



NETWORK SECURITY VULNERABILITIES IN 5G COMMUNICATION SYSTEMS AND THEIR MITIGATION TECHNIQUES

Idris, Saheed Asimiu¹; **Ibrahim**, Hussain²; **Koleosho**, Saheed Adedimeji³, **Amoo**, Mutiu Adewale⁴ and **Egbonwonu**, Patricia Nkiru⁵

^{1,2}Department of Computer Science, Federal Polytechnic Ohodo, Enugu State

³Owu College of Education, Wasimi, Ogun State, Nigeria

⁴Federal College of Forestry, Jericho, Ibadan

⁵Department of Computer Engineering, Federal Polytechnic Ohodo, Enugu State

saheed.idris@fedpod.edu.ng

ABSTRACT

Fifth Generation (5G) communication systems have enabled wireless communication to achieve ultra-high data rates, low latency, connectivity of a massive number of devices, and improved reliability. Rapid growth and acceptance of modern innovations such as the Internet of Things (IoT), Cloud Computing, Artificial intelligence, Autonomous Vehicles, Smart Health-care and Industrial Automation. However, the added advantages of 5G comes with its own set of complexities, which exposes new cyber-risk that are arising from SDN, NFV, network slicing edge computing and massive device connectivities. These advanced threats cannot be addressed with traditional network security mechanisms. In this article, principal security threats in 5G communication networks and review state-of-the-art mitigation methods to enhance the enterprise and telecommunications security. The paper conducts systematic literature review and analyses the common risks such as Distributed Denial-of-Service (DDoS) attacks, signalling attack, spoofing, malware/network slice/programming assault, virtualisation vulnerabilities and insider threats/privacy breaches. This suggest a theoretical framework security framework based on Zero Trust architecture, AI-based threat detection, encryption, and authentication intrusion detection systems (IDS) continuously monitoring security events. According to the review, incorporating AI Powered Security Analytics, Zero Trust Architecture, network segmentation and blockchain along with Automated Threat Response could substantially strengthen the posture of 5G infrastructures. Still, implementation challenges persist including computational overhead, interoperability and privacy concerns as well as new attack strategies. This study advises multi-layered security architectures, AI-enabled threat intelligence and continuous risk assessment in a bid to establish robust protection mechanisms for future 5G networks as well as having standardized policies set into action.

Keywords: 5G Security, Network security, Cybersecurity, Network Slicing, Artificial Intelligence. Internet of Things

INTRODUCTION

5G mobile communication technology is the next major step in wireless networking, with blazing-fast data transmission speeds, low latency, high bandwidth and ability to connect billions of devices. 5G is not just another generation of mobile communication, rather it offers intelligent connectivity for new-age applications including Internet of Things (IoT), autonomous transportation, smart healthcare, industrial

automation, cloud computing, augmented reality and smart cities. And now, these capabilities expedited haste digital transformation across national governments, corporate enterprises & academic institutions over the globe. The way of discussion is different according to the architecture of 5g networks which is not same as earlier generation mobile communication systems. It leverages technologies like SDN, NFV, edge computing, cloud-native infrastructure and network slicing to increase scalability, flexibility and service delivery. Despite improving the efficiency of the networks, these technologies also grow the attack surface available to cybercriminals. As a result, the security of 5G communication systems has emerged as one of the most pressing challenges for network administrators and cybersecurity practitioners.

The virtualisation, cloud integration, network slicing and large scale IoT connectivity in 5G communication systems poses unique security challenges arising from the rapid deployment of these system components. Traditional perimeter-based security methods are not sufficient to secure these highly decentralized environments against advanced cyber threats like DDoS, signaling attacks, virtualization exploits, insider threat and identity-based attacks. As a result, there is a compelling requirement for smart and dynamic security architectures that can defend next-generation 5G networks without compromising service availability, confidentiality, integrity, and privacy. This study focuses on 5G communication systems to research the network security vulnerabilities and assess state-of-the-art approaches to mitigate them for enhancing the communication security. The specific objectives are to:

1. Examine the architecture and security features of 5G communication systems;
2. Identify major network security vulnerabilities affecting 5G infrastructures;
3. Evaluate existing mitigation techniques for protecting 5G networks;
4. Propose a conceptual security framework for enhancing 5G communication security; and
5. Identify emerging research challenges and future directions in 5G cybersecurity.

