ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 11| Issue: 8| August 2025|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2025: 8.691 || ISI Value: 1.188

CHALLENGES AND UTILITY OF NETWORK RESILIENCE IN 6G COMMUNICATIONS

Ashish Mishra[1], Dr. Ratnesh Kumar Jain[2]
[1]*Research Scholar,* [2]*Professor*
Department of Electronics and Communication Engineering, RKDF University, Bhopal

ABSTRACT

This research paper delves into the critical domain of network resilience within the context of the upcoming Sixth Generation (6G) communication networks. It defines 6G network resilience as the inherent ability of these advanced systems to anticipate, withstand, recover from, and adapt to diverse disruptions, ensuring continuous and high-quality service delivery for an increasingly interconnected world. The paper explores the unique demands and capabilities of 6G, highlighting its evolution from 5G and the imperative for resilience in supporting critical services and AI-native applications. It details architectural approaches such as resilience-by-design, self-healing mechanisms, the integration of non-terrestrial networks, and Zero-Trust frameworks. Key enabling technologies, including advanced Artificial Intelligence/Machine Learning, quantum networking for enhanced security and optimization, and Digital Twin (DT)-native networks for autonomous management, are thoroughly examined. Furthermore, the paper addresses significant challenges, including scalability, cost, an expanding attack surface, complex critical infrastructure interdependencies, and regulatory hurdles. Methods for measuring and evaluating 6G network resilience, focusing on quantitative metrics and service-oriented frameworks, are also discussed. Finally, the paper concludes with a forward-looking perspective on future research directions, emphasizing the necessity of embedding resilience into the very fabric of 6G networks to safeguard economic activity, public trust, and national security.

I. INTRODUCTION

1.1. The Imperative of 6G Network Resilience

Network resilience is rapidly becoming a strategic imperative for modern digital infrastructures, particularly as the world stands on the threshold of Sixth Generation (6G) communication networks. At its core, network resilience signifies a system's capacity to withstand, adapt to, and recover from various forms of adversity with minimal disruption to essential services. 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 National Institute of Standards and Technology (NIST) defines cyber resilience as the comprehensive 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.

Mobile networks are increasingly central to daily life, public safety, and crisis response efforts, making their resilience a shared priority. We are placing ever-greater demands on these networks, and the question is not merely whether they can hold under pressure, but whether they are adequately prepared for the evolving demands of an increasingly uncertain world. The pervasive integration of the Internet into nearly every facet of modern society means that any disruption carries increasingly severe ramifications, making enhancing the resilience and survivability of both current and future networks an urgent priority. 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.

1.2. Evolution from 5G to 6G: New Demands and Capabilities

The transition from 5G to 6G marks a significant evolution in network capabilities and demands for resilience. While 5G has laid foundational groundwork, 6G aims to provide even greater improvements in capability and reliability, unlocking a variety of innovative use cases that leverage advancements in AI and integrated sensing and communication. 6G networks will be built on the foundations of existing 5G and 5G-Advanced infrastructure, but will offer enhanced capabilities and introduce novel ones.

The increasing complexity of use cases in 6G, spanning differentiated quality of experience (QoE) needs, diverse application requirements, and the emergence of AI-native systems, demands a shift from ad hoc resilience measures to a "resilience-by-design" approach. In the 6G era, the network's role extends beyond enabling reliable connectivity; it becomes a critical enabler of intelligence flow between systems. Many anticipated 6G applications impose increasingly rigorous reliability demands and are highly time-critical, particularly in sectors such as manufacturing, surgical procedures, and critical infrastructures, where communication interruptions may lead to hazardous situations endangering lives.

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 11| Issue: 8| August 2025|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2025: 8.691 || ISI Value: 1.188

II. CORE PRINCIPLES OF 6G RESILIENCE

At its core, 6G network resilience embodies the ability to provide desired service even when challenged by attacks, large-scale disasters, and other failures. This concept is deeply integrated into the foundational design principles for 6G architecture, which include simplicity, modularity, trustworthiness, cloud-native approaches, and seamless migration from 5G. Nokia, for instance, proposes four core principles for 6G: value-centric, AI-native, sustainability-by-design, and security-by-design.

Specifically, a resilient design for 6G aims for an end-to-end architecture that is fully resilient to enable zero downtime and faster service delivery, extending resilience to the Radio Access Network (RAN). This involves a holistic blueprint for the 6G system architecture, guided by key design principles and technical frameworks for a lean, resilient, and secure system. The goal is to ensure that the network can absorb, adapt to, and recover from adversarial or challenging conditions.

