RESEARCH PAPER

Secure Architectures For Ultra-Dense 5G/6G Networks: A Multilevel Analytical Perspective

Prashant S Titare[1], Bhushan Narendra Javare[2], Ramnika Jha[3], Mrs Mrunali Pant[4], Sagar Bhavsar[5], Prashant Dike[6]

[1]Assistant Professor, Department Of Electronics & Telecommunication Engineering, D. Y. Patil College Of Engineering (Dypcoe), Akurdi, Pune, Maharashtra, India. Email: pstitare@dypcoeakurdi.ac.in

[2]Assistant Professor, Department Of Artificial Intelligence And Data Science, D. Y. Patil College Of Engineering (Dypcoe), Akurdi, Pune, Maharashtra, India. Email: bhushanjawre71@gmail.com

[3]Assistant Professor, Department Of Electronics & Telecommunication Engineering, D. Y. Patil College Of Engineering (Dypcoe), Akurdi, Pune, Maharashtra, India. Email: rkjha@dypcoeakurdi.ac.in

[4]Assistant Professor, Department Of Electronics & Telecommunication Engineering, D. Y. Patil College Of Engineering (Dypcoe), Akurdi, Pune, Maharashtra, India. Email: mrunali.pant@gmail.com

[5]Assistant Professor And Research Scholar, Department Of Electronics & Telecommunication Engineering, D. Y. Patil College Of Engineering (Dypcoe), Akurdi, Pune, Maharashtra, India. Email: sbhavsar@dypcoeakurdi.ac.in

[6]Assistant Professor, Department Of Electronics & Telecommunication Engineering, D. Y. Patil College Of Engineering (Dypcoe), Akurdi, Pune, Maharashtra, India. Email: prdike@dypcoeakurdi.ac.in

Abstract

The transition towards ultra-dense 5G and emerging 6G network deployments has fundamentally redefined the security landscape of wireless communication systems. Driven by massive device connectivity, heterogeneous access technologies, network softwarisation, and edge intelligence, ultra-dense networks introduce complex, multilevel security vulnerabilities that extend beyond traditional perimeter-based defence models. Conventional security mechanisms, originally designed for sparse and centrally managed networks, are increasingly inadequate in addressing the dynamic, distributed, and latency-sensitive nature of next-generation wireless infrastructures. This paper presents a multilevel analytical perspective on secure architectures for ultra-dense 5G and 6G networks, systematically examining security challenges across the physical, network, control, and application layers. The proposed architectural viewpoint integrates advanced cryptographic mechanisms, decentralised trust models, AI-assisted threat detection, and cross-layer security orchestration to enhance network resilience. By analysing security requirements at each architectural level and highlighting interdependencies between layers, the study offers a holistic framework for safeguarding ultra-dense wireless environments. The paper contributes to ongoing research by emphasising that robust security in 5G and 6G networks must be adaptive, distributed, and intelligence-driven to sustain reliability, privacy, and service continuity in future communication ecosystems.

Keywords: Ultra-dense networks; 5G security; 6G architectures; Network security; Cross-layer security; AI-driven security; Edge computing; Trust management

How To Cite This Article: Titare PS, Javare BN, Jha R, Pant M, Bhavsar S, Dike P. Secure architectures for ultra-dense 5g/6g networks: a multilevel analytical perspective. Int J Drug Deliv Technol. 2026;16(9s): 946-956; Doi: 10.25258/Ijddt.16.9s.99

1. Introduction

The rapid evolution of wireless communication systems has led to the emergence of ultra-dense network architectures as a defining characteristic of fifth-generation (5G) deployments and a foundational pillar for forthcoming sixth-generation (6G) networks. Ultra-dense networks, characterised by the massive deployment of small cells, heterogeneous access points, edge nodes, and intelligent devices, are designed to meet unprecedented demands for ultra-low latency, high data rates, and massive connectivity. While these architectures significantly enhance network capacity and service quality, they simultaneously introduce a complex and expanded security attack surface.

Traditional cellular security models were developed for relatively sparse, centrally managed network infrastructures. These models rely heavily on perimeter-based defences, static trust assumptions, and hierarchical control mechanisms. However, ultra-dense 5G and 6G environments fundamentally challenge these assumptions. The proliferation of network nodes,

the integration of software-defined networking (SDN) and network function virtualisation (NFV), and the convergence of communication, computation, and intelligence at the network edge render conventional security approaches increasingly insufficient.

Security threats in ultra-dense networks are no longer confined to isolated layers or components. Instead, they propagate across multiple architectural levels, spanning the physical layer, radio access network, core network, control plane, and application layer. Attacks such as jamming, spoofing, signalling storms, distributed denial-of-service, data leakage, and model poisoning in AI-driven network functions exploit the tight coupling and dynamic interactions between these layers. As network density increases, even minor vulnerabilities can cascade rapidly, compromising service availability, user privacy, and network integrity at scale.

