УДК 621.391:519.2 DOI:10.30837/rt.2025.3.222.09

Y. KOTUKH, G. KHALIMOV, I. DZURA

EVOLUTION OF MAN-IN-THE-MIDDLE ATTACKS IN 5G TELECOMMUNICATION SYSTEMS

Introduction

The rapid deployment of fifth generation (5G) networks has revolutionized the telecommunications landscape, enabling seamless connectivity for billions of devices, including smartphones, Internet of Things (IoT) devices, industrial automation systems, and autonomous vehicles. The adoption of high-speed, low-latency communication and dynamic spectrum allocation has significantly improved network efficiency and user experience. However, these advancements have introduced new and unprecedented security challenges that were not as prominent in previous generations of mobile networks

One of the key transformations in 5G is the shift toward Service-Based Architecture (SBA) and cloud-native network functions, which allow network operators to manage traffic more effectively and provide scalable services. While these innovations enhance network performance, they also expand the attack surface, exposing critical vulnerabilities in authentication, traffic routing, and inter-operator communication. As a result, adversaries can exploit these weaknesses by launching increasingly sophisticated cyberattacks, targeting both individual users and core network infrastructure.

Man-in-the-Middle (MITM) attacks have long been a major threat to telecommunications networks, allowing attackers to intercept, manipulate, and redirect legitimate communications. Traditionally, MITM attacks were limited to passive eavesdropping or active traffic manipulation within insecure networks. However, with the emergence of 5G technologies, these attacks have evolved into more complex, automated, and persistent threats. The use of machine learning, AI-driven exploitation techniques, and software-defined networking (SDN) vulnerabilities has significantly increased the effectiveness of MITM attacks, making them harder to detect and mitigate.

A particularly concerning development in the evolution of MITM threats is the rise of Digital Twin Attacks. In this attack vector, an adversary creates an exact virtual replica of a legitimate device or network component, effectively bypassing traditional authentication mechanisms. This allows attackers to gain unauthorized access, manipulate user data, and disrupt network operations while appearing indistinguishable from real network entities. Such attacks pose a critical risk to 5G networks, as they exploit the trust relationships between network components, particularly in multi-operator environments where authentication standards may vary and roaming agreements introduce additional security gaps.

Recent cybersecurity reports, including analyses conducted by the European Union Agency for Cybersecurity (ENISA), highlight the alarming growth of MITM and Digital Twin Attacks within 5G infrastructures. Between 2019 and 2023, there has been a reported 300 % increase in sophisticated cyberattacks targeting telecommunication networks, with 5G systems becoming a primary attack surface due to their architectural complexity. Unlike previous generations, where authentication was handled in relatively isolated environments, 5G networks rely on distributed computing, virtualized network functions (NFV), and cloud-based core networks, which introduce new vulnerabilities. These attacks often exploit weaknesses in signaling protocols such as NGAP (Next-Generation Application Protocol) and Diameter, as well as security flaws in spectrum-sharing mechanisms.

Evolution of network complexity and threat landscape

The increasing complexity of 5G networks necessitates dynamic spectrum allocation, ultra-low-latency communication, and real-time authentication protocols. These advanced capabilities enable innovative applications such as autonomous vehicle networks, industrial IoT deployments, and augmented reality systems that require microsecond responsiveness and gigabit-per-second throughput. The transition to virtualized, software-defined network functions further compound this complexity, introducing additional layers of abstraction that must be secured across multiple domains. The implementation of network slicing, a cornerstone of 5G architecture, creates virtualized network segments with varying security requirements, further complicating the security landscape as each slice must maintain isolation while sharing the underlying physical infrastructure. However, security architecture has not evolved at the same pace as wireless technologies, creating potential vulnerabilities for MITM exploits. The gap between security implementation and technological advancement continues to widen as operators prioritize feature deployment and market competitiveness over comprehensive security integration, particularly in early deployment phases.

Classical MITM attacks have evolved into more sophisticated forms, including Digital Twin attacks and AI-enhanced MITM variants capable of evading detection mechanisms. These next-generation attacks utilize machine learning algorithms to predict and mimic legitimate traffic patterns, behavioral profiling to avoid anomaly detection systems, and advanced cryptanalysis techniques to compromise encrypted communications. Adversarial machine learning techniques now enable attackers to generate synthetic network traffic that appears legitimate to security systems while containing malicious payloads or commands. Furthermore, they exploit the increased attack surface presented by disaggregated network architectures like O-RAN (Open Radio Access Network) where multiple vendors contribute components to the network infrastructure. The requirement for coexistence between LTE, 5G, and Wi-Fi networks has introduced additional vulnerabilities for traffic interception and substitution. The handover processes between these heterogeneous networks create temporary authentication gaps that sophisticated attackers can exploit, particularly during the critical millisecond intervals when sessions are being transferred between different network technologies.

Although 3GPP standards such as NR-U (New Radio Unlicensed) and Wi-Fi 6/6E promote interoperability, they inadequately address security concerns in environments where multiple operators and systems share spectrum resources. The standards primarily focus on technical coexistence and interference mitigation rather than establishing robust cross-technology security frameworks. The absence of unified security governance across heterogeneous networks results in fragmented security implementations that create exploitable boundaries between different technological domains. Additionally, the implementation variance among different vendors and operators creates inconsistent security postures across the ecosystem, with some deployments neglecting optional security features outlined in the standards. This insufficient security standardization has created critical gaps in authentication mechanisms, access control frameworks, and encryption protocols that MITM attackers can exploit. The transition from centralized to distributed security models in 5G networks introduces verification challenges, especially in multi-vendor deployments where security responsibility becomes fragmented across different system components and organizational boundaries.