2.1. Distinguishing 6G Resilience from Traditional Concepts

While related, 6G network resilience is a broader and more dynamic concept than traditional notions like reliability, robustness, and fault tolerance.

- **Reliability:** Aims to prevent failures.
- **Robustness:** Focuses on performing well during anticipated disturbances.
- **Fault Tolerance:** Involves designing a system to continue functioning despite the failure of one or more of its components.
- **Resilience:** Goes beyond these by emphasizing the network's ability to seamlessly cope with and recover from unforeseen failures and disruptions. It includes the capacity to adapt to changing conditions and withstand and recover rapidly from disruptions.

In the context of 6G, resilience is not just about preventing failures or enduring expected conditions; it's about dynamic adaptation and rapid recovery from the unpredictable. This means a resilient 6G network is designed to be adaptable, robust, and capable of learning from experiences to ensure continuous operation and minimal impact on users, even in challenging or adverse conditions.

III. ARCHITECTURAL APPROACHES FOR 6G NETWORK RESILIENCE

Achieving robust 6G network resilience necessitates a multi-faceted architectural approach that integrates proactive design principles and dynamic mechanisms.

3.1. Resilience-by-Design Paradigm

A fundamental paradigm shift is occurring from a traditional "secure-by-design" approach to a more comprehensive "resilience-by-design" model. The conventional "secure-by-design" mindset, which focuses on embedding security features from the outset, is no longer sufficient because the complex and evolving threat landscape makes preventing all cyberattacks unrealistic.

Instead, "resilience-by-design" aims to ensure that systems can withstand and recover from the inevitable attacks and disruptions that will occur. This involves embedding resilience principles into every stage of technology development and deployment, designing systems that can absorb attacks, maintain critical functions, and recover quickly with minimal impact. This approach emphasizes continuous monitoring, rapid response, and the ability to learn from incidents to strengthen defenses over time. For 6G, this means integrating notions of resilience and criticality from the ground up.

3.2. Self-Healing and AI-Powered Automation

Self-healing capabilities are a cornerstone of 6G resilience, enabling networks to detect and automatically respond to challenges, dynamically adapting to maintain service levels. 6G networks will rely heavily on AI-native operations to manage networks with minimal human intervention.
This includes:

- **Automatic Detection and Fixes:** The ability to automatically detect and fix issues (self-healing).
- **Predictive Optimization:** Adjusting performance in real-time.
- **Efficient Management:** Managing vast numbers of connected devices and services.

AI-powered automation is expected to make recovery faster and more flexible in 6G networks. This level of automation is essential as 6G networks grow in scale and complexity, ensuring higher reliability, lower operational costs, and faster response times, making the network smarter, more resilient, and instantly adaptable to changing demands.

3.3. Non-Terrestrial Networks (NTN) and Seamless Coverage

Achieving seamless coverage, especially in remote or non-line-of-sight areas (e.g., indoors, underground tunnels), remains a challenge for 6G. Full terrestrial network (TN) coverage is expensive, particularly in very remote locations.
6G aims to address this through:

- **Fallback Networks:** Seamless coverage will include the use of fallback networks, such as satellites, to provide basic mobile broadband everywhere.
- **Non-Terrestrial Network (NTN) Solutions:** Satellites can provide wide area coverage, albeit with limited capacity, in line-of-sight areas. An efficiently shared traffic uptake by a combination of large terrestrial cells and non-terrestrial satellite cells is an attractive solution for expanding network coverage.

3.4. Zero-Trust Frameworks

The rapid advancement in 6G networks, driven by the proliferation of distributed edge and fog computing, introduces unprecedented challenges in securing these decentralized

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 11| Issue: 8| August 2025|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2025: 8.691 || ISI Value: 1.188

architectures. Traditional security paradigms are often inadequate.

A Zero-Trust Framework for 6G Networks (ZTF-6G) is a novel model that integrates Zero-Trust principles to secure distributed edge and fog computing environments. It adopts a "never trust, always verify" approach, comprising adaptive authentication, continuous verification, and fine-grained access control against all entities within the network. This multi-layering extends to AI-driven anomaly detection and blockchain-based identity management for authentication and real-time monitoring of network interactions. ZTF-6G aims to maintain low latency while providing more resilience to insider threats, unauthorized access, and data breaches, which are key requirements of 6G networks.