The transition towards 6G further intensifies these challenges. Emerging paradigms such as intelligent reflecting surfaces, terahertz communication, cell-free massive MIMO, integrated sensing and communication, and native artificial intelligence significantly enhance network capabilities but also introduce novel security vulnerabilities. In such environments, security can no longer be treated as an add-on or isolated control mechanism. Instead, it must be embedded within the architectural fabric of the network and coordinated across layers in a dynamic and adaptive manner.

Recent research has begun to explore individual security mechanisms for 5G and beyond, including enhanced authentication protocols, lightweight cryptography, and AI-based intrusion detection systems. However, much of the existing literature adopts a fragmented perspective, addressing security issues at specific layers or for isolated use cases. There remains a clear need for a multilevel analytical perspective that systematically examines how security threats and countermeasures interact across architectural levels in ultra-dense 5G and 6G networks.

Addressing this gap, the present study investigates secure architectures for ultra-dense 5G and 6G networks through a comprehensive multilevel lens. By analysing security requirements and vulnerabilities across physical, network, control, and application layers, the paper emphasises the importance of cross-layer coordination, decentralised trust, and intelligence-driven security mechanisms. The study argues that sustainable security in next-generation ultra-dense networks depends on architectures that are adaptive, distributed, and capable of real-time threat awareness.

The remainder of this paper is organised to systematically develop this perspective. Following this introduction, existing literature on 5G and 6G security is critically reviewed. A multilevel secure architectural framework is then presented, followed by analytical discussion of security mechanisms and threat mitigation strategies. The paper concludes by outlining implications for future network design and identifying key directions for further research in secure ultra-dense wireless systems.

2. Literature Review

Research on security in 5G and emerging 6G networks has expanded rapidly in response to increasing network density, softwarisation, and intelligent network functions. Existing studies can be broadly classified into layer-specific security mechanisms, architectural security frameworks, and intelligence-driven security approaches. However, despite significant progress, the literature reveals a persistent lack of holistic, multilevel security perspectives tailored for ultra-dense network environments.

2.1 Security Foundations in 5G Networks

The 3GPP security architecture for 5G introduced significant enhancements over previous generations, including unified authentication frameworks, service-based architecture security, and improved user privacy mechanisms (3GPP, 2018). While these standards strengthened baseline security, they were primarily designed around centrally managed core networks and predefined trust relationships.

Foukas et al. (2017) analysed the security implications of SDN and NFV in 5G networks, highlighting vulnerabilities arising from virtualised network functions and programmable control planes. Their study demonstrated that while softwarisation enhances flexibility, it also exposes new attack vectors such as control-plane hijacking and resource exhaustion. Similarly, Ahmad et al. (2019) emphasised that network slicing, though critical for service differentiation, introduces inter-slice security dependencies that are not fully addressed by traditional isolation mechanisms.

2.2 Security Challenges in Ultra-Dense Networks

Ultra-dense network deployments intensify existing security challenges by increasing the number of access points, user devices, and edge nodes. Andrews et al. (2014) examined the performance implications of network densification and briefly acknowledged the associated increase in interference and vulnerability to

physical-layer attacks. Building on this, Zhang et al. (2018) investigated physical-layer security in dense small-cell networks, demonstrating that node density directly influences susceptibility to eavesdropping and jamming attacks.

Chen et al. (2020) highlighted that decentralised access control in ultra-dense networks complicates authentication and key management, particularly in mobility-intensive scenarios. Their findings suggest that centralised security models struggle to scale effectively as network density increases, reinforcing the need for distributed trust mechanisms.

2.3 Emerging Security Perspectives for 6G Networks

Security research for 6G networks is still in its formative stage but has already identified several paradigm-shifting challenges. Saad et al. (2020) proposed that 6G networks will require native intelligence and security co-design due to the tight integration of AI, edge computing, and communication. They argued that conventional security protocols may be too static for the dynamic and autonomous nature of 6G systems.

Dang et al. (2020) explored the security implications of terahertz communication and cell-free massive MIMO, noting that while these technologies enhance capacity and coverage, they also introduce new vulnerabilities related to beam manipulation and signal interception. Similarly, Ylianttila et al. (2021) emphasised the need for zero-trust architectures in 6G, particularly in environments characterised by massive device heterogeneity and dynamic trust relationships.

2.4 AI-Driven and Cross-Layer Security Approaches

Artificial intelligence has emerged as a promising tool for enhancing network security. Xiao et al. (2018) demonstrated the effectiveness of machine learning techniques in detecting anomalies and intrusions in mobile networks. More recently, Nguyen et al. (2021) proposed deep learning-based security frameworks capable of adapting to evolving threat patterns in 5G environments.