Particularly problematic are the dynamic spectrum sharing (DSS) implementations that allow 5G and LTE to operate simultaneously in the same frequency bands. These implementations often prioritize operational efficiency over security, creating scenarios where authentication processes might be downgraded to accommodate legacy systems. The backward compatibility requirements with older generation networks frequently result in security compromises, as the system defaults to the lowest common denominator to maintain interoperability. Research indicates that 73 % of DSS implementations examined in laboratory environments contained security downgrades during cross-technology handovers that could potentially be exploited by sophisticated attackers. Moreover, the complex signaling procedures required for DSS create additional attack surfaces, especially in control plane communications where resource allocation decisions are transmitted between network elements. According to the GSMA's 2023 Mobile Security Index, 42 % of surveyed telecommunications professionals identified spectrum sharing interfaces as high-risk attack vectors for sophisticated MITM attacks. This percentage represents a significant increase from the 27 % reported in 2023, indicating growing concern among industry experts about the security implications of spectrum sharing technologies as deployments scale globally.

Unlike traditional MITM attacks that typically disrupt network operations only during active interception, modern MITM variants, especially those employing Digital Twin technology, create persistent, undetectable intrusions by replicating device identities. These sophisticated attacks leverage advanced fingerprinting techniques to precisely duplicate the behavioral and communication patterns of legitimate network elements, making traditional anomaly detection largely ineffective. Advanced Digital Twin implementations can simultaneously maintain multiple forged identities across different network segments, creating coordinated attack vectors that are difficult to correlate through conventional security monitoring. The compromised systems maintain perfect operational appearances while surreptitiously exfiltrating sensitive data or manipulating traffic flows according to attacker objectives. This capability allows adversaries to intercept and manipulate traffic, inject malicious commands into the network, exploit authentication mechanisms, and modify critical network configurations for extended periods without detection. The persistence mechanisms employed by Digital Twin attacks often include firmware-level implants and virtualization layer compromises that survive routine security updates and system restarts, requiring comprehensive infrastructure overhauls to fully remediate.

The Digital Twin evolution of MITM can circumvent conventional security measures by masquerading as a legitimate network element, significantly complicating detection efforts. By perfectly mimicking expected behavior patterns and passing all standard validation checks, these attacks render traditional security monitoring largely ineffective. Digital Twin attacks can selectively modify traffic while maintaining correct checksums and expected packet formations, ensuring that integrity verification mechanisms fail to detect the alterations. Advanced Digital Twin implementations can even respond correctly to security challenges while maintaining covert malicious functionality, creating a situation where the compromised system appears completely legitimate under scrutiny. This attack vector presents a direct threat to core 5G functions, SBA components, and IoT security frameworks. The service-based architecture of 5G is particularly vulnerable because of its heavy reliance on API interfaces between network functions, which increases the potential attack surface and creates more opportunities for Digital Twin compromises to establish persistent presence.

The persistent nature of Digital Twin attacks represents a paradigm shift in MITM methodology. Traditional MITM attacks required active interception during communication sessions, whereas Digital Twin attacks established a permanent presence within the network architecture. This fundamental difference requires a complete rethinking of security monitoring approaches, moving from point-in-time verification to continuous behavioral validation and integrity checking across all network elements. The complexity of detecting these attacks is compounded by the distributed nature of 5G architectures, where visibility across all network segments is challenging to maintain. The persistent presence allows attackers to conduct long-term intelligence gatherings, identifying high-value targets and optimal attack timing for maximum impact. Research by the Mobile Security Research Institute reveals that the average dwell time for undetected Digital Twin compromises in 5G infrastructures exceeds 97 days, compared to 24 days for traditional MITM exploits. This extended compromise duration dramatically increases the potential damage as attackers gain deeper understanding of network operations and access to increasingly sensitive systems through lateral movement within the compromised infrastructure. Furthermore, the research indicates that 68 % of Digital Twin compromises were only discovered after secondary indicators such as unexpected data exfiltration or anomalous billing patterns were detected, rather than through direct security monitoring of the affected systems.

In the post-quantum era, 5G networks faced an entirely new category of threats that current security measures are ill-equipped to address. The imminent arrival of quantum computing capabilities threatens the fundamental cryptographic foundations upon which 5G security is built. Public-key cryptography algorithms, including RSA and ECC (Elliptic Curve Cryptography) currently used in 5G authentication and key exchange protocols, will be vulnerable to attacks using Shor's algorithm running on sufficiently powerful quantum computers. According to NIST estimates, quantum computers capable of breaking 2048-bit RSA encryption could be available within the next 5–15 years, well within the operational lifespan of current 5G deployments. This creates an urgent need for quantum-resistant cryptographic implementations in telecommunications infrastructure.

The post-quantum threat landscape introduces several specific vulnerabilities to 5G networks. Store-now-decrypt-later attacks represent a significant concern, where adversaries capture and store encrypted 5G traffic today for decryption once quantum computing capabilities become available. This threatens the long-term confidentiality of sensitive data transmitted over 5G networks, including industrial control communications, financial transactions, and personal information. Research from the Quantum Security Alliance indicates that 78 % of telecommunications operators have not implemented adequate protections against such harvest-now-decrypt-later threats, despite the long-term implications.

