Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 13 Issue 11, November 2024

Secure 5G Network Architecture for Armed Forces

Arjun V Kansal, Tony K Joseph

Faculty of Communication Engineering,
Military College of Telecommunication Engineering,
Mhow, Madhya Pradesh (India)

***Abstract*—Technologies like 5G, 6G, and beyond are designed to usher in a new era of services, accompanied by freshdemands and complexities, all geared towards providing seamless and higher data rate mobile connectivity on a global scale. These next-generation networks, surpassing the capabilities of 5G, are anticipated to deliver superior quality of service, exceptionally high data speeds, enhanced network security, increased capacity, minimal latency, and cost- effectiveness. While these technologies hold great promise for network advancement, they also introduce a host of security concerns and challenges, underscoring the critical importance of network security in the future landscape of wireless communication. This paper delves into a thorough exploration of recent developments in security issues related to 5G, each stemming from the aforementioned key enabling technologies. It scrutinizes methods to fortify the network's security while simultaneously addressing the demands of emerging services and the requisites of users. In this manuscript, the challenges of modern era warfare wireless network scenario are discussed which susceptible to attacks and threats. The paper discuss various security overlays shall be added to strengthen the security of military communication. The paper is supported by a PQC core architecture on a 5G core network.**

***Keywords*—5G, NFV, SDN, network slicing, security, privacy**

I. INTRODUCTION

The deployment of 5G wireless networks involves the expansion of advanced data and coverage through the deployment of denser stations with larger capacity, thereby improving the quality of service (QoS) of ultra-fast and low-latency (URLLC), which is a large machine (mMTC) and Enhanced Mobile Broadband (eMBB). In order to realize the desired services, many important supporting technologies are introduced. These applications improve network connectivity, detailed network management and control, and eliminate the barriers to OEM-independent solutions. Therefore, they are considered to be important for the future development of the website. 5G generally takes it to another level compared to previous generation and is designed for communication technology. But despite these new technologies and ideas, ensuring network security and protecting user privacy still poses a major challenge for future wireless networks.

The security framework of 5G builds upon the foundation of 4G security, albeit with significant enhancements. 4G cellular networks encompassing network access security and network domain security remains largely unchanged in 5G with additional security features to safeguard the distributed base station designs. The most significant alterations occur in authentication mechanism, while in 4G, authentication is only done in the access/service network, in 5G, two new nodes are introduced in the mobile device and network path, which is the security anchor that runs the authentication server function and security repositories.

The nodes are used to create more isolation between the existing network serving customers and the home network, which makes it difficult to generate certificates for the network core. While in previous cellular implementations, UEs send their IMSIs in an unencrypted format, which makes it vulnerable to interception and user tracking, 5G encrypts the user's identity before receiving the condition called SUCI (SUPI encrypted). This encryption is based on a private key pair that can only be decrypted by the home network. Therefore, the customer's identity is well hidden, which makes it difficult to track. In addition, the concept of GUTI (Global Temporary Identification) is a temporary identity provided in 5G, which is constantly changing and strengthens privacy by interfering with the user's ability and identity. 4G networks have encountered many challenges and security issues, including leaks in user privacy, wireless interface vulnerabilities, weak home controls, and infrastructure limitations. By incorporating these challenges from 4G security into its design, 5G aims to create a reliable security system that is effective in solving known problems and adapting to emerging threats in changing wireless communications.

The paper investigates the security challenges raised from the salient key enabler technologies. The paper is organised as follows: Part I discusses the security elements of 5G network followed by Part II highlighting security concerns in various key enabler technologies. Then, we discuss how the security vulnerabilities can be addressed in Part III. Part IV entails proposed security architecture for military 5G network. Part V includes challenges and implications in Armed Forces. Part VI includes conclusion and way ahead.