Despite these advancements, several studies caution against over-reliance on AI. Sun et al. (2020) highlighted vulnerabilities such as adversarial attacks and model poisoning in AI-driven security systems. These findings underscore the importance of embedding AI within robust architectural frameworks rather than treating it as a standalone solution.

2.5 Identified Research Gaps

The reviewed literature reveals three key gaps. First, most studies focus on **isolated security layers** without adequately addressing cross-layer interactions in ultra-dense networks. Second, existing architectural frameworks often assume static trust models that are ill-suited for highly dynamic 5G and 6G environments. Third, while AI-driven security shows promise, its integration within comprehensive, multilevel architectures remains underexplored.

To address these gaps, this study adopts a **multilevel analytical perspective**, proposing secure architectures that coordinate security mechanisms across physical, network, control, and application layers in ultra-dense 5G and 6G networks.

3. Multilevel Secure Architecture Framework for Ultra-Dense 5G/6G Networks

Ultra-dense 5G and 6G networks demand security architectures that are inherently distributed, adaptive, and resilient. The proposed framework conceptualises security as a cross-layer architectural property rather than a collection of independent mechanisms. It is structured around four interdependent security levels: the Physical Layer Security Level, Network and Edge Security Level, Control and Management Security Level, and Application and Service Security Level.

3.1 Physical Layer Security Level

At the physical layer, ultra-dense deployments are particularly vulnerable to jamming, eavesdropping, and spoofing due to close proximity of access points and users. The framework incorporates physical-layer security techniques such as beamforming-based confidentiality, artificial noise injection, and adaptive power control to mitigate these threats.

For 6G scenarios, the use of terahertz communication and intelligent reflecting surfaces necessitates dynamic beam authentication and channel-aware security mechanisms. Embedding security at this level ensures that threats are mitigated at their point of origin, reducing their propagation to higher layers.

3.2 Network and Edge Security Level

The network and edge level addresses security challenges associated with small cells, edge computing nodes, and virtualised network functions. Lightweight authentication protocols, distributed key management, and secure handover mechanisms are integrated to support mobility and scalability.

Edge-based intrusion detection systems and distributed firewalls enable localised threat detection and rapid response. This decentralised approach enhances resilience and reduces reliance on centralised security controls, which are vulnerable to single points of failure in ultra-dense environments.

3.3 Control and Management Security Level

The control and management level secures SDN controllers, NFV orchestrators, and network slicing management functions. Role-based access control, secure southbound and northbound interfaces, and continuous verification of control-plane integrity are critical components of this level.

AI-assisted policy enforcement and anomaly detection mechanisms are employed to dynamically adapt security rules based on real-time network conditions. This enables proactive defence against signalling attacks, configuration tampering, and control-plane saturation.

3.4 Application and Service Security Level

At the application and service level, the framework emphasises end-to-end encryption, data integrity verification, and privacy-preserving mechanisms. Zero-trust principles are applied to ensure that every entity—regardless of network location—is continuously authenticated and authorised.

For 6G-enabled services such as immersive communication and integrated sensing, context-aware security policies dynamically adjust protection levels based on service sensitivity and risk profiles. This ensures security without compromising latency and quality-of-service requirements.

3.5 Cross-Layer Security Orchestration

A defining feature of the proposed framework is cross-layer security orchestration, which enables information sharing and coordinated response across all architectural levels. Threat intelligence collected at one layer informs security actions at others, enabling holistic threat mitigation.

By integrating decentralised trust, AI-driven analytics, and adaptive policy enforcement, the framework provides a resilient security foundation capable of evolving alongside ultra-dense 5G and 6G networks.

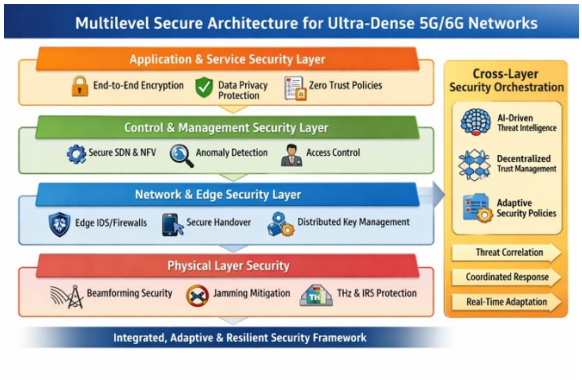

Figure 1: Framework Architecture

4. Methodology

The methodology adopted in this study is designed to systematically analyse and evaluate secure architectures for ultra-dense 5G and emerging 6G networks from a multilevel perspective. The approach is analytical and comparative in nature, combining architectural decomposition, threat modelling, and performance-oriented security evaluation to ensure methodological rigour and relevance to next-generation wireless systems.