This study provides a short review of the vulnerabilities and countermeasures in the cybersecurity of 5G networks, and is a preliminary step to deepening this work. It will be useful to researchers, students, cybersecurity experts in various fields of telecommunications and engineers at organizations implementing 5G technologies, not to mention policy makers. The proposed conceptual framework serves as a practical reference for the security improvement of next generation communication systems.

Literature Review

5G Communication Systems: An Overview

Fifth Generation (5G) wireless communication technology is an advanced wireless network with high mobile broadband (eMBB), ultra-reliable low-latency communication (URLLC), and massive machine-type communications (mMTC). These features enable applications, including autonomous vehicles, smart

health care services, industrial automation and connection of devices and things (IoT or Internet of Things) in the Cloud Computing domain. It was a credible application node with noticeable benefits — higher bandwidth, lower latency initially true with up to/more connected nodes energy efficiency; 4G improved cellular generations outperformed all four fronts significantly.

5G Network Architecture

There are three main domains of 5G architecture such as UE (User Equipment) which include Mobile phones, IoT devices, sensors, autonomous systems or any other connected endpoint. It also include Radio Access Network (RAN). This is the portion of a telecommunication system which connects user devices to the core network via 5G base stations. 5G Core Network (5GC) provides authentication, mobility management, routing, policy enforcement and service orchestration in virtualized network functions. The integration of SDN and NFV enables dynamic resource allocation and simplified network management. However, virtualization also creates additional attack vectors that require advanced security controls.

Security Vulnerabilities in 5G Networks

The complexity of 5G introduces vulnerabilities that are less prevalent in earlier communication systems such as Software-Defined Networking (SDN) Vulnerabilities which involves the Use of SDN, which improves the flexibility of the network by separating the control plane from the data plane. Nevertheless, a localized SDN controller is still vulnerable — the centralized controller may be compromised, resulting in disruption of existing operations, modification of routing policies and unauthorized access to network resources. There are Network Function Virtualization (NFV) Risks. NFV (network function virtualization)- is used to eliminate specialized hardware appliances and Uses Virtual network Function instead. Virtualization platforms, or socialized hypervisors can also be exploited to maintain multiple network services simultaneously. Network Slicing Attacks also exist. Network slicing allows a number of logical networks to run over common physical infrastructure. Lack of proper isolation control between slices could lead to unauthorized access, information leakage or service disruption. There are Edge Computing Vulnerabilities. Multi-access Edge Computing (MEC) allows for the processing of data closer to end users, which helps with reducing latency. Edge nodes are also more susceptible to physical attack, malware infection and access by unauthorized users due to their geographical distribution. Internet of Things (IoT) Threats is also prevalent. The number of IoT devices using the 5G makes the attack surface much larger. IoT devices have turned out to be the ideal pray for botnets, malware and Distributed Denial-of-Service (DDoS) attacks, consideration exists in part because of their frail means of verification, secure firmware and update components.

There are Common Cyber Threats in 5G. Several cyber threats continue to challenge 5G security. These include Distributed Denial-of-Service (DDoS) Attacks. Thousands of infected devices are making traffic to

saturate the network resources and reduce service availability, distorting critical infrastructure. Signalling Attacks is another threat. Attackers abuse signalling protocols through these points in order to overwhelm both processes-control and data-plane elements of a signalling network, causing congestion as well as reducing its serving functions, e.g. service reservation or even denial or disruption of any signaling services. There is Spoofing and Identity Attacks. Cybercriminals impersonate actual users, devices or network elements to gain access to the communication. Man-in-the-Middle (MitM) Attacks represent another type of threat. Eavesdropping on or modification and replay of communication between two legitimate parties also breach data confidentiality and integrity. There is also the Malware and Ransomware. By virtualising network functions, malware can propagate from edge servers to connected devices to disable services as well as from access-controlled channels to extract data. And lastly, there is Insider Threats. It is recorded that the Authorized users can misuse privileges either intentionally or unintentionally leading to Data Leakage / illegitimate amendments of the corporate resource.