II. 5G SECURITY ARCHITECTURE

A. *5G Security Elements*

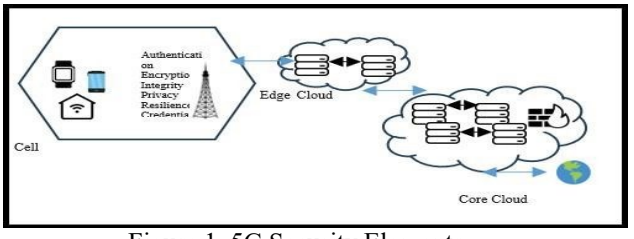

Figure 1. 5G Security Elements

The security elements in 5G can be broadly classified into three levels, i.e., Cell level, Edge Cloud level and Central Cloud level. Millions of devices not only phones, IoT and different types of base stations will be scattered in the cell level.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 13 Issue 11, November 2024

Devices at edge level mainly facilitate higher speed of processing various services and applications The Central cloud, called core network having various new technologies such as Network Slicing, SDN, NaaS, etc. In cell level, security features such as enhanced mutual authentication; identity concealment (privacy), encryption algorithms and deeper mandatory protection features has been introduced in 5G. The security aspects of each level are discussed in subsequent paragraphs.

B. Security Architecture Specified by 3GPP

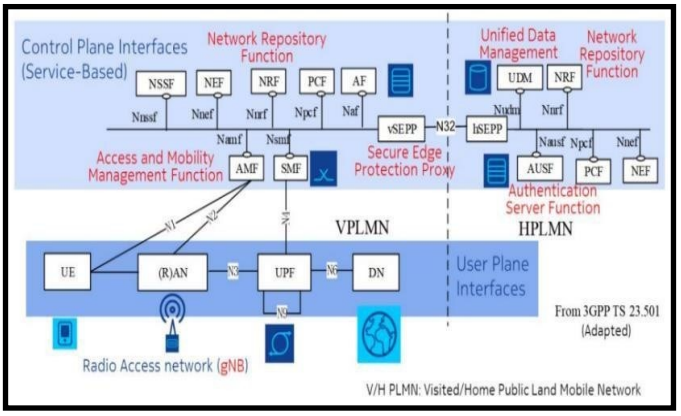

Figure 2. 3GPP Security Specification

5G security architecture is generally divided into the following areas as shown in figure 2: network access security (3GPP access network and non3GPP access network) to prevent radio interference from attacks; network security to ensure data security exchange and aircraft user data; user security to prevent users from accessing mobile devices; with other network domains. SBA uses IPsec and OAuth2.0. Another security feature introduced in 5G is the Secure Edge Protection Proxy (SEPP), which is located at the PLMN border and ensures confidentiality and/or integrity in the service used and developer services. It works as an access and management system for internal network operations and topology concealment by reducing the internal topology information visible to the outside.

The 5G system provides the various security features in the 5G core network: AUSF, self-authentication operator. AUSF is located in the home network and manages end-user authentication requests with the support of UDM, ARPF is the foundation of UDM, which enables the 5G Home Environment Authentication Vector (HE AV) based on user integration. SIDF, Record Hiding Function, is provided by UDM and is responsible for hiding SUPI from SUCI. SIDF access rights should be defined so that only network elements located in the network are allowed to make SIDF requests. Lastly, SEAF, Security Anchor Function, facilitates authentication through AMF (entry point for core network from radio side) in the serving network used during primary authentication using SUCI. It is located at serving network. The long-term keys used for the purpose of authentication and security setup are stored at UDM (Unifies Data Management) in home network to protect it from physical attacks maintaining the integrity of the specifications.

The security measures within the 5G core network encompass a range of operations, including the establishment of trust boundaries, imposition of essential security criteria on the service-based architecture, and the specification of requirements for end-to-end security in core network interconnections. Mobile network operators organize their networks into distinct trust zones, with sub networks operated by different entities residing in separate trust zones. These cross-border messages must comply with security procedures that include prerequisites such as service registration, discovery, and tracking permission to ensure confidentiality, integrity, and protection against reverse attacks. These are designed to prevent NFs in one trust or trust from being issued and owned by entities in another trust or trust. In the border region, each NF strictly verifies the identity of all incoming messages. Messages that do not comply with the network specifications and conditions will be rejected or discarded. End-to-end network security involves ensuring the confidentiality and/or integrity of specific messages defined by 3GPP, extending from the core network to the live target To meet this need, the Security Edge Provider (SEPP) is deployed at the edge between the base and the network. SEPP cooperation provides confidentiality and/or integrity for messaging between the two (PLMNs).

