network segmentation, are foundational. These are increasingly augmented by advanced technologies and protocols, including modern Ethernet switching protocols, link aggregation, virtual router redundancy, and the transformative capabilities of Software-Defined Networking and Network Function Virtualization. The adoption of Network as a Service and deep cloud integration further enhances resilience through distributed architectures and automated recovery. Automation, particularly through Zero-Touch Provisioning and AI-driven systems, is proving indispensable for accelerating recovery and minimizing human error.

References

1. Unified Architecture for Machine Learning in 5G and Future Networks, International Telecommunication Union–Telecommunication Standardization Sector, Technical Specification ITU-T FG-ML5G-ARC5G, Jan. 2019.
2. Q. Mao, F. Hu, and Q. Hao, “Deep learning for intelligent wireless networks: A comprehensive survey,” IEEE Commun. Surveys Tut., vol. 20, no. 4, pp. 2595–2621, 2018. doi: 10.1109/COMST.2018.2846401.

3. K. David and H. Berndt, “6G vision and requirements: Is there any need for beyond 5G? ” IEEE Veh. Technol. Mag., vol. 13, no. 3, pp. 72–80, Sept. 2018. doi: 10.1109/MVT.2018.2848498.
4. R. Li, “Network 2030: Market drivers and prospects,” in Proc. 1st International Telecommunication Union Workshop on Network 2030, New York, Oct. 2018. [Online]. Available: https://www.itu.int/en/ITU-T/Workshops-and-Seminars/201810/Documents/Richard_Li_Presentation.pdf
5. M. Latva-aho, “Radio access networking challenges towards 2030,” in Proc. 1st International Telecommunication Union Workshop on Network 2030, New York, Oct. 2018. [Online]. Available: https://www.itu.int/en/ITU-T/Workshops-and-Seminars/201810/Documents/Matt_Latva-aho_Presentation.pdf
6. IMT Vision—Framework and Overall Objectives of the Future Development of IMT for 2020 and Beyond, International Telecommunication Union–Radiocommunications Sector, Recommendation ITU-R M.2083-0, Sept. 2015.
7. J. Liu, Y. Shi, Z. M. Fadlullah, and N. Kato, “Space-air-ground integrated network: A survey,” IEEE Commun. Surveys Tut., vol. 20, no. 4, pp. 2714–2741, 2018. doi: 10.1109/COMST.2018.2841996.
8. I. Afolabi, T. Taleb, K. Samdanis, A. Ksentini, and H. Flinck, “Network slicing and softwarization: A survey on principles, enabling technologies, and solutions,” IEEE Commun. Surveys Tut., vol. 20, no. 3, pp. 2429–2453, 2018. doi: 10.1109/COMST.2018.2815638.
9. A.-A. A. Boulogeorgos et al. “Terahertz technologies to deliver optical network quality of experience in wireless systems beyond 5G,” IEEE Commun. Mag., vol. 56, no. 6, pp. 144–151, June 2018. doi: 10.1109/MCOM.2018.1700890.
10. E. Björnson, L. Sanguinetti, H. Wymeersch, J. Hoydis, T. L. Marzetta, Massive MIMO is a reality—What is next? Five promising research directions for antenna arrays. 2019. [Online]. Available: https://arxiv.org/abs/1902.07678
11. Y. Ren et al. “Line-of-sight millimeter-wave communications using orbital angular momentum multiplexing combined with conventional spatial multiplexing,” IEEE Trans. Wireless Commun., vol. 16, no. 5, pp. 3151–3161, May 2017. doi: 10.1109/TWC.2017.2675885.
12. P. H. Pathak, X. Feng, P. Hu, and P. Mohapatra, “Visible light communication, networking, and sensing: A survey, potential and challenges,” IEEE Commun. Surveys Tut., vol. 17, no. 4, pp. 2047–2077, Sept. 2015. doi: 10.1109/COMST.2015.2476474.
13. P. Botsinis et al., “Quantum search algorithms for wireless communications,” IEEE Commun. Surveys Tut., vol. 21, no. 2, pp. 1209–1242, 2019. doi: 10.1109/COMST.2018.2882385.
