5G Network Security Risks and Countermeasures in Power Industry Applications

***Kamaldeep Kaur*[1]*, Sabhyata Uppal Soni*[2]*, Sarpreet Kaur*[3]**
[1]*Research Scholar, UIET, Panjab University, Chandigarh, India*
[2,3]*Assistant Professor, UIET, Panjab University, Chandigarh, India*

Abstract: Wireless communication systems have encountered security challenges since their inception. In the first-generation (1G) networks, mobile devices and wireless links were susceptible to illegal cloning and identity spoofing. Second-generation (2G) networks experienced a rise in message spamming, which facilitated large-scale attacks and the spread of misinformation and unwanted advertisements. Many of the security flaws in the fifth-generation (5G) networks originate from vulnerabilities inherited from LTE (Long-Term Evolution) systems, such as unauthorized data access, denial of service (DoS) attacks, data breaches, and audio surveillance. To address these issues, a variety of security enhancement methods have been proposed in recent years. This paper reviews several of these strategies, evaluating their effectiveness in mitigating threats based on defined assessment criteria.

Keywords: *Security Analysis, 5G, LTS, Software defined networks*

1. INTRODUCTION

The next generation of wireless communication networks have been greatly impacted by the huge expansion in communication traffic. In order to improve the performance of wireless communication, the 4G (the fourth generation of wireless mobile communication) utilized technologies including TD-SCDMA (Time Division Synchronous CDMA), OFDM (Orthogonal Frequency Division Multiplexing), and others. This strategy was successful. These technologies must be enhanced to be used with 5G due to the rapid expansion of mobile communication needs and user expectations. Three main usage scenarios—eMBB (improved Mobile Broadband), mMTC (massive Machine Type Communications), and URLLC (Ultra-reliable and Low Latency Communications) are anticipated to benefit from the 5G. Technologies like f-OFDM are being discussed widely as a means of meeting the needs of eMBB. IoT (Internet of Things), which includes smart electricity meters, street lighting, home gadgets, and security cameras, is one application of mMTC. Physical layer light weight authentication techniques could demonstrate their skills in mMTC. Self-driving cars, remote surgery, and industrial automation are some of URLLC's more notable offerings [1].

2. SECURITY OF 5G TECHNOLOGIES IN POWER SYSTEMS

The direction of mobile communication technology development is towards 5G technology. It is feasible to "wirelessly" control production control systems, such as power monitoring systems, thanks to their low latency and high reliability properties. Users in the power industry can establish specialized "business private network" services using 5G network slicing technologies to better fulfil the varied needs of power grid services. Acquisition, transmission, and on-site processing are strongly supported by 5G's large access capacity, high bandwidth, and edge computing abilities.

Newer and safer standards for communication encryption, access authentication, and other topics have been proposed by 5G. However, there continue to be lot of security concerns that have not been overcome in the application process for the power industry. While innovative network designs and key technologies like network slicing, core network sinking, mobile edge computing, and ultralow latency business bearers better enable a wide range of application scenarios, they also present new problems for the architecture of the power network security protection system in areas like edge computing, network access, business security, network management, and so forth.

3. ANALYSIS OF 5G REQUIREMENTS IN POWER SYSTEM APPLICATIONS

The power business primarily entails the generation, transmission, transformation, distribution, and usage of electricity from a consumption and production standpoint. Optical fibres coverage construction costs are currently high, and installation, operation, and maintenance are challenging due to wide-ranged power distribution stations. In scenarios requiring ubiquitous wide-area coverage and power usage, 5G networks are mostly deployed. The production control area, the information management area, and the Internet area are the three primary business kinds that the 5G power communication network focuses on from a business standpoint. Distribution differential protection, synchronous phasor measurement (PMU), intelligent distribution automation, power load demand side response, intelligent inspection, facility operation status monitoring, and other things are the primary components of the specific subdivision business [2]. Figure 1 depicts a hybrid networking design for 5G and the power communication network depending on the usual operations of the three main power grid areas.