3.5. Modular and Lean Architecture

To avoid unnecessary system complexity, 6G standards should focus on true multi-vendor interfaces and avoid duplication of functionalities in different network functions (NFs) and domains to enable a truly interoperable and lean system. A modularized design for 6G systems involves following a modular protocol design approach, where network functions are separated into strictly independent modules. This means 6G should be designed with a foundational protocols layer offering basic functionalities for low-cost devices, with enhanced functionalities built upon this layer for specific services.

IV. CHALLENGES AND LIMITATIONS IN ACHIEVING 6G RESILIENCE

Despite the advanced capabilities envisioned for 6G, achieving robust network resilience faces significant challenges.

4.1. Scalability, Cost, and Complexity

Building and maintaining resilient 6G networks is a complex undertaking, often constrained by issues of scale, financial investment, and architectural intricacy.

- **Scalability:** Ensuring a network can expand to smoothly manage increased demand without sacrificing performance or dependability presents a significant hurdle. A network that is resilient but not scalable may falter when demand exceeds its limits.
- **Cost:** Implementing comprehensive resilience measures, such as extensive redundancy, geographically diverse data centers, and advanced security tools, requires substantial financial investment. The economic pressures on telecom operators can lead to a fixation on short-term returns, potentially weakening the foundations of future resilience.
- **Complexity:** Modern networks are inherently complex, especially with the shift towards distributed systems, hybrid cloud, and multi-cloud environments. The increasing number of software applications and accelerated change in disaggregated and virtualized networks add further complexity, particularly in the network's management plane, where new software-based vulnerabilities can emerge with network-wide impacts.

4.2. Expanding Attack Surface and Evolving Threats

The digital transformation and proliferation of connected devices are expanding the potential entry points for cyberattacks, making network defense increasingly challenging for 6G.

- **Expanding Attack Surface:** The anticipated surge of Internet of Things (IoT) devices, projected to surpass 32 billion globally by 2030, introduces countless potential entry points for cyberattacks, significantly expanding the digital attack surface. Each additional node in an expanding network introduces potential vulnerabilities.
- **Evolving Threats:** Cyber threats are becoming more sophisticated, requiring continuous adaptation of defense strategies. Attackers constantly seek to exploit new vulnerabilities, including zero-day exploits. The interconnected nature of emerging technologies, such as AI, quantum computing, and IoT, further expands this attack surface and introduces novel vulnerabilities. AI systems, for instance, introduce new vulnerabilities such as data poisoning, model manipulation, and adversarial attacks. Quantum computing poses significant threats to current encryption methods, with some actors already harvesting encrypted data for future decryption.

4.3. Critical Infrastructure Interdependencies

The deep interconnections among critical infrastructure systems (e.g., communications, energy, transportation, healthcare, financial services) can amplify negative effects during a crisis, leading to cascading failures.

- **Unforeseen Spillover Effects:** A major cyberattack on one sector can have difficult-to-predict spillover effects on others. For example, the energy sector is "super critical" because most other sectors cannot operate without it, yet other sectors may underestimate their dependency on energy data, assuming backups will suffice for brief outages, leaving them unprepared for extended disruptions.
- **Data Flow Threats:** The functioning of critical infrastructure heavily depends on communication and data exchange. Threats to data availability (whether data can be accessed when needed) and confidentiality/integrity (data being disclosed or changed without authorization) are significant.
- **Management Challenges:** Effective management of these interdependencies is hampered by fragmented initiatives, a lack of integrated decision support systems, and challenges in data sharing due to commercial, security, and proprietary concerns. There is often a bias in decision-making, where sectors focus on their internal network dependencies rather than their interconnectedness with other infrastructures, leading to neglect of cascading failures.

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 11| Issue: 8| August 2025|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2025: 8.691 || ISI Value: 1.188

4.4. Regulatory and Governance Challenges

Ensuring 6G network resilience often intersects with complex regulatory and governance frameworks, which may not keep pace with technological advancements and evolving threats.

- **Outdated Frameworks:** Current regulatory frameworks are often ill-equipped for the uncertainties, transboundary nature, and rapid pace of risks in an increasingly interconnected world. Narrow, sector-based regulations can lose relevance in hyperconnected environments, potentially escalating issues or stifling innovation.
- **Prioritization Dilemmas:** Regulators face political dilemmas, such as balancing investments needed for resilience against immediate cost impacts on consumers.
- **Need for New Governance Models:** There is a growing interest in reimagining regulatory systems to enhance resilience, moving towards polycentric governance designs that emphasize self-organization, timely adaptive responses, and leveraging diverse knowledge through collaboration and cooperation. This approach suggests a central authority to orchestrate multiple semi-autonomous decision centers, including independent regulators, to strengthen the resilience of essential functions.