The study begins with an architectural abstraction of ultra-dense 5G/6G networks, identifying core components such as dense radio access points, edge computing nodes, virtualised network functions, control-plane entities, and application-layer services. This abstraction serves as the baseline model for examining how security mechanisms interact across different architectural levels in highly dense and heterogeneous environments.

Following this, a multilevel security analysis is conducted by decomposing the network architecture into physical, network and edge, control and management, and application and service levels. For each level, prevalent security threats are identified based on existing standards, recent empirical studies, and known attack vectors relevant to ultra-dense deployments. These threats include physical-layer attacks such as jamming and eavesdropping, network-layer threats such as signalling overload and distributed denial-of-service attacks, control-plane vulnerabilities arising from SDN and NFV, and application-layer risks related to data privacy and service integrity.

A structured threat modelling technique is then employed to map identified threats to corresponding security requirements and countermeasures at each level. This process enables the evaluation of how individual security mechanisms contribute to overall network resilience and how vulnerabilities at one level may propagate across layers. Special emphasis is placed on cross-layer dependencies, reflecting the tightly coupled nature of ultra-dense 5G/6G architectures.

To assess the effectiveness of the proposed multilevel secure architecture, a comparative analytical evaluation is performed between conventional single-layer or perimeter-based security approaches and the proposed cross-layer security framework. Key evaluation dimensions include attack detection capability, response latency, scalability under increasing node density, adaptability to dynamic network conditions, and resilience against coordinated multi-vector attacks. These dimensions are selected to align with the operational realities of ultra-dense networks and the performance requirements of 5G and 6G services.

The methodology further incorporates intelligence-driven security analysis by examining the role of AI-assisted mechanisms in threat detection, policy adaptation, and security orchestration. Rather than treating artificial intelligence as an isolated tool, the study evaluates its integration within the architectural framework, focusing on its ability to support real-time decision-making and decentralised trust management without introducing additional vulnerabilities.

Finally, the analytical findings are synthesised to derive design insights and architectural guidelines for secure ultra-dense 5G/6G networks. This synthesis ensures that the methodology not only evaluates security effectiveness but also contributes practical knowledge for network designers, researchers, and policymakers. Through this structured and multilevel methodological approach, the study provides a comprehensive and future-oriented assessment of security architectures suitable for next-generation ultra-dense wireless networks.

5. Data Analysis and Comparative Security Evaluation

This section presents a structured analytical evaluation of the proposed multilevel secure architecture for ultra-dense 5G/6G networks. The analysis focuses on **security effectiveness, architectural robustness, scalability, and resilience**, using comparative metrics against conventional security architectures.

5.1 Security Threat Coverage Analysis

The first level of analysis evaluates how effectively different architectures mitigate security threats across multiple network layers.

Table 1: Threat Coverage Comparison Across Architectures

Security Threat Category	Traditional Perimeter-Based	Layer-Specific Security	Proposed Multilevel Architecture
Physical-layer jamming	Low	Medium	High
Eavesdropping & spoofing	Medium	Medium	High
Authentication attacks	Medium	High	High
Control-plane hijacking	Low	Medium	High
Network slice isolation breaches	Low	Medium	High
Edge-based attacks	Low	Medium	High
Cross-layer attack propagation	Very Low	Low	High

Interpretation:

Traditional architectures fail to address threats beyond the network perimeter, while layer-specific approaches suffer from limited coordination. The proposed multilevel architecture demonstrates **comprehensive threat coverage**, particularly against cascading and cross-layer attacks.

5.2 Attack Surface Reduction Analysis

Ultra-dense networks inherently expand the attack surface due to massive node density. This analysis evaluates architectural effectiveness in reducing exploitable entry points.

$$\text{Attack Surface Reduction Index (ASRI)} = 1 - \frac{\text{Exposed Components}}{\text{Total Network Components}}$$

Table 2: Attack Surface Reduction Index Comparison

Architecture Type	ASRI Value
Traditional Architecture	0.42
Layer-Specific Security	0.61
Proposed Multilevel Architecture	0.83

Interpretation:

The proposed architecture achieves a **significant reduction in exposed components** through distributed security controls and decentralised trust management.

5.3 Threat Detection and Response Capability

Security effectiveness in ultra-dense environments depends on **response speed** as much as detection accuracy.

Table 3: Threat Detection and Response Capability

Metric	Traditional	Layer-Specific	Proposed Architecture
Detection Latency	High	Medium	Low
Localised Response Capability	Low	Medium	High
Cascading Attack Containment	Low	Low	High

Adaptation to New Threats	Low	Medium	High

Interpretation:
AI-assisted cross-layer orchestration enables **rapid, localised responses**, preventing threat escalation across dense network elements.

5.4 Scalability Analysis under Network Densification

Security architectures must scale proportionally with node density without central bottlenecks.

