Horizon | Journal of Humanity and Artificial Intelligence

5G NETWORKS SECURITY TECHNIQUES AND ALGORITHMS

G'ulomov Sh. R., Sulaymonov A. A., Baymatova M. X.

Tashkent University of Information Technologies named after Muhammad al-Khwarizmi, Tashkent, Uzbekistan

---

Abstract

The development of 5G networks has brought about a new era of high-speed data transmission and connectivity, enabling us to communicate and interact with each other in ways that were previously impossible. However, with this increased connectivity comes an increased risk of cyber threats and security breaches. The security challenges associated with 5G networks are complex and require robust security techniques and algorithms to ensure the safety and privacy of users' data. This article explores the various security threats in 5G networks and discusses the different security techniques and algorithms that can be used to mitigate these threats. The article highlights the importance of developing effective security measures for 5G networks to ensure the protection of sensitive information and the continuity of services.

Keywords: 5G networks, models, algorithms, security techniques, cyber threats.

I. INTRODUCTION

The introduction of 5G networks has ushered in a new era of high-speed data transmission and connectivity, offering unprecedented levels of communication and interaction. However, the increased connectivity also brings with it an increased risk of cyber threats and security breaches. The security challenges associated with 5G networks are complex and require robust security techniques and algorithms to ensure the safety and privacy of users' data. This article explores the various security threats in 5G networks and discusses the different security techniques and algorithms that can be used to mitigate these threats. It emphasizes the importance of developing effective security measures for 5G networks to protect sensitive information and ensure service continuity. 5G has the potential to revolutionize various aspects of social and economic life, but its security issues must be addressed to ensure its safe and secure operation. Despite the highly sophisticated and robust security architecture and cryptographic algorithms designed for 5G networks, there are still potential security issues that need to be addressed, including those related to LTE protocol vulnerabilities. Table 1 summarizes some of the most relevant LTE protocol exploits that are still a potential threat in the 5G network.

***Table 1.* Major LTE protocol exploits, threats, and their impact on 5G**

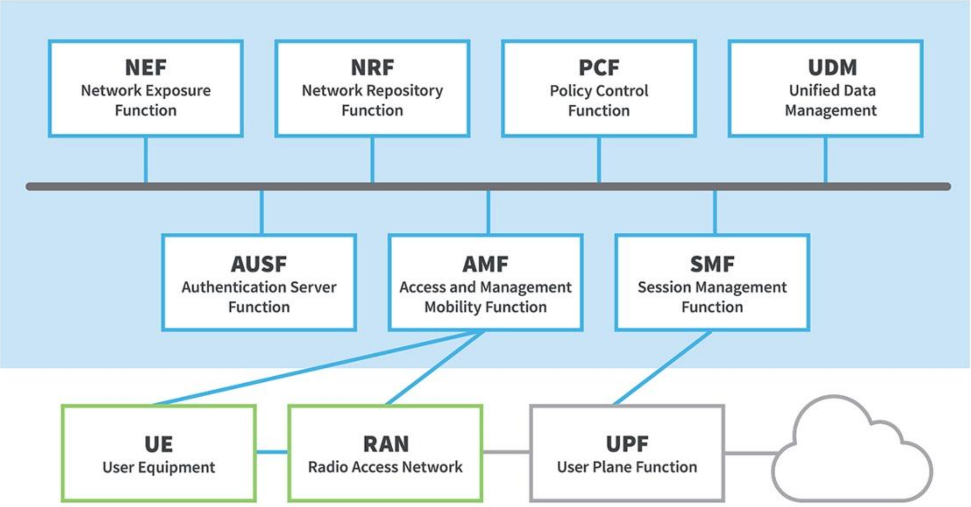
LTE protocol exploit	Threat	Impact on 5G
IMSI catching	Privacy threat, location leaks, SS7 leaks, etc. [1–6]	Potential for IMSI/SUPI catching in some protocol edge cases, such as when an unauthenticated emergency call is maliciously triggered
Device fingerprinting using exposed device capabilities	Identification attacks, bidding down attacks, and battery draining attacks [7]	Exploiting unprotected device capabilities' information identification attacks, bidding down attacks, and battery drain