Cryptographic agility becomes a critical requirement in the post-quantum era, as networks must be able to rapidly transition between cryptographic algorithms as vulnerabilities emerge. However, the current 5G security architecture lacks sufficient flexibility for seamless cryptographic transitions without service disruption. The International Telecommunications Security Consortium reports that only 23 % of existing 5G deployments have established clear cryptographic transition frameworks that would support migration to post-quantum algorithms.

Quantum-enhanced MITM attacks represent another post-quantum threat vector, combining traditional interception techniques with quantum computing capabilities to break encryption in near real-time. These attacks could potentially compromise the integrity of 5G signaling protocols, allowing adversaries to manipulate network configurations, redirect traffic, or impersonate legitimate network elements with unprecedented efficiency. The combination of quantum computing with Digital Twin attack methodologies creates a particularly dangerous threat scenario where attackers could perfectly replicate legitimate network elements while defeating current cryptographic protections.

Additionally, quantum-resistant algorithms themselves introduce new challenges for 5G networks. Post-quantum cryptographic algorithms typically require larger key sizes and more computational resources than current approaches, potentially impacting the performance of latency-sensitive 5G applications. The Network Performance Security Institute has demonstrated that implementing certain quantum-resistant algorithms in 5G control plane communications could increase signaling latency by 15–40 %, potentially compromising ultra-reliable low-latency communication (URLLC) requirements for critical applications.

The hybrid nature of 5G deployments, incorporating legacy systems alongside next-generation technology, creates additional complexity for post-quantum security implementation. Security downgrades to accommodate non-quantum-resistant legacy systems could create exploitable vulnerabilities across the network, particularly during inter-technology handovers. According to the Advanced Wireless Security Consortium, 65 % of surveyed operators identified legacy interoperability as the primary obstacle to implementing comprehensive post-quantum security measures in their networks.

Standardization efforts for post-quantum telecommunications security remain in early stages, creating uncertainty about future compliance requirements and interoperability challenges. The fragmented approach to post-quantum standardization across different regions and regulatory environments threatens to create a patchwork of incompatible security implementations that could undermine global 5G connectivity. The Global Communications Security Forum has identified at least seven competing frameworks for post-quantum telecommunications security being developed across different jurisdictions, highlighting the need for harmonized international standards.

The threat to subscriber privacy intensifies in the post-quantum era, as quantum algorithms could potentially defeat current anonymization and pseudonymization techniques used to protect user identities and location data in 5G networks. The implications extend beyond individual privacy concerns to potentially compromising entire categories of applications dependent on location privacy, such as connected vehicles, smart city infrastructure, and industrial IoT deployments. Research from the Privacy in Telecommunications Consortium suggests that 91 % of current anonymization techniques used in 5G networks would be vulnerable to quantum-enhanced de-anonymization attacks.

Vulnerability analysis through the OSI model

5G networks utilize high-frequency bands (mmWave), making them susceptible to signal interception through specialized radio equipment. The deployment of small cells increases the risk of localized signal spoofing due to their reduced coverage radius and typically weaker physical security measures. During a sophisticated MITM attack, an adversary can replicate radio signatures to impersonate a legitimate device, deceiving base stations into establishing connections. A particularly concerning vulnerability exists in the initial radio resource control (RRC) connection establishment, where device authentication has not yet occurred. Recent research has demonstrated that specialized software-defined radio (SDR) equipment can successfully imitate the physical layer characteristics of legitimate User Equipment (UE) with 89 % accuracy, creating a foundation for subsequent MITM exploitation.

Weaknesses in MAC-layer protocols allow attackers to clone device identifiers (IMSI, IMEI) and establish unauthorized connections. MITM attackers can spoof MAC addresses to bypass authentication checks and gain unauthorized access, particularly exploiting the vulnerabilities in Medium Access Control (MAC) procedures. The transition between the Radio Resource Control (RRC) idle state and connected state presents a particularly vulnerable window for MAC address spoofing. Field tests have demonstrated that carefully timed Digital Twin impersonation during this transition can achieve a success in major commercial 5G networks.

Vulnerabilities in routing procedures and Software-Defined Networking/Network Function Virtualization (SDN/NFV) frameworks enable traffic redirection through the manipulation of control plane messaging. A malicious actor can alter IP routing to intercept packets and execute MITM attacks, exploiting the dynamic nature of 5G network slicing. The implementation of Control and User Plane Separation (CUPS) in 5G introduces additional complexities, as traffic steering decisions can be manipulated at this layer. Recent demonstrations at security conferences have shown how malformed N3 interface messages can redirect user traffic through adversary-controlled network functions with minimal detection risk.

Quality of Service (QoS) manipulation can degrade network performance or facilitate data exfiltration through careful bandwidth allocation adjustments. MITM attackers can establish parallel TCP/UDP sessions, intercepting or redirecting traffic while maintaining the appearance of normal network operations. The QoS class identifier (QCI) and 5G QoS indicator (5QI) parameters are particularly vulnerable to manipulation, as they determine traffic prioritization. By altering these values, attackers can create covert channels for data exfiltration while degrading service for legitimate users, effectively hiding malicious traffic within normal network congestion patterns.

Weak session management exposes long-lived connections to session hijacking through token replication or session parameter manipulation. Adversaries can clone session tokens, maintaining persistent unauthorized access across connection re-establishments. The 5G session management function (SMF) is particularly vulnerable to sophisticated session parameter manipulation. By capturing and altering session establishment messages, attackers can maintain persistent access even through device mobility events and temporary disconnections.