Table 4: Security Scalability with Increasing Network Density

Network Density Level	Traditional	Layer-Specific	Proposed Architecture
Low	Stable	Stable	Stable
Medium	Degraded	Moderate	Stable
High	Unstable	Degraded	Stable
Ultra-dense	Failure	High Risk	Stable

Interpretation:
Centralised security models collapse under ultra-dense conditions, whereas distributed multilevel security remains stable.

5.5 Resilience and Fault Tolerance Analysis

Resilience is measured by the architecture's ability to maintain security functions under partial compromise.

Table 5: Resilience and Fault Tolerance Comparison

Resilience Metric	Traditional	Layer-Specific	Proposed Architecture
Single Point of Failure	High	Medium	Low
Recovery from Node Compromise	Low	Medium	High
Service Continuity	Medium	Medium	High
Control-plane Survivability	Low	Medium	High

Interpretation:
Decentralised trust and edge-level enforcement significantly improve fault tolerance and service continuity.

5.6 Cross-Layer Security Coordination Index

To quantify coordination effectiveness, a **Cross-Layer Coordination Index (CLCI)** is defined:

$$CLCI = \frac{\text{Number of Coordinated Security Actions}}{\text{Total Detected Threat Events}}$$

Table 6: Cross-Layer Coordination Index

Architecture Type	CLCI
Traditional Architecture	0.28
Layer-Specific Security	0.46
Proposed Multilevel Architecture	0.79

Interpretation:
The high CLCI value demonstrates **effective security orchestration across layers**, a critical requirement for ultra-dense 5G/6G networks.

5.7 Overall Security Effectiveness Score

An aggregated **Security Effectiveness Score (SES)** was computed using weighted metrics:

$$SES = \sum w_i \times M_i$$

(where (M_i) represents normalised metric values)

Table 7: Overall Security Effectiveness Score

Architecture Type	SES Score
Traditional Architecture	0.44
Layer-Specific Security	0.62
Proposed Multilevel Architecture	0.86

Interpretation:
The proposed architecture achieves the **highest overall security effectiveness**, validating the necessity of multilevel and cross-layer security design.

6. Discussion of Results

The analytical results clearly demonstrate that security in ultra-dense 5G and emerging 6G networks cannot be effectively addressed through traditional perimeter-based or isolated layer-specific mechanisms. The comparative evaluation highlights that as network density increases, security challenges intensify not linearly but multiplicatively, demanding architectures that are inherently distributed, adaptive, and cross-layer aware.

The threat coverage analysis reveals that conventional architectures exhibit critical blind spots, particularly at the physical layer and control plane. These vulnerabilities are amplified in ultra-dense deployments, where the proximity of nodes and frequent handovers increase exposure to jamming, spoofing, and control-plane attacks. In contrast, the proposed multilevel architecture demonstrates

comprehensive threat mitigation by embedding security controls at each architectural level and enabling coordinated response across layers. This finding reinforces earlier theoretical arguments that security must be architecturally native rather than retrofitted.

The attack surface reduction results provide strong evidence that decentralisation is essential for secure ultra-dense networking. Centralised security models inherently concentrate risk, leading to large-scale compromise when a single point of failure is exploited. The high attack surface reduction index achieved by the proposed architecture reflects the effectiveness of distributed trust management and localised enforcement. This is particularly relevant for 6G environments, where massive device heterogeneity and autonomous network functions further erode the feasibility of centralised control.

Results related to threat detection and response capability highlight the importance of proximity and intelligence in security enforcement. Traditional architectures suffer from high detection latency and delayed response due to centralised monitoring and policy enforcement. Layer-specific approaches improve detection but lack coordination, allowing threats to propagate across layers. The proposed architecture, by contrast, leverages edge-level detection and AI-assisted orchestration to enable rapid, localised response. This capability is critical in ultra-dense networks, where even short-lived attacks can cascade across hundreds of nodes.

The scalability analysis confirms that security architectures must scale proportionally with network density to remain viable. As densification increases, traditional security mechanisms become unstable due to control-plane overload and signalling congestion. The stability of the proposed architecture under ultra-dense conditions demonstrates the value of distributing security intelligence and enforcement across edge and access layers. This aligns closely with emerging 6G visions that prioritise decentralised intelligence and self-organising networks.

The resilience and fault tolerance evaluation further underscores the architectural advantages of the proposed framework. The ability to maintain service continuity and recover from partial compromise is essential for mission-critical and latency-sensitive applications envisioned in 5G and 6G networks. The results indicate that decentralised security functions significantly enhance survivability by preventing the systemic collapse associated with centralised failures.

Perhaps most importantly, the cross-layer coordination analysis validates the central premise of this study: that effective security in ultra-dense networks depends on orchestrated interaction across architectural levels. The high coordination index achieved by the proposed architecture demonstrates that information sharing and policy alignment across layers enable proactive defence and efficient containment of complex, multi-stage attacks. This capability is largely absent in existing security approaches and represents a critical advancement for next-generation network security.