Contemporary Mitigation Techniques

Protecting 5G infrastructures requires multiple complementary security mechanisms. Among the techniques is Zero Trust Architecture (ZTA). Zero Trust lives by the principle that trust cannot be assumed — users, devices and applications must authenticate in accordance with policy to gain access. This risk of undetected intrusion can be minimized with authentication, least-privilege access and continuous monitoring. Artificial Intelligence and Machine Learning is another tool that supports mitigation. When we speak of cybersecurity and the way machine learning and AI are improving its stature, it is in rapid-looking at all network traffic for any unusual behaviour. Signature-based solutions might struggle to combat zero-day attacks, AI-powered Intrusion Detection Systems (IDS) help in this regard. Encryption and Secure Authentication which involves integrated mutual authentication and Multi-Factor Authentication (MFA) will safeguard user identities, protecting them while also hardening communications against interception risk and credential theft. Another advanced technology for threat mitigation is the Blockchain Technology. It provides the building blocks for decentralized identity management to be generated wherever needed and transactions that are recorded in an immutable way, increased trust between disparate parts of a distributed network, while reducing single points of failure.

Network Segmentation and Slice Isolation is an ideal technique. Good segmentation makes it so that once an attacker gains access to a specific slice they cannot move around whilst taking advantage of the compromise; but proper isolation means even if success is achieved, service by service attack success becomes infeasible. There is also the Continuous Monitoring technique. SIEM, SOAR and XDR Solutions

allow automated threat detection systems with rapid incident response mechanism to perform 24/7 monitoring.

Empirical Review

Recent studies identify the necessity of enhancing the security in 5G communication systems.

Sicari et al. (2018), the heterogeneous devices and high end-to-end contact resource requirements for security solutions, IoT safety continues to be one of the last incredible challenges for next-generation conversation networks. Ahmad et al. (2022) show that Artificial Intelligence integration into intrusion detection enhances the accuracy and expedites response time. Khan et al. (2021) found that, although SDN and NFV provide protection flexibility in the network level, they increase vulnerability and need more protection against virtualization attacks.

Hussain et al. (2023) demonstrated that Zero Trust Principles for Access Control and Mitigating Insider Threats under 5G Environments. Research into how blockchain-based authentication not only assists identity management, but also provides a higher level of trust between the connected components in a distributed network configuration is also recent.

Despite important advances in securing emerging 5G communication systems, some challenges are still open. Most existing papers deal with AI or a blockchain, SDN security technology and divided part of protection. There has been little attention too, to practical implementation challenges in developing countries ranging from infrastructure constraints, lack of skilled personnel and regulatory bottlenecks. Additionally, it is very little to date evaluating integrated security frameworks on real-world 5G deployments. Keywords - Zero Trust Architecture, AI-enabled threat detection, secure network slicing, blockchain-based identity.

Methodology

This study utilized both systematic literature review (SLR) and conceptual framework approaches to explore potential threats in Fifth Generation (5G) communication systems and current countermeasures against these vulnerabilities. This systematic review synthesised evidence from peer-reviewed journal articles, conference proceedings, international standards, books and technical reports published on the topic of 5G security. A conceptual framework was then derived from the literature review to represent how multiple security technologies can be combined towards efficiently improving the confidentiality, integrity availability and resilience of 5G communication networks. The study was conducted using only secondary data sourced from both academic and professional literature such as Peer-reviewed journal articles, International conference proceedings, Books on network security and wireless communications, 3rd Generation Partnership Project (3GPP) security specifications, National Institute of Standards and

Technology (NIST) publications, European Telecommunications Standards Institute (ETSI) reports, International Telecommunication Union (ITU) recommendations, Reports from cybersecurity organizations and telecommunications vendors, This research prioritized on more recent publication works related to 5G architecture and those specifically oriented towards Software-Defined Networking (SDN), Network Function Virtualization (NFV), Artificial Intelligence (AI) based, Zero Trust Architecture (ZTA), blockchain, and Internet of Things (IoT) security aspects. A multi-layered conceptual security framework is proposed to enhance the protection of 5G communication systems based on the information gathered from the performed literature review. The framework spans across several layers in the same network and has preventive, detective and responsive security controls. This framework consists of more components such as User and Device Authentication, Identity and Access Management (IAM), Zero Trust Access Control, Secure Network Slicing, AI-Based Intrusion Detection System (IDS), Encryption and Secure Communication, Continuous Security Monitoring and Automated Incident Response. This reduces the attack surface and allows cyber threats to be identified/remediated more quickly.