14. O. B. Akan, H. Ramezani, T. Khan, N. A. Abbasi, and M. Kuscu, “Fundamentals of molecular information and communication science,” Proc. IEEE, vol. 105, no. 2, pp. 306–318, Feb. 2017. doi: 10.1109/JPROC.2016.2537306.
15. E. Khorov, A. Kiryanov, A. Lyakhov, and G. Bianchi, “A tutorial on IEEE 802.11ax high efficiency WLANs,” IEEE Commun. Surv. Tut., vol. 21, no. 1, pp. 197–216, 1st Quarter 2019.
16. IEEE Standard for High Data Rate Wireless Multi-Media Networks–Amendment 2: 100 Gb/s Wireless Switched Point-to-Point Physical Layer, IEEE Standard 802.15.3d, 2017.
17. Alsharif, M. H. & Nordin, R. Evolution towards fifth generation (5G) wireless networks: current trends and challenges in the deployment of millimetre wave, massive MIMO, and small cells. Telecommun. Syst. 64, 617–637 (2017).

18. David, K. & Berndt, H. 6G vision and requirements: is there any need for beyond 5G? IEEE Veh. Technol. Mag. 13, 72–80 (2018). This publication looks at 6G from the perspective of service.
19. Raghavan, V. & Li, J. Evolution of physical-layer communications research in the post-5G era. IEEE Access 7, 10392–10401 (2019). This paper points out the potential research directions of physical-layer communications in the post -5G era.
20. Yastrebova, A., Kirichek, R., Koucheryavy, Y., Borodin, A. & Koucheryavy, A. Future networks 2030: architecture & requirements. In Proc. IEEE ICUMT 1–8 (2018). This paper details the project of Future Networks 2030.
21. Saad, W., Bennis, M. & Chen, M. A vision of 6G wireless systems: applications, trends, technologies, and open research problems. IEEE Netw. https://doi.org/10.1109/MNET.001.1900287 (2019).
22. Calvanese Strinati, E. et al. 6G: the next frontier: from holographic messaging to artificial intelligence using subterahertz and visible light communication. IEEE Veh. Technol. Mag. 14, 42–50 (2019).
23. Tariq, F. et al. A speculative study on 6G. Preprint at https://arxiv.org/abs/1902.06700 (2019).
24. Chen, S., Zhao, J. & Peng, Y. The development of TD-SCDMA 3G to TD-LTE-advanced 4G from 1998 to 2013. IEEE Wireless Commun. 21, 167–176 (2014).
25. Rissen, J. & Soni, R. The evolution to 4G systems. Bell Labs Tech. J. https://doi.org/10.1002/bltj.20333 (2009).
26. Raivio, Y. 4G-hype or reality. In Proc. Int. Conf. 3G Mobile Commun. Technol. 346–350 (IET, 2001).
27. Dohler, M., Meddour, D., Senouci, S. & Saadani, A. Cooperation in 4G—hype or ripe? IEEE Technol. Soc. Mag. 27, 13–17 (2008).
28. Frias, Z. & Pérez, J. Techno-economic analysis of femtocell deployment in long-term evolution networks. EURASIP J. Wireless Commun. Netw. 2012, 288 (2012).
29. Moral, A. et al. Technoeconomic evaluation of cooperative relaying transmission techniques in OFDM cellular networks. EURASIP J. Adv. Sig. Proc. https://doi.org/10.1155/2011%2F507035 (2011).
30. Wang, Z., Dang, S., Shaham, S., Zhang, Z. & Lv, Z. Basic research methodology in wireless communications: the first course for research-based graduate students. IEEE Access 7, 86678–86696 (2019).
31. Andrews, J. G. et al. What will 5G be? IEEE J. Sel. Area. Commun. 32, 1065–1082 (2014).
32. Parkvall, S., Dahlman, E., Furuskar, A. & Frenne, M. NR: the new 5G radio access technology. IEEE Commun. Stand. Mag. 1, 24–30 (2017).