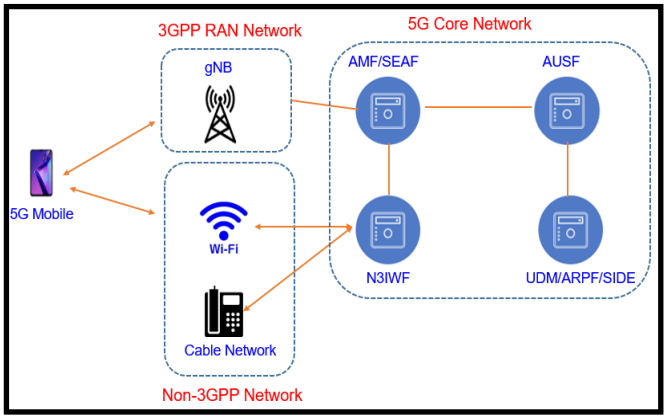

Figure 3. NFs relevant to 5G authentication

C. Authentication and Key Agreement

The 3GPP AKA protocol is used for symmetric key- based challenge-response authentication between the user equipment and the network. After the mutual authentication, encryption keys will be sent for further communication in the C-plane and U-plane data. The 5G AKA process is independent of network access and has three authentication techniques, namely 5G-AKA, EAP-AKA™ and EAP-TLS. The process of authentication is segregated into two phases i.e., Authentication Initiation and Authentication. In Phase 1, UE sends RRC setup request to gNB. gNB sends back an acknowledgement as RRC setup response. UE further sends RRC setup request complete and NAS message which is directed to AMF (Initial UE registration request). AMF seeks for SUCI from UE as NAS ID request and UE forwards SUCI as NAS ID response

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 13 Issue 11, November 2024

If the service network is not allowed to use SNN, the AUSF responds with "Service Network Not Allowed" in the authentication response (NAUSF UE Authentication Authentication Response), otherwise the authentication request (NUDM UE Authentication Acquisition Request) is sent to the UDM/SUCI or ARPF/ SIDF including SUPI and SNN. The AMF sends a challenge to the UE NAS Authentication request. Once calculated, the UE sends the UE NAS Authentication Response. The AMF will check the authenticity and notify the UE and AUSF that the authentication was successful. Release the security channel set.

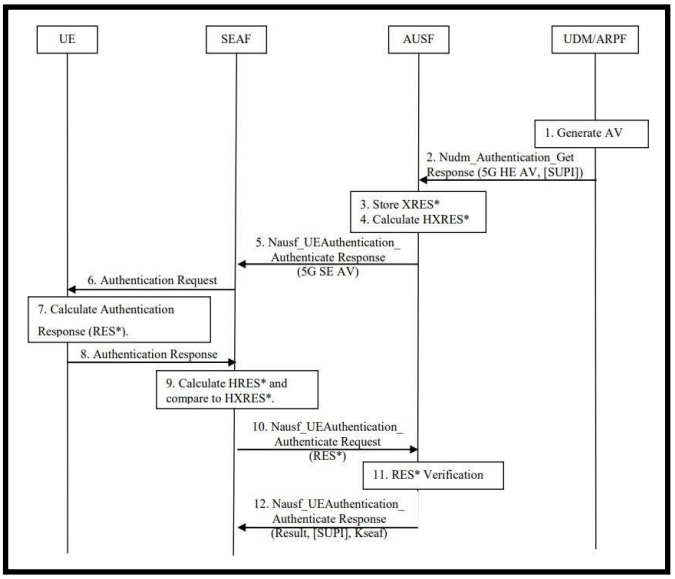

Figure 4. 5G AKA

D. 5G Cipher and Integrity Algorithms

The selection of security algorithms is very important to protect the security of the air interface signal. 5G supports three encryption and security protection algorithms called New Radio Encryption Algorithm and New Radio Integrity Algorithm. NEA1 and NIA1 utilize the SNOW 3G cipher, NEA2 and NIA2 rely on AES, and NEA3 and NIA3 rely on ZUC. They can make emergency calls without a valid USIM and therefore a valid key. Maintaining integrity is crucial to ensuring the authenticity of messages exchanged by constantly proving that both parties have valid keys. Empty security algorithms (such as NEA0 and NIA0) are used for normal communication and are only available to UEs with limited service. They do not provide cryptographic protection or security. Bad actors can use this to launch cyber-attacks.