V. MEASUREMENT AND EVALUATION OF 6G NETWORK RESILIENCE

Measuring and evaluating 6G network resilience is essential for understanding a network's strengths and weaknesses, tracking progress, and prioritizing improvements. This involves a combination of quantitative metrics and structured evaluation frameworks.

5.1. Quantitative Metrics and SLAs

Quantitative metrics provide measurable factors to assess how resilient a network is. For 6G, these metrics will be crucial for specifying and tracking Service Level Agreements (SLAs).
Key metrics include:

- **Uptime Percentage:** The percentage of time the network is operational. Tier 1 telecom operators often target 99.999 percent or higher core network availability.
- **Mean Time to Repair (MTTR):** The average time it takes to fix an issue.
- **Mean Time Between Failures (MTBF):** The expected mean time between successive failures.
- **Recovery Time Objective (RTO):** The maximum tolerable duration of time in which a business process can be down following a disaster.
- **Failure Impact:** How much a failure disrupts overall network performance or user experience.
- **Structural Metrics:** Such as node degree, edge connectivity, and largest connected component ratio, which describe the network's stability when links or nodes are removed.
- **Centrality Metrics:** Like betweenness centrality and closeness centrality, which identify the importance of nodes or links.
- **Functional Metrics:** Measuring network performance and response to failures, often focusing on Quality of Service (QoS) parameters like packet loss, throughput, jitter, and delay.

Observability parameters will be crucial for specifying the desired details of end-to-end (E2E) SLAs between providers and consumers, building trust by consistently delivering on these SLAs.

5.2. Service-Oriented Frameworks

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

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. For 6G, a core resilience strategy, a unified resilience metric, different criterion for service criticality, and prioritization frameworks are being developed to augment resilience prospects.

This framework aims to provide robust security, low latency, and enhanced resilience against insider threats, unauthorized access, and data breaches, which are critical requirements for 6G networks.

VI. CONCLUSION

Network resilience has transitioned from a technical consideration to a strategic imperative, particularly with the advent of 6G communication networks. The increasing societal and economic reliance on interconnected digital infrastructures for critical services means that disruptions carry profound and cascading consequences, impacting not only financial stability but also 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 6G network resilience requires a comprehensive, multi-layered approach. This involves a deep understanding of the diverse threat landscape, encompassing sophisticated

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 11| Issue: 8| August 2025|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2025: 8.691 || ISI Value: 1.188

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 the "resilience-by-design" paradigm, self-healing mechanisms, the integration of non-terrestrial networks, and Zero-Trust frameworks, are foundational. These are increasingly augmented by advanced technologies and protocols, including advanced Artificial Intelligence/Machine Learning for proactive threat detection and automated response, quantum networking for enhanced security and optimization, and Digital Twin (DT)-native networks for autonomous management and "future shots."

Measuring and evaluating 6G network resilience is crucial for continuous improvement, utilizing a blend of quantitative metrics (e.g., uptime, MTTR, structural, centrality, and functional indicators) and service-oriented evaluation frameworks. However, significant challenges persist, including the inherent complexities of scaling resilient networks, managing escalating costs, navigating an ever-expanding attack surface, addressing the intricate interdependencies of critical infrastructure, and overcoming regulatory and governance hurdles.