33. Patzold, M. 5G is coming around the corner. IEEE Veh. Technol. Mag. 14, 4–10 (2019). This editorial summarizes the latest achievements of 5G research deployment.
34. Dohler, M., Heath, R. W., Lozano, A., Papadias, C. B. & Valenzuela, R. A. Is the PHY layer dead? IEEE Commun. Mag. 49, 159–165 (2011). This paper describes a number of common issues that have lasted for a long time in the research community of wireless communications.
35. Clazzer, F. et al. From 5G to 6G: has the time for modern random access come? Preprint at https://arxiv.org/abs/1903.03063 (2019).

36. Zhang, Z. et al. 6G wireless networks: vision, requirements, architecture, and key technologies. IEEE Veh. Technol. Mag. 14, 28–41 (2019).
37. Rommel, S., Raddo, T. R. & Monroy, I. T. Data center connectivity by 6G wireless systems. In Proc. IEEE PSC https://doi.org/10.1109/PS.2018.8751363 (IEEE, 2018).
38. Giordani, M., Polese, M., Mezzavilla, M., Rangan, S. & Zorzi, M. Towards 6G networks: use cases and technologies. Preprint at https://arxiv.org/abs/1903.12216 (2019).
39. Yanikomeroglu, H. Integrated terrestrial/non-terrestrial 6G networks for ubiquitous 3D super-connectivity. In Proc. 21st ACM Int. Conf. Modeling, Analysis and Simulation of Wireless and Mobile Systems 3–4 (ACM, 2018).
40. Yaacoub, E. & Alouini, M.-S. A key 6G challenge and opportunity—connecting the remaining 4 billions: a survey on rural connectivity. Preprint at https://arxiv.org/abs/1906.11541 (2019).
41. Mahmood, N. H. et al. Six key enablers for machine type communication in 6G. Preprint at https://arxiv.org/abs/1903.05406 (2019).
42. Rappaport, T. S. et al. Wireless communications and applications above 100 GHz: opportunities and challenges for 6G and beyond. IEEE Access 7, 78729–78757 (2019).
43. Stoica, R.-A. & de Abreu, G. T. F. 6G: the wireless communications network for collaborative and AI applications. Preprint at https://arxiv.org/abs/1904.03413 (2019).
44. Letaief, K. B., Chen, W., Shi, Y., Zhang, J. & Zhang, Y. A. The roadmap to 6G: AI empowered wireless networks. IEEE Commun. Mag. 57, 84–90 (2019).
45. Nawaz, S. J., Sharma, S. K., Wyne, S., Patwary, M. N. & Asaduzzaman, M. Quantum machine learning for 6G communication networks: state-of-the-art and vision for the future. IEEE Access 7, 46317–46350 (2019).
46. Renzo, D. et al. Smart radio environments empowered by reconfigurable AI meta-surfaces: an idea whose time has come. EURASIP J. Wireless Commun. Netw. 2019, 129 (2019).
47. Zhao, J. A Survey of intelligent reflecting surfaces (IRSs): towards 6G wireless communication networks. Preprint at https://arxiv.org/abs/1907.04789v3 (2019).
48. Nadeem, Q.-U.-A., Kammoun, A., Chaaban, A., Debbah, M. & Alouini, M.-S. Asymptotic max-min SINR analysis of reconfigurable intelligent surface assisted MISO systems. Preprint at https://arxiv.org/abs/1903.08127v3 (2019).
49. Nadeem, Q.-U.-A., Kammoun, A., Chaaban, A., Debbah, M. & Alouini, M.-S. Intelligent reflecting surface assisted wireless communication: modeling and channel estimation. Preprint at https://arxiv.org/abs/1906.02360v2 (2019).
50. Basar, E. Reconfigurable intelligent surface-based index modulation: a new beyond MIMO paradigm for 6G. Preprint at https://arxiv.org/abs/1904.06704v2 (2019).Oh, J., Thiel, M. & Sarabandi, K. Wave-propagation management in indoor environments using micro-radio-repeater systems. IEEE Antenn. Propag. Mag. 56, 76–88 (2014).