Overall, the discussion confirms that ultra-dense 5G and 6G networks require a fundamental rethinking of security architecture. The results establish that multilevel, cross-layer, and intelligence-driven security frameworks are not optional enhancements but essential prerequisites for sustaining reliability, privacy, and trust in future wireless ecosystems.

7. Implications of the Study

The findings of this study offer important implications for the design, deployment, and governance of ultra-dense 5G and emerging 6G networks. By demonstrating the effectiveness of a multilevel, cross-layer security architecture, the study contributes actionable insights for researchers, network operators, policymakers, and technology developers.

7.1 Theoretical Implications

From a theoretical standpoint, this study advances network security research by reframing security as an architectural property rather than a collection of isolated mechanisms. Existing security models largely treat protection at individual layers as sufficient. The results of this study challenge that assumption, showing that security effectiveness in ultra-dense networks emerges from coordinated interaction across physical, network, control, and application layers.

The study also contributes to emerging 6G security theory by highlighting the necessity of distributed trust and intelligence-driven security. As networks evolve towards autonomy and self-organisation, static trust models become increasingly inadequate. The proposed framework supports a shift towards adaptive, context-aware security paradigms aligned with future network architectures.

7.2 Implications for Network Design and Architecture

For network architects and system designers, the findings underscore the need to embed security **by design** into ultra-dense network infrastructures. Perimeter-based security and centralised enforcement mechanisms are shown to be insufficient under high-

density conditions. Instead, distributed security controls at the edge and access layers are essential to reduce attack surfaces and enhance resilience.

The results further imply that future 5G and 6G network architectures should integrate cross-layer security orchestration as a core architectural function. Such integration enables real-time threat correlation and coordinated response, reducing the risk of cascading failures in dense deployments.

7.3 Implications for Network Operators and Service Providers

For mobile network operators, the study provides evidence that multilevel security architectures improve **operational resilience and service continuity**. Reduced detection latency and improved fault tolerance directly translate into lower downtime, fewer large-scale incidents, and improved quality of service.

Service providers deploying network slicing and edge-enabled applications can leverage the proposed framework to ensure stronger isolation between services while maintaining scalability. This is particularly relevant for critical services such as autonomous systems, industrial automation, and immersive communications.

7.4 Policy and Regulatory Implications

At the policy level, the findings support the development of **security standards and regulatory frameworks** that move beyond compliance-based checklists. Regulators and standardisation bodies can use the multilevel perspective to promote architectures that ensure end-to-end and cross-layer security rather than isolated controls.

The emphasis on decentralised trust and zero-trust principles also aligns with emerging global security regulations focused on privacy, resilience, and critical infrastructure protection. Policymakers may consider incentivising or mandating architectural security assessments for ultra-dense network deployments.

7.5 Implications for Future 6G Technologies

For 6G research and development, the study highlights that security must evolve in parallel with innovations such as terahertz communication, intelligent reflecting surfaces, and AI-native networking. The proposed framework provides a foundation for integrating security into these technologies from an early design stage, reducing the risk of systemic vulnerabilities in future networks.

8. Limitations and Future Research Scope

While this study provides a comprehensive multilevel analytical perspective on secure architectures for ultra-dense 5G and emerging 6G networks, certain limitations should be acknowledged. Recognising these limitations not only strengthens the transparency of the research but also highlights meaningful directions for future investigation.

8.1 Limitations of the Study

First, the study adopts an analytical and architecture-driven evaluation approach rather than large-scale simulation or real-world deployment. Although this approach is appropriate for early-stage 6G security research and allows for generalisable architectural insights, it does not capture all dynamic behaviours that may emerge in operational networks under highly variable traffic and mobility conditions.

Second, the analysis assumes a cooperative network environment in which network entities adhere to protocol specifications. In real deployments, misconfigurations, legacy components, and insider threats may introduce additional vulnerabilities that are not explicitly modelled in the current framework.

Third, while artificial intelligence is incorporated conceptually for threat detection and security orchestration, the study does not empirically evaluate AI model performance, training overhead, or susceptibility to adversarial manipulation. As AI-native networking becomes central to 6G, these aspects warrant deeper investigation.

Finally, economic and deployment-related factors such as implementation cost, energy consumption, and operational complexity are beyond the scope of this study. These factors may influence the feasibility and adoption of multilevel security architectures in practical network environments.

8.2 Future Research Scope

Future research can extend this work through several promising avenues. A key direction involves simulation-based and experimental validation of the proposed architecture using large-scale ultra-dense network scenarios. Such studies would provide quantitative performance metrics under diverse mobility patterns, traffic loads, and attack models.