Conceptual 5G Security Architecture

5G Users / IoT Devices



Identity Verification & MFA



Identity and Access Management



Zero Trust Policy Engine



Secure Network Slicing

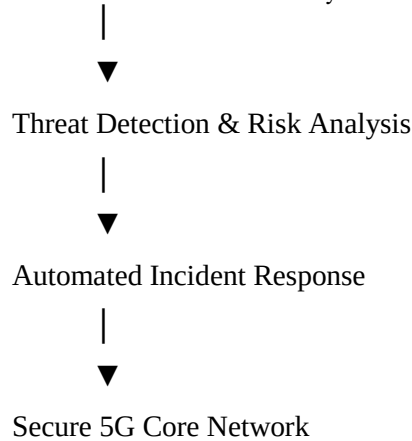


AI-Based Intrusion Detection System



Continuous Security Monitoring

(SIEM / SOAR / XDR)



This architecture focuses on ongoing authentication, smart traffic review, network segmentation and automatic reaction to help lessen the repercussions of cyberattacks.

Security Implementation Process

The framework can be implemented through the series of sequential phases. The initial step involves recognizing vital assets and services in the 5G communication domain. Classifying users, devices and network functions based on risk; Implement a strong identity and multi-factor authentication (MFA); Enforce Zero Trust Access Policies on the Network; Logical isolation: Secure network slices; Employ AI based Intrusion Detection and Prevention Systems (IDS/IPS); Encrypt communication channels and sensitive data and Use SIEM & Behavioural analytics and Active Network monitoring. SOAR (Security Orchestration, Automation and Response) — automates the threat response to incidents. This phased rollout of organizations provides security with reduced disruption to ongoing services.

Evaluation Criteria

The effectiveness of the proposed framework may be assessed using the following performance indicators:

Performance Metric	Purpose
Threat Detection Rate	Measures ability to identify cyberattacks
False Positive Rate	Evaluates detection accuracy
Mean Time to Detect (MTTD)	Measures speed of attack detection
Mean Time to Respond (MTTR)	Measures effectiveness of incident response
Service Availability	Assesses network resilience during attacks
Authentication Success Rate	Evaluates identity verification effectiveness
Data Confidentiality	Measures protection of sensitive information
Network Slice Isolation Efficiency	Evaluates separation between virtual networks

These metrics provide a balanced assessment of both security effectiveness and operational performance.

All methods were based on publicly available scientific publications, international standards and technical reports. The study did not involve human participants, confidential telecommunications data, or proprietary organizational information. Because you can only avoid plagiarism by crediting your information sources, this source must also be referenced according to APA 7th edition. In summary, the methodology combines systematic review with a conceptual multi-layered security framework to explore vulnerabilities and mitigation strategies of 5G communication system. The proposed framework serves as a concrete pathway towards strengthening the security and resilience of next generation communication networks, by synergising Zero Trust Architecture with Artificial Intelligence, along with secure network slicing, encryption, Identity and Access Management (IAM), and continuous monitoring.

Results and Discussion

Results

The reviewed literature suggests that 5G communication systems offer significant enhancements in network performance yet at the same time expose a more extensive and complex range of cybersecurity threats than earlier generations of mobile networks. As SDN, NFV, MEC and cloud-native services evolve alongside the expansion of threat vectors from network slicing.

The findings show that the most common security vulnerabilities in 5G communication systems include Distributed Denial-of-Service (DDoS) attacks; Network slice attacks; SDN controller compromise; NFV hypervisor vulnerabilities; Edge computing attacks; IoT device compromise; Identity spoofing; Signalling attacks; Malware and ransomware; Insider threats; The studies reviewed unanimously show that 5G environments are highly distributed, and perimeter-based security mechanisms alone cannot protect them for highly distributed 5G environments. A multi-layered security architecture based on Artificial Intelligence (AI), Zero Trust Architecture (ZTA), encryption, IAM, blockchain and continuous monitoring can provide a better protection instead.