The AES-128 cipher has a 10-round function, AES-192 has a 12-round function, and AES-256 has a 14-round function. Each round contains four mathematical variables (Sub Bytes function, Sub Bytes function, Mixed line, and Add Round Key function). The AES-128 encryption algorithm works by using electronic technology (AES-CTR) and is claimed to be a secured encryption algorithm. This standard is used for confidentiality and integrity algorithms in 4G and 5G networks. According to the cryptanalysis of AES encryption algorithm, data complexity (2105), time complexity and memory complexity are equal to (274). AES-CTR (GCM) includes 10 rounds and 4 code changes (sub bytes, row changes, shuffled rows and additional round keys). In order to allow brute force attacks, this encryption algorithm relies on a secret key (K =128 bits). It is recommended to increment the length of the switch and shelf block T and use the shelf block to be safer.

The ZUC encryption algorithm requires two keys, including a 128-bit secret key (K) and a 128-bit initial vector key. The first element of ZUC is called LFSR. The second is bit rearrangement (BR) (words: X#0, X#1, X#2, and X#3). NLF includes the names R#1 and R#2; S-box replaces S#0 and S-box replaces S#1. For example, the attack targets the difference in the value of the first byte of the IV key (IV#0). The attacker searches for the key location (299.4) to recover the key. The spectrum analysis method is designed to attack the ZUC cryptographic algorithm, which is the 256-bit version of ZUC. This method is based on the difference in the resistance of the equal value (223).

III. THREATS AND VULNERABILITIES IN 5G SECURITY

The three fundamental pillars for safeguarding 5G network are security, privacy, and trust. Security involves the encryption of user data, while privacy pertains to shielding the actual content of this data. Trust encompasses the processes of authenticating as well as identifying both parties involved. Although vulnerabilities and conventional attacks remains, mitigation techniques to counteract these threats has been incorporated in 5G security architecture. It is also vulnerable to threats and attacks introduced due to use cases. Solutions to protect the above threats are an urgent requirement which is discussed in subsequent paragraphs.

	Use-Case	DL	UL	Network Latency	Reliability	Cost Sensitivity	Security
Consumers	Mobile Broadband	100-300M	10-50M	15-25ms	Medium	Medium	Medium
	Fixed Wireless Access	1-5G	100-200M	1-20ms	High	High	Medium
	Event experience	1-100M	1-5G	1-5ms	Medium	Medium	Medium
	In-vehicle Infotainment	5-100M	1k-1M	1-20ms	Medium	Medium	Medium
Industries	Critical automation	1M	1-10M	1-5ms	Very high	Low	Very High
	Tele-operation	1M	1-10M	1-25ms	Very high	Low	Very-High
	Highly interactive AR	5-100M	1-100M	1-10ms	High	Medium	High
	Mass sensor arrays	1k-1M	1k-1M	200-500ms	Low	Very High	Medium-High

Figure 5. Security Implications of Use Cases

1. Man-in-the-Middle Attack - The attack happens when an attacker stealthily intercepts and intentionally alters the communication between two parties (e.g., a user and the network) without their knowledge. In 5G networks, MitM attacks pose a heightened risk due to the complex and distributed architecture. Attackers deploy fake base stations that mimic legitimate 5G cells to trick nearby devices into connecting to them. Once connected, the attacker can intercept or modify traffic. Vulnerabilities in protocols such as HTTP/2, Diameter, or even legacy signaling systems (SS7, SIP) can be exploited. An attacker sitting in the middle may intercept authentication tokens, session keys, or sensitive data

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 13 Issue 11, November 2024

2. Quantum Computing Attacks - It uses quantum mechanical principles like superposition with entanglement to resolve problems quicker than traditional computers. While this promises to reform fields like artificial intelligence and cryptography, it also creates serious security issues. Many encryption algorithms used in 5G, such as RSA, ECC, and Diffie-Hellman, rely on mathematical complexity like factorization and discrete logarithms. Quantum algorithms like Shor's algorithm could solve these problems faster, rendering current encryption methods obsolete. Attackers can now capture and store 5G encrypted traffic so they can decrypt it in the future, just as quantum computers do. Quantum computing can weaken the security of authentication mechanisms and critical transactions, making the network vulnerable to attacks. If private keys or certificates are compromised, an attacker can control an entire slice of the 5G network. It can occur at any security layer of the 5G network. The impact of quantum risk will be the decryption of sensitive data transmitted over 5G networks, bypassing authentication methods based on classical cryptography, and the impact of 5G-enabled smart grid, healthcare, and related transportation.