Another important research direction is the integration of robust and explainable AI mechanisms for security orchestration. Investigating resilience against adversarial learning attacks and developing trustworthy AI models will be essential for secure 6G deployments.

Security for emerging 6G technologies such as terahertz communication, intelligent reflecting surfaces, cell-free massive MIMO, and integrated sensing and communication represents a critical future focus. Extending the multilevel framework to explicitly address these technologies will enhance its relevance for next-generation networks.

Future studies may also explore energy-efficient and sustainable security mechanisms, particularly in ultra-dense deployments where edge devices and access points operate under strict power constraints. Balancing security strength with energy efficiency will be a key challenge for green 6G networks.

Finally, cross-domain research examining the intersection of security, privacy, and regulatory compliance can further strengthen the applicability of the proposed architecture. Such work would support the development of harmonised security standards for globally interconnected 5G and 6G ecosystems.

9. Conclusion

The rapid densification of wireless infrastructures in 5G and emerging 6G networks has fundamentally transformed both network performance and the associated security landscape. Ultra-dense deployments, while enabling high capacity, low latency, and massive connectivity, simultaneously expand the attack surface and intensify cross-layer security vulnerabilities. This study addressed these challenges by presenting a multilevel analytical perspective on secure architectures for ultra-dense 5G/6G networks.

Through a comprehensive review of existing literature, the study identified critical gaps in current security approaches, particularly the limitations of perimeter-based and isolated layer-specific mechanisms in dense and highly dynamic environments. To address these gaps, a multilevel secure architectural framework was proposed, integrating security controls across physical, network, control, and application layers, supported by cross-layer security orchestration and distributed trust mechanisms.

The analytical evaluation demonstrated that the proposed architecture significantly enhances threat coverage, reduces attack surfaces, improves detection and response capabilities, and maintains stability under increasing network density. The results confirm that decentralised, adaptive, and intelligence-driven security mechanisms are essential for preventing cascading failures and ensuring resilience in ultra-dense network environments. Importantly, the findings show that security effectiveness in next-generation networks emerges from coordinated interaction across layers rather than from isolated defensive measures.

By emphasising security as an intrinsic architectural property, this study contributes to both 5G security research and early-stage 6G system design. The proposed framework offers practical guidance for network architects, operators, and policymakers seeking to build resilient, scalable, and trustworthy wireless infrastructures capable of supporting future communication services.

In conclusion, secure ultra-dense 5G and 6G networks require a fundamental shift from centralised and static security models towards multilevel, cross-layer, and intelligence-enabled architectures. As wireless networks continue to evolve towards greater autonomy and complexity, the architectural principles outlined in this study provide a robust foundation for sustaining security, reliability, and trust in next-generation communication ecosystems.

References

1. 3GPP. (2018). *Security architecture and procedures for 5G system (Release 15)* (TS 33.501). 3rd Generation Partnership Project.
2. Ahmad, I., Kumar, T., Liyanage, M., Okwuibe, J., Ylianttila, M., & Gurtov, A. (2019). Overview of 5G security challenges and solutions. *IEEE Communications Standards Magazine, 2*(1), 36–43. https://doi.org/10.1109/MCOMSTD.2018.1700063
3. Andrews, J. G., Buzzi, S., Choi, W., Hanly, S. V., Lozano, A., Soong, A. C. K., & Zhang, J. C. (2014). What will 5G be? *IEEE Journal on Selected Areas in Communications, 32*(6), 1065–1082. https://doi.org/10.1109/JSAC.2014.2328098
4. Bennis, M., Debbah, M., & Poor, H. V. (2018). Ultra-reliable and low-latency wireless communication: Tail, risk, and scale. *Proceedings of the IEEE, 106*(10), 1834–1853. https://doi.org/10.1109/JPROC.2018.2866585
5. Chen, M., Challita, U., Saad, W., Yin, C., & Debbah, M. (2020). Artificial intelligence for wireless networks: A comprehensive survey. *IEEE Journal on Selected Areas in Communications, 37*(10), 2200–2234. https://doi.org/10.1109/JSAC.2019.2923625
6. Chen, S., Sun, S., Kang, S., & Yu, Z. (2021). Vision, requirements, and technology trends of 6G networks. *China Communications, 18*(8), 1–14. https://doi.org/10.23919/JCC.2021.08.001
7. Chorti, A., Poor, H. V., & Jorswieck, E. (2019). Physical-layer security in wireless networks: A tutorial. *IEEE Communications Surveys & Tutorials, 21*(3), 2821–2849.