Table 1 Major 5G Vulnerabilities and Mitigation Techniques

Vulnerability	Potential Impact	Recommended Mitigation
DDoS Attack	Service disruption	AI-based traffic analysis, rate limiting
SDN Controller Attack	Network takeover	Controller redundancy, secure APIs
NFV Exploits	Virtual infrastructure compromise	Hypervisor hardening, VM isolation
Network Slice Attack	Cross-slice compromise	Strong slice isolation, access control
Edge Computing Attack	Data manipulation	Secure edge authentication, encryption
IoT Device Attack	Botnets, malware	Device authentication, firmware updates
Spoofing Attack	Unauthorized access	Multi-Factor Authentication (MFA)

Vulnerability	Potential Impact	Recommended Mitigation
Insider Threat	Data leakage	Least-privilege access, behavioural monitoring

Discussion

The results indeed proves that the security issues of 5G are not only an enhancer of what other wireless communication technologies were dealing with. It means that SDN, NFV, edge computing & network slicing has moved network architecture from hardware fixtures to software created environments. While this increases flexibility, it exposes a larger attack surface. One of the main discoveries is that network slicing has become a factor in providing custom services for different applications, and that each slice needs to be logically isolated from one another through strict enforcement, so as not to allow an attack on one slice impacting adjacent slices. Likewise, virtualization technology improves the security of hypervisors and virtual machines to avoid compromising multiple network functions. AI is one of the most prospective technologies for securing 5G networks. With the help of AI, Intrusion Detection Systems (IDS) and behavioural analytics can now be used to detect anomalies like abnormal traffic, zero-day attacks, and advanced malware within seconds. The response time and false-positive rate improves here too as machine learning algorithms are based on the constant metadata from network behaviour learned.

4.3 Recommendations

Based on the finding of this particular study, the study recommends the multi-layered security architectures element indicates that telecommunications operators operate more mitigations within the layers of the network, rather than rely only on perimeter defense; Merge Artificial Intelligence and Machine Learning with Intrusion Detection and Prevention Systems for real-time threat identification; Zero trust architecture (ZTA) — Continuous run redundancy, if possible, and secure APIs and continuous vulnerability assessments in Software-Defined Networking controllers, Network Function Virtualization platforms. It was also recommended to deploy Security Information and Event Management (SIEM) and Security Orchestration, Automation and Response (SOAR) platforms that provide automated monitoring and incident response capabilities for telecommunications providers.

References

- Ahmad, Z., Shahid Khan, A., Wai Shiang, C., Abdullah, J., & Ahmad, F. (2022). Network intrusion detection system: A systematic study of machine learning and deep learning approaches. *Transactions on Emerging Telecommunications Technologies*, 33(1), e4150.
- 3rd Generation Partnership Project. (2023). *3GPP security architecture for 5G systems (TS 33.501)*. <https://www.3gpp.org>

- Ferrag, M. A., Maglaras, L., Argyriou, A., Kosmanos, D., & Janicke, H. (2020). Security for 4G and 5G cellular networks: A survey of existing authentication and privacy-preserving schemes. *Journal of Network and Computer Applications*, 101, 55–82.
- Humayed, A., Lin, J., Li, F., & Luo, B. (2017). Cyber-physical systems security: A survey. *IEEE Internet of Things Journal*, 4(6), 1802–1831.
- International Telecommunication Union. (2022). *IMT-2020 (5G) network security recommendations*. ITU.
- Khan, L. U., Yaqoob, I., Imran, M., Han, Z., & Hong, C. S. (2021). 6G wireless systems: A vision, architectural elements, and future directions. *IEEE Access*, 8, 147029–147044.
- Li, X., Xu, H., Wang, X., & Zhang, Y. (2021). Security challenges and solutions in Software-Defined Networking: A review. *IEEE Access*, 9, 125027–125049.
- National Institute of Standards and Technology. (2020). *Security and privacy controls for information systems and organizations (SP 800-53 Rev. 5)*. U.S. Department of Commerce.
- Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2018). Security, privacy, and trust in Internet of Things: A survey. *Computer Networks*, 76, 146–164.
- Sun, Y., Peng, M., Zhou, Y., Huang, Y., & Mao, S. (2020). Application of machine learning in wireless networks: Key techniques and open issues. *IEEE Communications Surveys & Tutorials*, 21(4), 3072–3108.
- Roman, R., Lopez, J., & Mambo, M. (2018). Mobile edge computing, fog computing, and security: A survey. *Future Generation Computer Systems*, 78, 680–698.