3. Distributed Denial of Service Attack - A DDoS attack involves overwhelming a network, server with a flood of traffic from various sources, rendering it unavailable to lawful users. In 5G networks, DDoS risks are amplified due to increased connectivity, higher device density, and diverse use cases. Millions of poorly secured IoT devices in the 5G ecosystem can be hijacked and controlled by attackers to form botnets. Botnets like Mirai have already demonstrated the catastrophic potential of IoT-based DDoS attacks. 5G networks use network slicing to create virtualized, dedicated slices for specific services. A DDoS attack targeting one slice (e.g., an autonomous vehicle slice) can disrupt critical services and potentially spill over to other slices. 5G employs edge computing for low-latency applications. Compromised edge nodes can become sources of massive traffic directed at the network core.

4. M2M communication attack: In machine-to-machine communication, many devices are connected in the network and sensitive information is exchanged, which creates security and privacy issues. M2M attacks fall into three categories: information threats, attacks, and physical attacks. Threats target software systems and include DoS attacks, fraud, and threats. Physical threats cause physical damage through theft, software modification, sabotage, environmental damage, and external attacks. Data threats include selective redirection, personal access, and data tampering. Using network slicing helps create separate virtual networks tailored to specific applications. Each form can have its own security policies and procedures to ensure that M2M communication remains secure in the chosen form. Policies such as firewall rules, access lists, and role-based access control (RBAC) work well.

5. Data Interception and Privacy Breaches - With the advent of 5G networks, data interception and privacy breaches pose significant challenges. These threats exploit vulnerabilities in the network's architecture, communication protocols, and user behaviours to access, manipulate, or misuse sensitive data. If certain portions of communication are transmitted without encryption, attackers can intercept the data uses tools like packet sniffers and Unencrypted IoT devices, legacy 4G/3G interworking. Exploiting out dated or improperly implemented cryptographic algorithms can allow attackers to decrypt sensitive communication like Exploiting deprecated protocols like TLS 1.0 or insecure encryption keys. Malicious applications can request excessive permissions or embed spyware to collect user data like IoT devices sending telemetry data to unauthorized servers. Malicious insiders within telecom operators or service providers can misuse their access to intercept user data like Surveillance, corporate espionage, or data leaks.

While most of the cryptographic algorithms used in 5G (such as RSA, ECC, and Diffie-Hellman) are based on the complexity of mathematical problems such as factorization and discrete logarithms, we will focus on quantum computing attacks in 5G network security architectures. Quantum algorithms such as Shor's algorithm can solve these problems faster, making current encryption methods obsolete. Therefore, the cryptographic scheme in 5G (ECIES - Elliptic Curve Integrated Encryption Scheme) is not completely secure against quantum computing attacks and should be replaced with strong post-quantum cryptographic algorithms as post-quantum telecommunication networks.

IV. SECURITY OVERLAYS AND PROPOSED 5G NETWORK ARCHITECTURE FOR ARMED FORCES

The aim of this research is to implement, integrate, and migrate a robust and secure 5G network infrastructure that integrates post-quantum cryptography and quantum random number generators (QRNG) to protect against quantum computation. The project focuses on ensuring data integrity, confidentiality, and availability in future mobile communications by enhancing the security of 5G core networks. This will provide a protective and future-proof system that can prevent cyber threats, thus contributing to the security of5G technologies in critical applications and enterprises. The current 5G core relies on classical encryption algorithms such as ECC to ensure data security. However, due to the rapid development of quantum computing, these algorithms are vulnerable to quantum attacks.

RSA and ECC encryption methods rely on the complexity of parsing large numbers and solving the elliptic curve discrete logarithm problem accordingly, and can be effectively broken by quantum computers using Shor's algorithm, thus affecting their security. Current implementations such as ECIES for key exchange and AES-128 for 5G network encryption are not sufficient to deal with quantum threats. ECIES uses elliptic curve cryptography, which is vulnerable to quantum computer attacks, while the security of AES-128 will be halved by quantum attacks. These vulnerabilities pose a serious risk to the confidentiality of military communications and information, and require the adoption of quantum-safe encryption solutions to ensure long-term security against quantum threats.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 13 Issue 11, November 2024

A. Synergy Post Quantum Cryptography Solution

1. Quantum-Safe 5G Core System Architecture – It is proposed todeploy and migrate to a secure 5G core system and beyond integrated with advanced PQC technologies. This new architecture will provide a secure and resilient communication framework suitable for military applications. The solution will include the following components:

PQC Algorithms: Implement CRYSTALS-Kyber for key encapsulation andencryption.