51. Dang, S., Ma, G., Shihada, B. & Alouini, M.-S. Enabling smart buildings by indoor visible light communications and machine learning. Preprint at https://arxiv.org/abs/1904.07959 (2019).
52. Ullah, S. et al. A comprehensive survey of wireless body area networks. J. Med. Syst. 36, 1065–1094 (2012).
53. Li, X., Hong, S., Chakravarthy, V. D., Temple, M. & Wu, Z. Intercarrier interference immune single carrier OFDM via magnitude-keyed modulation for high speed aerial vehicle communication. IEEE Trans. Commun. 61, 658–668 (2013).

54. Zhang, X., Cheng, W. & Zhang, H. Heterogeneous statistical QoS provisioning over airborne mobile wireless networks. IEEE J. Sel. Area. Commun. 36, 2139–2152 (2018).
55. Philbeck, I. Connecting the Unconnected: Working Together to Achieve Connect 2020 Agenda Targets. In Special Session of the Broadband Commission and the World Economic Forum at Davos Annual Meeting (Broadband Commission, 2017).
56. Gopal, R. & BenAmmar, N. Framework for unifying 5G and next generation satellite communications. IEEE Netw. 32, 16–24 (2018).
57. Dang, S., Coon, J. P. & Chen, G. Outage performance of two-hop OFDM systems with spatially random decode-and-forward relays. IEEE Access 5, 27514–27524 (2017).
58. Saeed, N., Celik, A., Al-Naffouri, T. Y. & Alouini, M.-S. Underwater optical wireless communications, networking, and localization: a survey. Ad Hoc Netw. 94, 101935 (2019).
59. Zeng, Z., Fu, S., Zhang, H., Dong, Y. & Cheng, J. A survey of underwater optical wireless communications. IEEE Commun. Surv. Tut. 19, 204–238 (2017).
60. Dohler, M. et al. Internet of skills, where robotics meets AI, 5G and the Tactile Internet. In Proc. IEEE EuCNC https://doi.org/10.1109/EuCNC.2017.7980645 (IEEE, 2017).
61. 5G communications for automation in vertical domains. 5G Americas https://go.nature.com/2th2xi0 (2018).
62. Voigtlander, F. et al. 5G for robotics: ultra-low latency control of distributed robotic systems. In Proc. IEEE ISCSIC 69–72 (IEEE, 2017).
63. Cheng, N. et al. Big data driven vehicular networks. IEEE Netw. 32, 160–167 (2018).
64. Wakunami, K. et al. Projection-type see-through holographic three-dimensional display. Nat. Commun. 7, 12954 (2016).
65. Simsek, M., Aijaz, A., Dohler, M., Sachs, J. & Fettweis, G. 5G-enabled tactile internet. IEEE J. Sel. Area. Commun. 34, 460–473 (2016).
66. Kim, K. S. et al. Ultrareliable and low-latency communication techniques for tactile Internet services. Proc. IEEE 107, 376–393 (2019).
67. Prasad, R. Human bond communication. Wireless Pers. Commun. 87, 619–627 (2016).
68. Khalid, M., Amin, O., Ahmed, S., Shihada, B. & Alouini, M.-S. Communication through breath: aerosol transmission. IEEE Commun. Mag. 57, 33–39 (2019).
69. Shi, H., Prasad, R. V., Onur, E. & Niemegeers, I. G. M. M. Fairness in wireless networks: issues, measures and challenges. IEEE Commun. Surv. Tut. 16, 5–24 (2014).
70. Haenggi, M., Andrews, J. G., Baccelli, F., Dousse, O. & Franceschetti, M. Stochastic geometry and random graphs for the analysis and design of wireless networks. IEEE J. Sel. Area. Commun. 27, 1029–1046 (2009).
71. Nadeem, Q.-U.-A., Kammoun, A. & Alouini, M.-S. Elevation beamforming with full dimension MIMO architectures in 5G systems: a tutorial. IEEE Commun. Surv. Tut. 21, 3238–3273 (2019).