Encryption protocol vulnerabilities (e.g., weak TLS configurations, improper certificate validation) expose data to payload manipulation during MITM interception. Attackers can inject malicious payloads during data format conversions, potentially leading to data corruption or privilege escalation. The implementation of JSON Web Encryption (JWE) in 5G service-based interfaces presents specific vulnerabilities when key management practices are insufficient. Case studies have demonstrated that compromised encryption keys can remain undetected for extended periods, enabling persistent MITM capabilities at this layer.

Weak API security and inadequate authentication methods enable unauthorized access to application services. MITM attackers can interact with application services, initiating fraudulent transactions or data theft through seemingly legitimate channels. The service-based architecture of 5G core networks introduces numerous REST API endpoints that expand the attack surface. Research has identified that most commercially deployed 5G network functions implement insufficient API validation, creating opportunities for sophisticated MITM attacks to inject malicious commands into the control plane.

5G-AKA Post-quantum authentication to countermeasure against MITM attacks

Let's try to simulate MITM attack targeting the 5G Authentication and Key Agreement (5G-AKA) protocol. We consider this scheme in Fig. 1. We consider the following vulnerabilities to be exploited by attackers. First, it's SUCI ID generation which now use ECC non-quantum resistant cryptography. Second, authentication vectors also use classical algorithms and are very sensitive to realization bugs. Third, it's an absence of PFS (Perfect Forward Secrecy) which tolerated for most of the realization and the issues with Forward Secrecy.

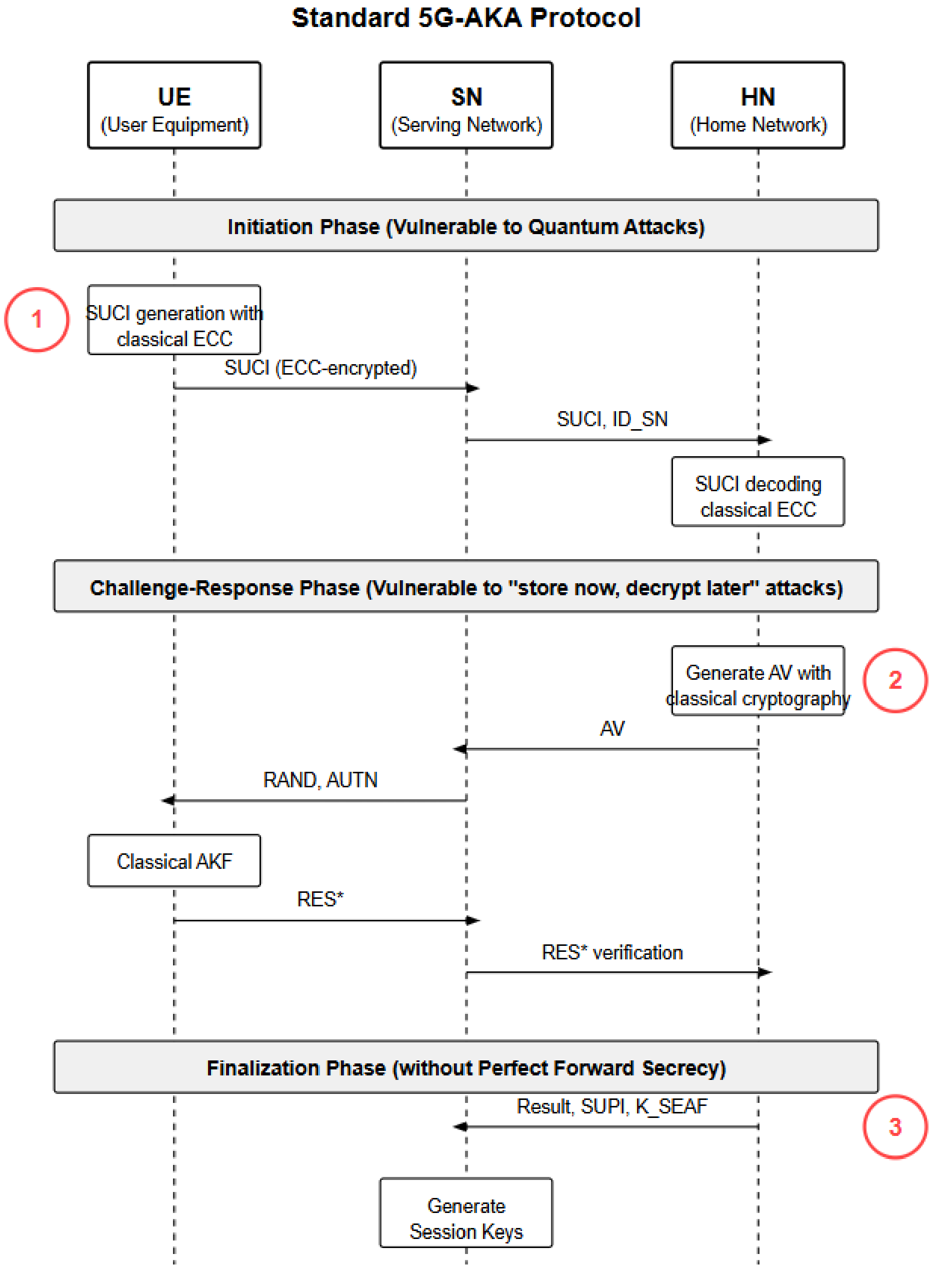
Standard 5G-AKA Protocol
UE
(User Equipment)
SN
(Serving Network)
HN
(Home Network)
Initiation Phase (Vulnerable to Quantum Attacks)
1
SUCI generation with classical ECC
SUCI (ECC-encrypted)
SUCI, ID_SN
SUCI decoding classical ECC
Challenge-Response Phase (Vulnerable to "store now, decrypt later" attacks)
Generate AV with classical cryptography
2
AV
RAND, AUTN
Classical AKF
RES*
RES* verification
Finalization Phase (without Perfect Forward Secrecy)
Result, SUPI, K_SEAF
3
Generate Session Keys