		attacks against cellular devices
Location tracking	Location leaks [7]	Link device fingerprints to SUPI and track user's location
Silent downgrade to GSM	Man-in-the-middle attacks, SMS snooping, and phone call [2, 4, 6, 7]	Silent GSM downgrade using preauthentication messages from a malicious base station broadcasting a Mobile Country and Network Code (MCC-MNC) of a network with no public key provisioned in the USIM
Attach/Tracking Area Update (TAU) request	DoS [2, 4, 6]	DoS of 5G mobile devices caused by malicious base stations broadcasting a valid MCC-MNC combination for a network with no public key provisioned in the USIM
Wireless eavesdropping	avesdropping attacks [8]	Eavesdropping attacks exploit unsecured network communications to gain access to data as they are sent or received by their target

The use of null security algorithms (NEA0 and NIA0) in regular communication poses a security risk that has not been fully addressed in the LTE network. These algorithms are only intended for limited service mode and cannot provide encryption or integrity protection for control plane signaling messages in the NAS and AS layers. However, during a normal attach procedure, the core network selects null security algorithms, leaving control plane signaling messages vulnerable to exploitation by malicious attackers. This vulnerability arises from network misconfiguration and has been observed in twelve commercial LTE networks in Europe. While 5G offers more advanced security features, some of these features will still be configured by providers, leading to potential discrepancies between specified and configured security. It remains unclear whether this vulnerability persists in the 5G network as no studies have been conducted on this issue so far.

II. 5G Network Architecture.

5G was designed from the ground up, and network functions are split up by service. That is why this architecture is also called 5G core Service-Based Architecture (SBA). The following 5G network topology diagram shows the key components of a 5G core network:

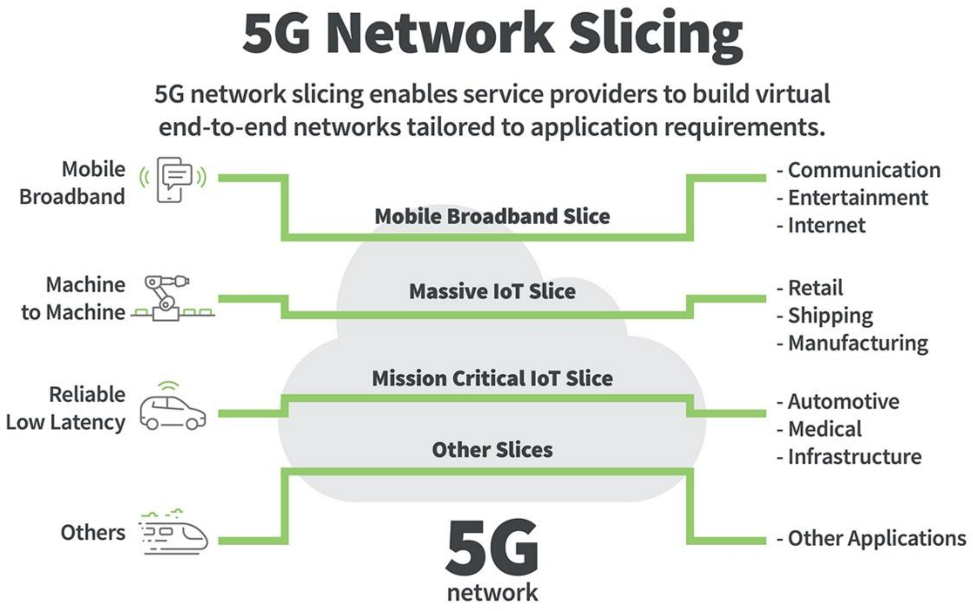

NEF
Network Exposure Function
NRF
Network Repository Function
PCF
Policy Control Function
UDM
Unified Data Management
AUSF
Authentication Server Function
AMF
Access and Management Mobility Function
SMF
Session Management Function
UE
User Equipment
RAN
Radio Access Network
UPF
User Plane Function