QRNGs: Utilize Quantum Random Number Generators for high-entropy keygeneration.

KEM-TLS: Integrate KEM-TLS for secure key exchange protocols in 5G and beyond Core enhancements.

Cloud-Native 5G Core: Develop a cloud-native 5G core architecture leveraging micro services and containerization for flexible, scalable, and efficient deployment. This will enable dynamic scaling of network functions and services, ensuring optimal performance and resource utilization.

Service-Based Architecture (SBA): Utilize SBA to enhance the modularity and flexibility of the 5G core network, allowing seamless integration of PQC algorithms and other security features. SBA enables efficient service discovery and communication between network functions.

Network Slicing: Implement advanced network slicing techniques to create isolated and secure network segments for different military applications. This ensures dedicated resources and optimized performance for critical communications.

Ultra-Reliable Low-Latency Communication (URLLC): Develop URLLC capabilities to support mission-critical applications that require extremely low latency and high reliability. This will ensure that critical military communications are delivered with the highest priority and with minimal delay.

2. Lattice Based Cryptography utilizes mathematical lattices for encryption and decryption, resisting quantum attacks due to the complexity of lattice problems. CRYSTALS-Kyber, a lattice-based key encapsulation mechanism (KEM), is designed for post-quantum security, and suitable for 5G/B5G applications. It facilitates efficient key exchange and encryption, ensuring robust security against quantum adversaries. The operations of Crystal-Kyber include:

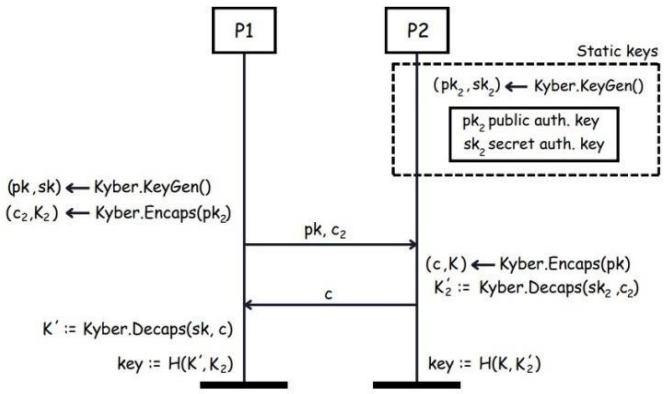

Figure 6. Crystal Kyber

Key Generation: Public and private keys creation. Encapsulation: Secure transmission of a message usinga shared secret and cipher text based on the recipient's public key.

Decapsulation: Retrieval of the shared secret using the recipient's private key.
Crystal-Kyber's efficiency and security make it an excellent choice for safeguarding 5G networks against future quantum threats as shown in figure 6.

3. KEM TLS integrates Key Encapsulation Mechanisms (KEMs) into the Transport Layer Security (TLS) protocol, enhancing secure key exchange mechanisms. In this protocol, the client initiates by sending a key encapsulation request to the server, thereafter the server responds with the encapsulated key and in the end the client decapsulates the key to establish a secure session. Compared to traditional TLS, KEM-TLS significantly reduces handshake latency andmemory footprint. It uses certified long-term KEM public keys for implicit authentication, eliminating the need for generating signatures during the handshake. Despite lattice-based KEMs performing similarly to ECDH, they offer superior security against quantum threats compared to ECDSA as shown in figure 7.