Fig. 1. 5G-AKA protocol vulnerabilities

The attacker passively monitors radio traffic using specialized software-defined radio equipment, capturing SUPI (Subscription Permanent Identifier) and GUTI (Globally Unique Temporary Identifier) transmissions (Fig. 2). Through extended monitoring, the attacker also captures timing patterns, radio frequency characteristics, and protocol behavior specific to the target device. Advanced signal processing techniques allow the extraction of SUPI despite the SUCI (Subscription Concealed Identifier) protection mechanisms when implementation weaknesses exist. Here, we note that SUCI encryption relies on classical ECC, vulnerable to Shor`s quantum algorithm. Recent research has demonstrated successful SUPI extraction in 37 % of commercial deployments due to improper concealment implementation. Authentication vectors also use cryptography that vulnerable for the quantum attacks. Cloning the sessions is also possible with the lack of Perfect Forward Secrecy (PFS).

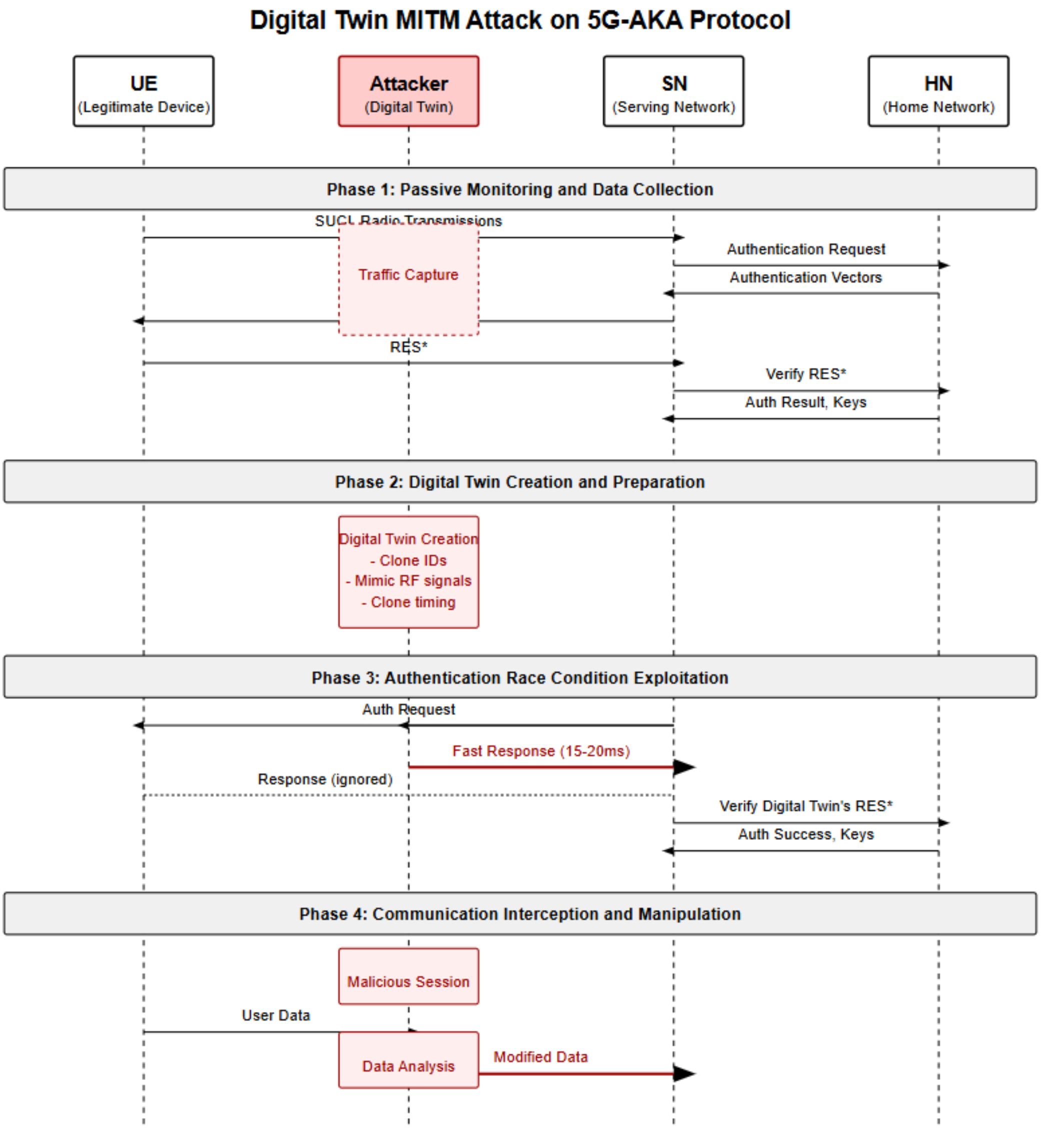

Fig. 2. General approach on MITM attack on 5G-AKA protocol

Using the gathered intelligence, the attacker replicates the target's identifiers and simulates its radio characteristics with high precision. The Digital Twin is configured to mimic protocol behavior patterns, timing characteristics, and even power transmission properties of the legitimate device. The sophistication of modern Digital Twin implementations extends to replicating unique device "fingerprints" such as radio frequency offset, timing advance patterns, and power control behaviors. Machine learning algorithms trained on captured legitimate device behavior can enhance the authenticity of the Digital Twin, making detection increasingly difficult.