REFERENCES

1. *Zhang, Z., Xiao, Y., Ma, Z., Xiao, M., Ding, Z., Lei, X., Fan, P., & Poor, H. V. (2019). 6G Wireless Networks: ision, Requirements, Architecture, and Key Technologies.* ***IEEE Vehicular Technology Magazine****, 14(3), 28–41. https://doi.org/10.1109/MVT.2019.2921208*
2. *Saeed, N., Bader, A., & Al-Naffouri, T. Y. (2021). Machine Learning for Intelligent Network Management in 6G: A Survey on Applications, Challenges, and Future Research Directions.* ***IEEE Open Journal of the Communications Society****, 2, 1336–1363. https://doi.org/10.1109/OJCOMS.2021.3088586*
3. *Yang, Y., Xiao, Y., Xiao, M., & Li, S. (2021). 6G Wireless Communications: Vision and Potential Techniques.* ***IEEE Network****, 35(1), 4–11. https://doi.org/10.1109/MNET.011.2000254*
4. *Zhang, Y., Wang, Y., Wang, K., & Liu, M. (2022). Security and Privacy in 6G Networks: Challenges and Solutions.* ***IEEE Wireless Communications****, 29(4), 72–79. https://doi.org/10.1109/MWC.006.2100535*
5. *Sterbenz, J. P. G., Hutchison, D., Çetinkaya, E. K., Jabbar, A., Rohrer, J. P., Schöller, M., & Smith, P. (2010). Resilience and Survivability in Communication Networks: Strategies, Principles, and Survey of Disciplines.* ***Computer Networks****, 54(8), 1245–1265. https://doi.org/10.1016/j.comnet.2010.03.005*
6. *Alwis, C. D., & Kalla, A. (2022). Digital Twins for 6G: Requirements, Applications, and Challenges.* ***IEEE Internet of Things Journal****, 9(1), 321–338. https://doi.org/10.1109/JIOT.2021.3106451*
7. *You, C., Huang, K., & Chae, H. (2021). Energy-Efficient Wireless Edge Intelligence for 6G Networks.* ***IEEE Wireless Communications****, 28(3), 40–47. https://doi.org/10.1109/MWC.101.2000480*
8. *M. Steinder et al. A survey of fault localization techniques in computer networks Science of Computer Programming (2004)*
9. *I.F. Akyildiz et al. Wireless sensor networks: a survey Computer Networks (2002)*
10. *S. Rinaldi et al. Identifying, understanding, and analyzing critical infrastructure interdependencies IEEE Control Systems Magazine (2001)*
11. *P.E. Heegaard, K.S. Trivedi, Network Survivability Modeling, Computer Networks 53(8) (2009) 1215–1234, ISSN 1389-1286.*
12. *Ahanger, T.A., 2018. An effective approach to detecting DDoS using artificial neural networks. Proceedings of the International Conference on Wireless Communications, Signal Processing and Networking, Mar. 22-24, IEEE Xplore Press, Chennai, India. DOI: 10.1109/WISPNET.2017.8299853*
13. *Al-Issa, A.I., M. Al-Akhras, M.S. Alsahli and M. Alawairdhi, 2019. Using machine learning to detect dos attacks in wireless sensor networks. Proceedings of the Jordan International Joint Conference on Electrical Engineering and Information Technology, Apr. 9-11, IEEE Xplore Press, Amman, Jordan, pp: 107-112. DOI: 10.1109/JEEIT.2019.8717400*
14. *Aljumah, A. and T. Ahamad, 2016. A novel approach for detecting DDoS using artificial neural networks. Int. J. Comput. Sci. Network Security, 16: 132-132.*
15. *Alrajeh, N.A. and J. Lloret, 2013. Intrusion detection systems based on artificial intelligence techniques in wireless sensor networks. Int. J. Distributed Sensor Networks.*
16. *Alsheikh, M.A., S. Lin, D. Niyato and H.P. Tan, 2014. Machine learning in wireless sensor networks: Algorithms, strategies and applications. Commun. Surveys Tutorials, 16: 1996-2018. DOI: 10.1109/COMST.2014.2320099*
17. *Ashikur, M. and S. Maruful, 2017. Intrusion detection system for wireless ADHOC network using time series techniques. Int. J. Comput. Applic., 162: 1-5. DOI: 10.5120/IJCA2017913408*
18. *Baig, Z.A., M. Baqer and A.I. Khan, 2006. A Pattern recognition scheme for Distributed Denial of Service (DDoS) attacks in wireless sensor networks.*
19. *Barki, L., A. Shidling, N. Meti, D.G. Narayan and M.M. Mulla, 2016. Detection of distributed denial of service attacks in software defined networks.*
20. *Proceedings of the International Conference on Advances in Computing, Communications and Informatics, Sept. 21-24, IEEE Xplore Press, Jaipur, India. DOI: 10.1109/ICACCI.2016.7732445*
21. *Cheng, B., L. Cui, W. Jia, W. Zhao and P.H. Gerhard, 2016. Multiple region of interest coverage in camera sensor networks for tele-intensive care units. Trans. Industrial Inform., 12: 2331-2341. DOI: 10.1109/TII.2016.2574305*
22. *Das, S., A. Abraham and B.K. Panigrahi, 2010. Computational intelligence: Foundations, perspectives and recent trends. Comput. Intell. Patt. Anal. Biol. Inform.*
23. *Di, M. and M.J. Er, 2007. A survey of machine learning in wireless sensor networks-from networking and application perspectives.*
24. *Proceedings of the 6th International Conference on Information, Communications and Signal Processing, Dec. 10-13, IEEE Xplore Press, Singapore. DOI: 10.1109/ICICS.2007.4449882*