Segmentation. Defence networks require strict

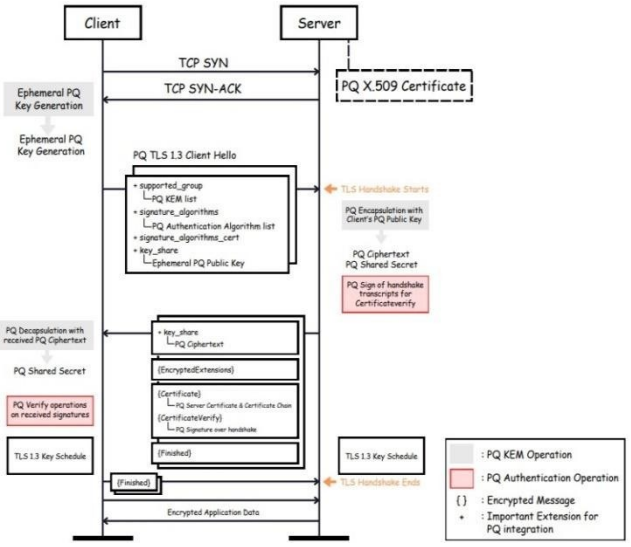

Figure 7. Post Quantum TLS 1.3 Hanshake

B. Proposed 5G Architecture Core

5G Core solution enhanced with Post-Quantum Encryption,operating in two distinct modes as shown in figure 8, It design aims to fortify 5G networks against quantum threats, providing resilient protection against potential vulnerabilities posed by quantum computing.
Hybrid Post-Quantum Encryption: Combines Crystal-Kyber with classical algorithms (Curve25519 and Secp256), leveraging the strengths of both approaches. Homogeneous Post-Quantum Encryption: Exclusively utilizes Crystal- Kyber, ensuring a robust and secure encryption method.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 13 Issue 11, November 2024

The Key components of the 5G Core architecture include:

1. Encryption and Decryption: Uses AES-256 in CTR mode for strong dataprotection.
2. Hashing: Implements HMAC SHA-256 for message integrity and authenticity.
3. Key Generation: Employs QRNG for generating cryptographic keys withhigh entropy and unpredictability.
4. Compliance: Adheres to 3GPP and NIST standards, offering multipleEncryption Profiles for enhanced security and adaptability

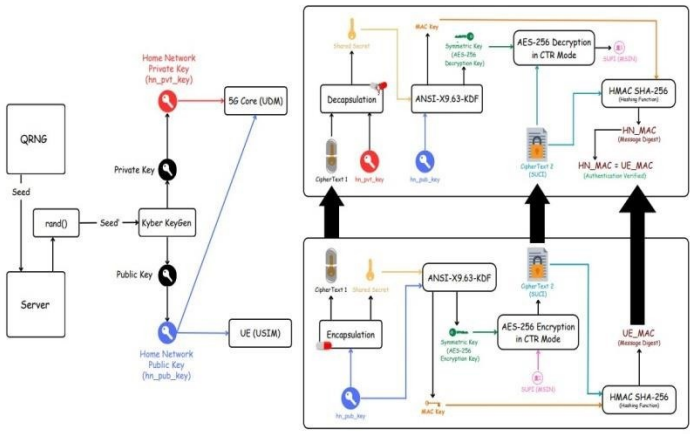

Figure 8. 5G Core

V. CHALLENGES AND MILITARY IMPLICATIONS

A. Challenges

1. Upgrading Complexities - Integrating PQC into existing infrastructure may require substantial changes to network architecture. The transition will likely need hybrid cryptographic approaches where classical and quantum-resistant algorithms coexist until PQC standards are fully adopted and proven. This dual system may complicate network management and security monitoring.

2. High Stake for Critical Infrastructure – Despite these advancements, there are challenges to consider. Transitioning to a quantum-resilient 5G network requires substantial R&D investment, hardware upgrades, and collaboration across multiple domains. Additionally, the secure integration of IoT devices in a tactical environment poses unique operational challenges.

3. Compatibility - Many existing military communication systems are not built with quantum security in mind. Transitioning to a quantum-safe infrastructure would involve replacing or upgrading legacy systems, which requires lots of time.

4. Data Harvesting Attacks – Harvest Now, Decrypt Later in which the Data will be harvested and stored now and it will be decrypted with able quantum computers.

5. High Cost of Implementation: Implementing quantum-secure technology, including PQC and QKD, involves significant upfront costs for research, development, and infrastructure. For example, quantum-secure communication systems often require high-end hardware, specialized cryptographic solutions, and dedicated R&D teams

B. Military Implications

1. Enhanced Communication and Coordination - It is faster and more reliable communication across battlefield units which provide Real-time data sharing and situational awareness with improved command and control (C2) systems using low-latency 5G.