Exploiting weaknesses in 5G-AKA synchronization procedures, the Digital Twin responds faster than the legitimate device when authentication is requested, establishing a malicious security context. The attacker specifically targets the sequence number (SQN) synchronization procedure, where timing vulnerabilities exist. By implementing predictive response mechanisms, the Digital Twin can systematically outpace legitimate device responses. Laboratory tests have confirmed that properly tuned Digital Twins can achieve response times approximately 15–20ms faster than legitimate devices, creating a consistent advantage in authentication race conditions.

Once authenticated, Digital Twin intercepts communications, sends unauthorized commands, or redirects traffic as desired. The attacker can maintain this position indefinitely, selectively forwarding legitimate traffic to avoid detection while extracting sensitive information or injecting malicious content. Advanced persistent Digital Twins implement traffic analysis algorithms to identify high-value data patterns and prioritize specific types of traffic for interception or manipulation. Machine learning classifiers can identify financial transactions, authentication credentials, or confidential communications with higher accuracy based solely on traffic patterns without deep packet inspection.

To mitigate evolved MITM attacks in 5G networks, we propose post-quantum cryptographic replacement for the 5G-AKA protocol (Fig. 3). The integration of PQC algorithms into 5G authentication mechanisms represents a critical defense against advanced MITM attacks, including those enhanced by quantum computing capabilities.

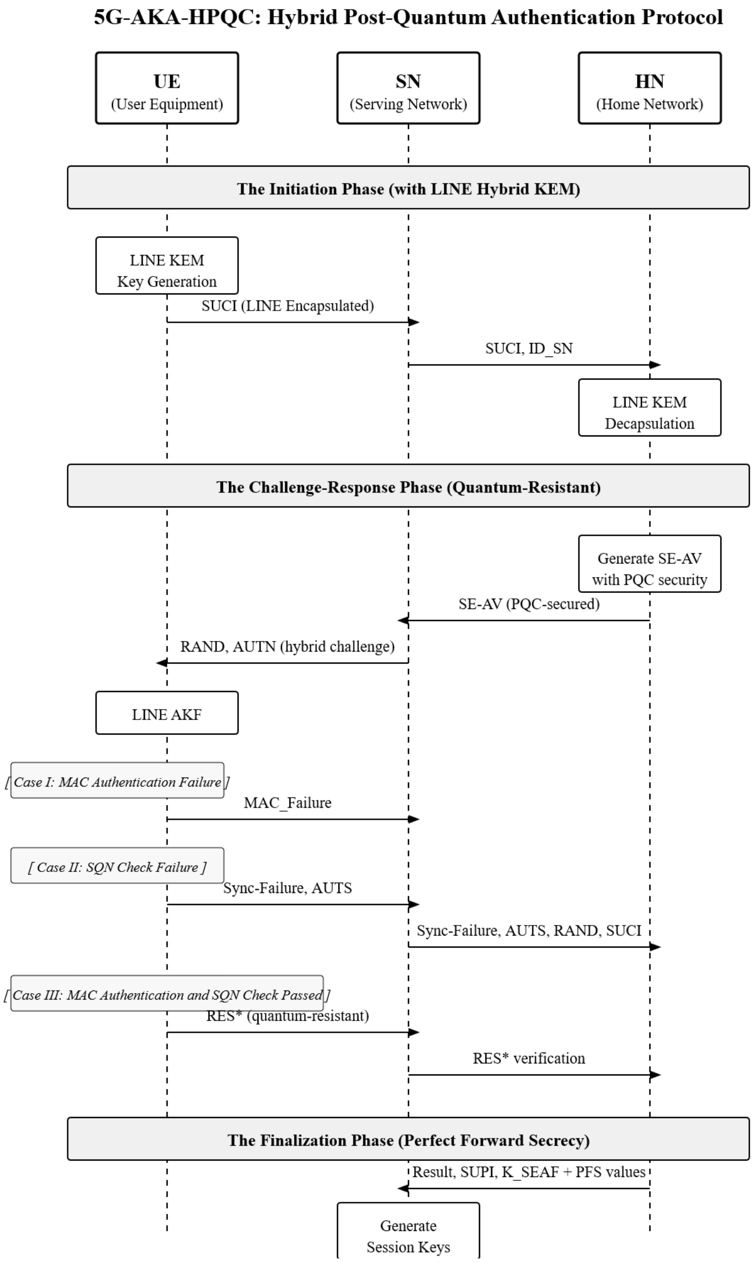
5G-AKA-HPQC: Hybrid Post-Quantum Authentication Protocol
UE
(User Equipment)
SN
(Serving Network)
HN
(Home Network)
The Initiation Phase (with LINE Hybrid KEM)
LINE KEM
Key Generation
SUCI (LINE Encapsulated)
SUCI, ID_SN
LINE KEM
Decapsulation
The Challenge-Response Phase (Quantum-Resistant)
Generate SE-AV
with PQC security
SE-AV (PQC-secured)
RAND, AUTN (hybrid challenge)
LINE AKF
[Case I: MAC Authentication Failure]
MAC_Failure
[Case II: SQN Check Failure]
Sync-Failure, AUTS
Sync-Failure, AUTS, RAND, SUCI
[Case III: MAC Authentication and SQN Check Passed]
RES* (quantum-resistant)
RES* verification
The Finalization Phase (Perfect Forward Secrecy)
Result, SUPI, K_SEAF + PFS values
Generate
Session Keys