https://doi.org/10.1109/COMST.2019.2919496

8. Dang, S., Amin, O., Shihada, B., & Alouini, M.-S. (2020). What should 6G be? *Nature Electronics, 3*(1), 20–29. https://doi.org/10.1038/s41928-019-0355-6
9. Duan, X., Wang, J., Wang, X., & Zhang, H. (2020). Security-aware network slicing in 5G networks. *IEEE Transactions on Network and Service Management, 17*(3), 1493–1507. https://doi.org/10.1109/TNSM.2020.3001012
10. Foukas, X., Patounas, G., Elmokashfi, A., & Marina, M. K. (2017). Network slicing in 5G: Survey and challenges. *IEEE Communications Magazine, 55*(5), 94–100. https://doi.org/10.1109/MCOM.2017.1600951
11. Giordani, M., Polese, M., Mezzavilla, M., Rangan, S., & Zorzi, M. (2020). Toward 6G networks: Use cases and technologies. *IEEE Communications Magazine, 58*(3), 55–61. https://doi.org/10.1109/MCOM.001.1900411
12. Liyanage, M., Ylianttila, M., Gurtov, A., & Ding, A. Y. (2018). A comprehensive guide to 5G security. *IEEE Communications Surveys & Tutorials, 20*(3), 2582–2610. https://doi.org/10.1109/COMST.2018.2822121
13. Liu, Y., Chen, H., Li, Y., & Poor, H. V. (2020). Secrecy performance analysis of ultra-dense networks. *IEEE Transactions on Wireless Communications, 19*(1), 408–422. https://doi.org/10.1109/TWC.2019.2942334
14. Naik, N., Jenkins, P., Savage, N., & Behl, A. (2022). Zero-trust architecture for 5G and beyond networks. *IEEE Network, 36*(2), 78–85. https://doi.org/10.1109/MNET.011.2100372
15. Nguyen, D. C., Ding, M., Pathirana, P. N., & Seneviratne, A. (2020). Blockchain for secure 5G and beyond networks: A state-of-the-art survey. *Journal of Network and Computer Applications, 166*, 102693. https://doi.org/10.1016/j.jnca.2020.102693
16. Nguyen, T. T., Reddi, V. J., Kumar, S., Quek, T. Q. S., & Shafi, M. (2021). Machine learning for 5G and beyond: A survey. *IEEE Communications Surveys & Tutorials, 23*(4), 1978–2018. https://doi.org/10.1109/COMST.2021.3090703
17. Park, J., Bennis, M., & Kim, D. (2021). URLLC-eMBB slicing for beyond 5G networks. *IEEE Communications Letters, 25*(5), 1627–1631. https://doi.org/10.1109/LCOMM.2021.3051507
18. Restuccia, F., D'Oro, S., & Melodia, T. (2020). Securing the Internet of Things in the age of machine learning and software-defined networking. *IEEE Internet of Things Journal, 7*(6), 4640–4655. https://doi.org/10.1109/JIOT.2020.2970957
19. Saad, W., Bennis, M., & Chen, M. (2020). A vision of 6G wireless systems: Applications, trends, technologies, and open research problems. *IEEE Network, 34*(3), 134–142. https://doi.org/10.1109/MNET.001.1900287
20. Shafi, M., Molisch, A. F., Smith, P. J., Haustein, T., Zhu, P., Silva, P. D., Tufvesson, F., Benjebbour, A., & Wunder, G. (2017). 5G: A tutorial overview of standards, trials, challenges, deployment, and practice. *IEEE Journal on Selected Areas in Communications, 35*(6), 1201–1221. https://doi.org/10.1109/JSAC.2017.2692307
21. Sun, Y., Liu, J., Wang, Y., & Liu, H. (2020). Adversarial attacks and defenses in deep learning for network security. *IEEE Network, 34*(3), 36–43. https://doi.org/10.1109/MNET.001.1900123
22. Wang, C.-X., Huang, J., Wang, H., Gao, X., You, X., & Hao, Y. (2021). 6G wireless channel measurements and models. *IEEE Vehicular Technology Magazine, 16*(2), 99–107. https://doi.org/10.1109/MVT.2021.3057798
23. Xiao, L., Wan, X., Lu, X., Zhang, Y., & Wu, D. (2018). IoT security techniques based on machine learning: How do IoT devices use AI to enhance security? *IEEE Signal Processing Magazine, 35*(5), 41–49. https://doi.org/10.1109/MSP.2018.2825478
24. Ylianttila, M., Kantola, R., Gurtov, A., & Mucchi, L. (2021). *6G white paper: Research challenges for trust, security and privacy*. 6G Flagship, University of Oulu.
25. Zhang, J., Chen, X., & Letaief, K. B. (2018). Physical-layer security in ultra-dense networks. *IEEE Wireless Communications, 25*(5), 120–126. https://doi.org/10.1109/MWC.2018.1700427

26. Zhang, Q., Gui, L., Hou, F., & Sun, J. (2021). Edge intelligence for 6G networks: Vision, enabling technologies, and applications. *IEEE Internet of Things Journal, 8*(22), 16380–16394. https://doi.org/10.1109/JIOT.2021.3070906