2. Deployment of IoT and Smart Systems - 5G's massivemachine-type communication (mMTC) supports the connection of billions of IoT devices. This is beneficial for deploying smart sensors across battlefields. Smart systems can automate routine tasks such as inventory management, equipment tracking, and supply chain logistics, reducing manual workload and human error

3. Network Resilience and Redundancy - 5G's network slicing feature allows dedicated virtual networks for military operations, ensuring high reliability and minimal interference. Adaptive routing and self-healing networks improve operational continuity in adverse conditions. High-bandwidth connectivity ensures seamless service even during peak demand or in the aftermath of infrastructure damage

4. Cyber security and Data Privacy - 5G introduces advanced encryption and mutual authentication mechanisms, which strengthen the security of sensitive military communications. Quantum-resistant cryptography will provide additional security to the network from adversaries. Improved network visibility allows real-time detection and mitigation of cyber threats

VI. CONCLUSION AND WAY AHEAD

1. Transition to Post-Quantum Cryptographic (PQC) Algorithms - Replacing or augmenting old cryptographic algorithms, such as RSA and ECC, with PQC algorithms that are resistant to quantum computing attacks. Military and tactical 5G networks need to assess various PQC algorithms (e.g., lattice-based, hash-based, multivariate polynomial) and determine the most suitable algorithms for different applications.

2. Developing a Quantum Network Backbone - Establishing a quantum-resistant network infrastructure that incorporates elements Quantum Random Number Generators (QRNGs) to enhance security.

3. Securing Critical Hardware Components - Protecting physical network hardware, such as base stations, routers, and IoT devices, against tampering, physical attacks, and supply chain vulnerabilities.

4. Dedicated Research & Development (R&D) Programs - Establishing long-term R&D programs focused on advancing quantum-resilient technology, which will allow the military to stay ahead of evolving cyber threats.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 13 Issue 11, November 2024

5. Quantum-Resilient Cyber Defense Frameworks- Developing and implementing cyber defense strategies tailored to quantum threats, enabling continuous monitoring, threat detection, and mitigation of quantum-specific cyber risks.

REFERENCES

[1] Fatima Salahdine, Tao Han and Ning Zhang Noble, “Security in 5G and beyond recent advances and future challenges” Wiley published on 20 September 2022.

[2] 5G; Security architecture and procedures for 5G System (3GPP TS 33.501 version 15.4.0 Release 15)

[3] Ijaz Ahmad, Tanesh Kumar, Madhusanka Liyanage, Jude Okwuibe, Mika Ylianttila, and Andrei Gurtov, “Overview of 5G Security Challenges and Solutions,” in IEEE Communications Standards Magazine • March 2018

[4] Ijaz Ahmad, Tanesh Kumary, Madhusanka Liyanagez, Jude Okwuibex, Mika Ylianttila, Andrei Gurtov, “5G Security: Analysis of Threats and Solutions,”. 2017 IEEE Conference on Standards for Communications and Networking (CSCN).

[5] Joanna Śliwa and Marek Suchański, “Security threats and countermeasures in military 5G systems”, Warsaw University of Technology MIKON-2022, Gdańsk, Poland

[6] Günther Horn, Peter Schneider, “Towards 5G Security”, 2015 IEEE Trustcom/BigDataSE/ISPA.

[7] W. Yang and C. Fung, “A Survey on Security in Network Functions Virtualization,” 2016 IEEE NetSoft Conf. and Wksps., June 2016, pp. 15–19.

[8] Sentas Global, The impact of quantum computing on cryptography

[9] P. W. Shor, "Algorithm for quantum computation: Discretelogarithm and factoring", Proc. 35th IEEE Annual Symp. On Foundations of Computer Science, pp. 24-134, November 1994

[10] Chandra Sourabh, Paira Smita, Alam Sk and Bhattacharyya Siddhartha, "A comparative survey of Symmetric and Asymmetric Key Cryptography", 2014 International Conference on Electronics Communication and Computational Engineering ICECCE 2014, 2014

[11] P. Kulkarni, R. Khanai, and G. Bindagi “Security Frameworks for Mobile Cloud Computing: A Survey,” 2016 Int’l. Conf. Electrical, Electronics, and Optimization Techniques, Mar. 2016, pp. 2507–11.

[12] L. Lydersen et al., "Hacking commercial quantum cryptography systems by tailored bright illumination", Nature Photon., vol. 4, no. 10, pp. 686- 689, 2010.