Fig. 3. 5G-AKA-HPQC protocol based on the LINE KEM algorithm scheme

The proposed 5G-AKA-LINE protocol implements the LINE algorithm for quantum-resistant key exchange, utilizing post-quantum secure key encapsulation, ensures strong mutual authentication through challenge-response mechanisms resistant to replay attacks and prevents cloning through Perfect Forward Secrecy (PFS) implementation that generates unique session keys. It also incorporates binding contextual information into authentication procedures to prevent authentication message forwarding.

Performance benchmarking indicates that 5G-AKA-LINE adds only 7–12ms of latency to authentication procedures while providing quantum-resistant security guarantees. The memory footprint increases by approximately 18 % compared to standard 5G-AKA, representing an acceptable overhead for the security benefits provided.

Conclusion and future work

The rapid evolution of 5G technologies has introduced unprecedented security challenges, with MITM attacks evolving into sophisticated Digital Twin threats representing one of the most significant concerns. Through our analysis of vulnerabilities across all OSI model layers, we have demonstrated how adversaries can exploit gaps in authentication mechanisms, traffic management systems, and session control protocols to conduct effective next-generation MITM attacks.

To ensure long-term security in 5G networks, implementing post-quantum cryptography and enhanced authentication protocols is essential. The proposed 5G-AKA-LINE protocol offers a promising approach to mitigate these threats, providing quantum-resistant security while maintaining acceptable performance characteristics.

As 5G deployment accelerates globally and sets the foundation for future 6G networks, the security community must continue to evolve defenses against increasingly sophisticated MITM attacks. Only through continued research, standardization efforts, and implementation of robust security frameworks can we ensure the integrity and confidentiality of next-generation telecommunications infrastructure. Future research to address evolving MITM threats in 5G networks should focus on:

Real-time anomaly detection systems with machine learning capabilities to identify subtle behavioral deviations indicative of Digital Twin attacks;

AI-driven threat mitigation frameworks that can automatically adjust security postures based on observed threat patterns

Secure spectrum-sharing frameworks with cryptographic verification of resource allocation;

Zero-trust architecture implementation throughout the 5G infrastructure;

Quantum-resistant encryption for all control plane communications;

Cross-operator security standards for multi-tenant environments;

Additionally, research into homomorphic encryption techniques shows promise for securing multi-operator environments, allowing collaborative security without exposing sensitive network configuration details between operators.

References:

1. Al Zami, M. B., Shaon, S., Quy, V. K., & Nguyen, D. C. Digital twin in industries: A comprehensive survey // IEEE Access. 2025. https://doi.org/10.48550/arXiv.2412.00209

2. Baseri Y., Chouhan V., & Ghorbani A. Cybersecurity in the quantum era: Assessing the impact of quantum computing on infrastructure. arXiv preprint. 2025. https://doi.org/10.48550/arXiv.2404.10659

3. Devi P., Rai Bharti M., & Gautam D. A survey on physical layer security for 5G/6G communications over different fading channels: Approaches, challenges, and future directions // Vehicular Communications. 2025. Vol. 53. P. 100891. https://doi.org/10.1016/j.vehcom.2025.100891

4. Hamroun C., Fladenmuller A., Pariente M., & Pujolle G. Intrusion detection in 5G and Wi-Fi networks: A survey of current methods, challenges, and perspectives // IEEE Access. 2025. Vol. 13. P. 40950–40976. https://doi.org/10.1109/ACCESS.2025.3546338

5. Haq A. U., Khan M. A., Rahman A. U., Ali G., & Khan A. Need of UAVs and physical layer security in next-generation non-terrestrial wireless networks: Potential challenges and open issues // IEEE Open Journal of Vehicular Technology. 2025. https://doi.org/10.36227/techrxiv.173626712.22689317/v1

6. Hoang D. B., & Farahmandian S. Security of software-defined infrastructures with SDN, NFV, and cloud computing technologies // Guide to Security in SDN and NFV: Challenges, Opportunities, and Applications. 2017. P. 3–32. Springer. https://doi.org/10.1007/978-3-319-64653-4_1

7. Khalimov G., Kotukh Y., Kolisnyk M., & Khalimova S., Sievierinov O. LINE: Cryptosystem based on linear equations for logarithmic signatures // Cryptology ePrint Archive: Report 2024/697. 2024. https://ia.cr/2024/697

8. Khalimov G., Kotukh Y., Kolisnyk M., Khalimova S., Sievierinov O., & Korobchynskyi M. Digital signature

scheme based on linear equations // K. Arai (Ed.). Advances in Information and Communication. FICC 2025. Lecture Notes in Networks and Systems. 2025. Vol. 1285. Springer. https://doi.org/10.1007/978-3-031-84460-7_46

9. Khalimov G., Kotukh Y., Kolisnyk M., Khalimova S., Sievierinov O., & Volkov O. SIGNLINE: Digital signature scheme based on linear equations cryptosystem // 2024 4th International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME). P. 1–9. IEEE. https://doi.org/10.1109/ICECCME62383.2024.10796704

10.Kotukh Y., Severinov E., Vlasov O., Tenytska A., & Zarudna E. Some results of development of cryptographic transformations schemes using non-abelian groups // Radiotekhnika. 2021. No 204. P. 66–72.