Picture.1

Here's how it works:

- User Equipment (UE) like 5G smartphones or 5G cellular devices connect over the 5G New Radio Access Network to the 5G core and further to Data Networks (DN), like the Internet.
- The Access and Mobility Management Function (AMF) acts as a single-entry point for the UE connection.
- Based on the service requested by the UE, the AMF selects the respective Session Management Function (SMF) for managing the user session.
- The User Plane Function (UPF) transports the IP data traffic (user plane) between the User Equipment (UE) and the external networks.
- The Authentication Server Function (AUSF) allows the AMF to authenticate the UE and access services of the 5G core.
- Other functions like the Session Management Function (SMF), the Policy Control Function (PCF), the Application Function (AF) and the Unified Data Management (UDM) function provide the policy control framework, applying policy decisions and accessing subscription information, to govern the network behavior.

As you can see, the 5G network architecture is more complex behind the scenes, but this complexity is needed to provide better service that can be tailored to the broad range of 5G use cases.

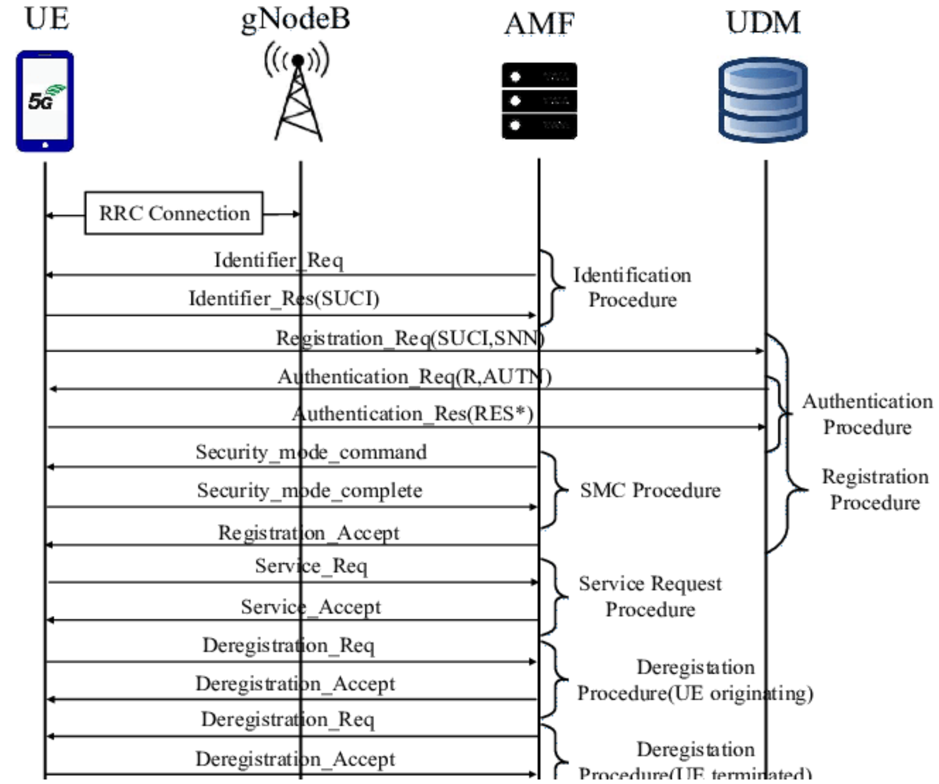

5G Network Slicing

5G network slicing enables service providers to build virtual end-to-end networks tailored to application requirements.

Picture.2

Attach Procedure with NAS Security and AS Security. User equipment **(**UE) management in 5G is split into two layers, nonaccess stratum (NAS) and access stratum (AS). The NAS protocol manages the connection between the UE and the core network, while the AS protocol manages the radio layer between the UE and gNB using the Radio Resource Control (RRC) protocol. NAS security ensures secure transmission of signaling between UE and AMF on the control plane, while AS security aims to securely deliver RRC messages and IP packets. The initial attach procedure involves the UE sending an Attach Request message with identifying information and supported security algorithms. Mutual authentication is established through an Authentication Request message containing a random nonce and authentication token. NAS security is enabled through the selection of ciphering and integrity algorithms, and AS security is initiated through the generation of an AS Security Mode Command message based on selected security algorithms. The network assigns an IP address with the Attach Accept message and contains UE Security Capabilities to initiate AS security. The gNB generates an AS

Security Mode Command message based on selected security algorithms, and the UE acknowledges with an AS Security Mode Complete message.