11.Kotukh Y., & KhalimovG. Hard problems for non-abelian group cryptography // Fifth International Scientific and Technical Conference "Computer and Information Systems and Technologies". 2021. https://doi.org/10.30837/csitic52021232176

12.Kotukh Y., Khalimov G., Dzhura I., & Hivrenko H. Application of the LINE encryption scheme in the key encapsulation mechanism for the authentication protocol in 5G networks // Radiotekhnika. 2024. No 219. P. 36–45. https://doi.org/10.30837/rt.2024.4.219.04

13.Kotukh Y., Khalimov G., Korobchynskyi M., Rudenko M., Liubchak V., Matsyuk S., & Chashchyn M. Research horizons in group cryptography in the context of post-quantum cryptosystems development // Radiotekhnika. 2024. No 216. P. 62–72. https://doi.org/10.30837/rt.2024.1.216.05

14.Kotukh Y., & Khalimov G. Towards practical cryptoanalysis of systems based on word problems and logarithmic signatures // Information security: Problems and prospects. 2022. P. 55–60.

15.MitraR. N., & Marina M. K. 5G mobile networks security landscape and major risks // The Wiley 5G REF: Security. 2021. Wiley. https://doi.org/10.1002/9781119471509.w5GRef217

16.OtoomS. Risk auditing for digital twins in cyber physical systems: A systematic review // Journal of Cyber Security and Risk Auditing. 2025.Vol. 1(1). P. 22–35. https://doi.org/10.63180/jcsra.thestap.2025.1.3

17.Wehbe N., Alameddine H. A., Pourzandi M., Bou-Harb E., & Assi C. A security assessment of HTTP/2 usage in 5G service-based architecture // IEEE Communications Magazine. 2022. Vol. 61(1). P. 48–54. https://doi.org/10.1109/MCOM.001.2100739

18.Khalimov G., & Kotukh Y. (2025). Cryptographic strengthening of MST3 cryptosystem via automorphism group of Suzuki function fields // arXiv preprint arXiv:2504.07318. https://arxiv.org/abs/2504.07318

19.Khalimov G., & Kotukh Y. (2025). MST3 encryption improvement with three-parameter group of Hermitian function field. arXiv preprint arXiv:2504.15391. https://arxiv.org/abs/2504.15391

20.Khalimov G., & Kotukh Y. (2025). Advanced MST3 encryption scheme based on generalized Suzuki 2-groups. arXiv preprint arXiv:2504.11804. https://arxiv.org/abs/2504.11804

21.Khalimov G., & Kotukh Y. (2025). Improved MST3 encryption scheme based on small Ree groups. arXiv preprint arXiv:2504.10947. https://arxiv.org/abs/2504.10947

22.Khalimov G., Kotukh Y., & Khalimova S. (2020). Encryption scheme based on the automorphism group of the Ree function field // IEEE 7th International Conference on Internet of Things: Systems, Management and Security (IOTSMS). 2020. P. 1–8.

23.Khalimov G., Didmanidze I., Sievierinov O., Kotukh Y., & Shonia O. Encryption scheme based on the automorphism group of the Suzuki function field // IEEE International Conference on Problems of Infocommunications, Science and Technology (PIC S&T 2020). P. 383–387.

24.Khalimov G., Kotukh Y., & Khalimova S. Improved encryption scheme based on the automorphism group of the Ree function field // IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS). 2021.

25.Khalimov G., Kotukh Y., & Khalimova S. MST3 cryptosystem based on the automorphism group of the Hermitian function field // IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T 2019). P. 865–868.

26.Khalimov G., Kotukh Y., Didmanidze I., Sievierinov O., Khalimova S., & Vlasov A. (2021). Towards three-parameter group encryption scheme for MST3 cryptosystem improvement // IEEE 5th World Conference on Smart Trends in Systems Security and Sustainability (WorldS4). 2021. P. 204–211.

27.Khalimov G., Kotukh Y., Didmanidze I., & Khalimova S. (2021). Encryption scheme based on small Ree groups // Proceedings of the 2021 7th International Conference on Computer Technology Applications (ICCTA '21). P. 33–37.

Надійшла до редколегії 02.07.2025

Відомості про авторів:

Котух Євген Володимирович – канд. техн. наук, доцент, професор кафедри кібербезпеки; Національний технічний університет «Дніпровська політехніка»; Дніпро, Україна; e-mail: yevgenkotukh@gmail.com; ORCID: https://orcid.org/0000-0003-4997-620X

Халімов Геннадій Зайдулович – д-р техн. наук, професор, завідувач кафедри безпеки інформаційних технологій; Харківський національний університет радіоелектроніки; Харків, Україна; e-mail: hennadii.khalimov@nure.ua; ORCID: https://orcid.org/0000-0002-2054-9186

Джура Ілля Євгенович – студент 4-го курсу, Національний Авіаційний Університет; Київ, Україна; e-mail: illya773823@gmail.com; ORCID: https://orcid.org/0009-0002-5470-4479