Picture.3-5G attach procedure with NAS security and AS security

According to the above analysis, we can see that the selection of security algorithm is significant for the security protection of the air interface signaling. 5G supports three ciphering and integrity protection algorithms, known as New radio Encryption Algorithm (NEA) and New radio Integrity Algorithm (NIA). NEA1 and NIA1 use the SNOW 3G cipher, NEA2 and NIA2 lean upon AES, and NEA3 and NIA3 rely on ZUA. The null algorithms NEA0 and NIA0 disable security, allowing data to be transmitted unprotected. They enable emergency calls to be made in the absence of a valid USIM and, as a result, a valid key. Integrity protection is crucial to ensure the authenticity of exchanged messages, and it continuously demonstrates that both parties have valid keys.

III. Conclusion.

This paper uses a systematic approach to analyze the security vulnerability of 5G by applying model checking principles. The authors create synchronous communication finite-state machines for UE and AMF, extract properties from 3GPP specifications, and construct an adversary model to test the system's security. By analyzing protocol behavior and observing state machine operations, they find that the null security algorithm (NEA0 and NIA0) used in normal communication poses a security threat in the 5G network, leading to IP spoofing and SUPI catching attacks. They also propose an anomaly detection method to prevent these attacks from occurring and analyze their root cause.

References

1. S. R. Hussain, M. Echeverria, O. Chowdhury, N. Li, and E. Bertino, “Privacy Attacks to the 4G and 5G Cellular Paging Protocols Using Side Channel Information,” in *Proceedings of the Network and Distributed Systems Security (NDSS) Symposium 2019*, San Diego, CA, USA, March 2019.
2. R. Piqueras Jover, V. Marojevic, and V. Marojevic, “Security and protocol exploit analysis of the 5G specifications,” *IEEE Access*, vol. 7, pp. 24956–24963, 2019.

3. A. Shaik, R. Borgaonkar, N. Asokan, V. Niemi, and J.-P. Seifert, "Practical attacks against privacy and availability in 4G/LTE mobile communication systems," in *Proceedings of the 23rd Annual Network Distribution System Security Symposium (NDSS)*, San Diego, CA, USA, January 2016.
4. S. Hussain, O. Chowdhury, S. Mehnaz, and E. Bertino, "LTEInspector: a systematic approach for adversarial testing of 4G LTE," in *Proceedings of the Network and Distributed Systems Security (NDSS) Symposium 2018*, San Diego, CA, USA, February 2018.
5. R. Borgaonkar, A. Shaik, N. Asokan, V. Niemi, and Jean, "LTE and IMSI catcher myths," Proc. of BlackHat Europe, 2015.
6. S. R. Hussain, M. Echeverria, I. Karim, O. Chowdhury, and E. Bertino, "5GReasoner: a property-directed security and privacy analysis framework for 5G cellular network protocol," in *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, London, November 2019.
7. A. Shaik, R. Borgaonkar, S. Part, and J.-P. Seifert, "New vulnerabilities in 4G and 5G cellular access network protocols: exposing device capabilities," in *Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks*, pp. 221–231, Miami, FL, USA, May 2019.
8. D. Fang, Y. Qian, and R. Q. Hu, "Security for 5G mobile wireless networks," *IEEE Access*, vol. 6, pp. 4850–4874, 2017.
9. Y. Xu, J. Liu, Y. Shen, X. Jiang, Y. Ji, and N. Shiratori, "QoS-aware secure routing design for wireless networks with selfish jammers," *IEEE Transactions on Wireless Communications*, vol. 20, 2021.