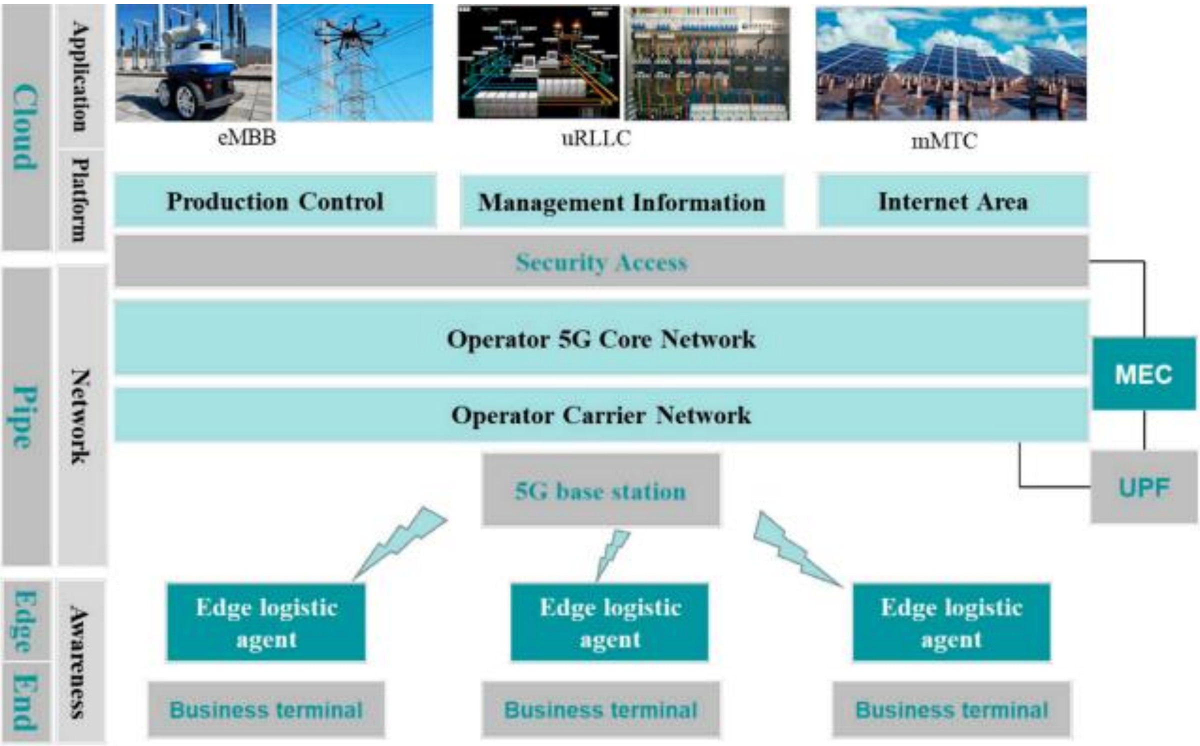

Figure 1: A hybrid networking architecture of 5G and power communication network.

- The hybrid networking framework of the 5G and electric power communication network consists of four layers: end, edge, pipe, and cloud. In this structure, the northbound interface connects terminal devices in the three "end" regions to the edge-layer IoT agent hardware. The IoT agent at the "edge" layer then communicates with the 5G base station through the wireless air interface. Certain power-related tasks in the "pipe" layer are either handled by the 5G edge-side User Plane Function (UPF) and terminated at the Multi-access Edge Computing (MEC) node, or pre-processed by the MEC and forwarded to the application systems in the "cloud" layer via a dedicated city-level line. Additionally, other "pipe" layer services transmit data to the "cloud" layer application systems through the power communication network supported by the 5G bearer network.The "end" and "edge" components of the original 4G network architecture are included in the perception layer, and some terminals explicitly allow 5G communication via transformation [3]. By incorporating 5G functionalities into the edge IoT agent, the original edge layer terminals can satisfy the access function necessities.
- The operator's network, commercially available MEC equipment, the production control area's dispatching data network, and the management information area's data communications infrastructure all make up the network layer, which is the "pipe" portion of the network infrastructure.
- The "cloud" portion of the network architecture, which includes the production control area, management information area, and Internet area, is made up of the platform layer and the application layer collectively. MEC hardware and network slicing are the key examples of how 5G contributes new technologies to the hybrid networking architecture in the "cloud-pipe-edge-end" system.

MEC/UPF is set up in two separate places depending on the type of business. One such component is the MEC/UPF installed in the core network, which is primarily in charge of processing impractical, low-bandwidth business in the management information area and Internet area. The second is the MEC/UPF, which is installed at the power grid plant and station side and is primarily in charge of processing high-bandwidth, low-latency, and high-reliability business in the production control zone and the management information zone.

4. SECURITY RISK ANALYSIS OF 5G NETWORKING IN POWER SYSTEMS

Terminal access risks, edge computing risks, network channel risks, and core network risks are the primary new security threats and difficulties posed by 5G. Below is a detailed analysis of the dangers introduced in the four sections:

i. Risks Associated with Terminal Access Caused by Various Business Scenarios: Threats like malicious software, firmware flaws, eavesdropping, and user data tampering are unavoidable when utilizing smart terminals. Additionally, the high concurrency, high throughput, and low latency 5G scenarios put forward various demands for the access authentication protocol. The desired outcomes of the three application scenarios cannot be fulfilled by merely utilizing a general access authentication protocol:

- The transmission rate is high and there is a greater concern for user privacy and sensitive data in the eMBB situation. Distinct businesses have different security needs within the same application context. As a result, when the terminal is accessed, a greater level of authentication and information integrity protection must be established, and simultaneously, a high-rate encryption capacity must be guaranteed [4].
- The number of terminals linked to the network in the mMTC situation is enormous, but their security capabilities are poor and their energy usage is constrained. A signaling storm could clog the network if the terminals keep using the conventional access mode. When an access attempt fails, the terminal repeatedly tries to connect to the network to start the authentication process, which increases battery usage. Because of this, the access authentication system in this case primarily has to be portable, effective, trustworthy, and affordable.
- Applications utilizing uRLLC have stricter requirements for latency and communication dependability. Nevertheless, improving the network security defense system would unavoidably result in decreased network productivity and effectiveness. A set of mechanism optimizations in each link of end-to-end transmission are necessary to achieve ultralow delay.

ii. Risks to Edge Computing from Business Traffic Offloading: Following are the two main risks caused by business traffic offloading

- **Risk Associated with UPF Traffic Offloading:** Once business traffic is offloaded through a local edge node, it becomes difficult to effectively monitor and control. If the UPF is improperly configured, traffic may be redirected to unintended MEC platforms. In such cases, an attacker could exploit the system by offloading large-scale computing tasks or initiating malicious transitions, overloading one or more MEC servers. This can lead to service timeouts for other users and exhaust the available computing resources.
- **Risk of MEC Data Offloading:** The business data processed by MEC applications is vulnerable to leakage due to the sensitive nature of data transmission and storage. Without proper encryption and integrity verification during the transfer of virtual machines or data between platforms, the likelihood of data being intercepted or tampered with by attackers increases. Additionally, the absence of hierarchical data classification, lack of desensitization measures, and unauthorized sharing with third parties further elevate the risk of confidential data theft during data exchange.

iii. **Network Slicing-Related Risks to Network Channels**: Following are the two network channel risks caused by networking slicing:

- The Threat of Network Slicing Attacks: In logically separated bearer network slices, overloading of one slice may result in anomalous operation of other virtual slices within the same physical network [5]. The assailant actively attacks other slices by using the controlled slice as a launchpad.
- The Risk of Network Slice Access: If an attacker gains access to a slice, they may deplete the resources of other slices, leaving them with insufficient resources. Other slices may be the target of DoS attacks. Cross-slice side-channel assaults can also be carried out by attackers.
- The Communication Risk Between Slices: Core network slices, RAN network slices, and other network slices all involve interactions. The interfaces between network slices are vulnerable to attack in any inter-network slice communications. A user plane attack can also corrupt or maliciously transfer user data, affecting single or maybe more UEs.

iv. Network Risks Caused by the Opening of the Network Capability: Following are the network risks caused by network capability opening:

- Information and data from the operator's closed platform are made available through network ability opening. Operators' skills to control and regulate data have been compromised, leaving them vulnerable to security concerns like data outflow and illegal access. Assailants can carry out denial-of-service attacks using the API made available by the open architecture for 5G networks.

- Cross-industry application development necessitates open sharing of corresponding data information, raising the possibility of data leakage. The network capacity opening increases the attack surfaces available to external adversaries, making it easier to manipulate the network setup and for inside assailants to do the same.
- When a security issue, like user data leakage, occurs during cross-industry data sharing, it will be hard to supervise data security since there will be a hazy separation of duties between the parties involved.
- The network capability opening interface uses the standard Internet protocol, which will expose the 5G network to additional security threats already present on the Web.

5. COUNTERMEASURES AGAINST SECURITY AND PRIVACY RISKS IN 5G APPLICATIONS

For developers and providers of 5G application services, the following specific security procedures are advised in various application situations.

i. **eMBB Scenario**: The lack of efficient monitoring tools and user privacy leaks are the key security issues in the eMBB scenario, and the following remedies are used [6]:

- Utilize edge computing nodes to deploy application traffic monitoring, and in some circumstances, assist the suspension of high-risk services.
- To verify the authenticity of the terminal and system identities and the legitimacy of the application, secondary identity authentication and authorization are performed between the terminal and the eMBB application service platform using the secondary authentication and key management mechanism. Encrypt and safeguard user data while also managing the service layer key between the two parties to stop hackers from listening in.
- The user plane of the 5G network can be protected by physical isolation or encryption in applications with high security needs to guarantee the security of user data transmission between network services.
- A secured data transmission channel is established via network slicing or a data reserved line between the operator's 5G core network and the eMBB application service platform to guarantee the security of user business data communication.

ii. **uRLLC Scenario**: The DDoS attack and the data security risk are the two key security threats in the uRLLC scenario, and the accompanying solutions are discussed below:

- To stop phoney users from connecting, set up a two-way identity authentication method between the user terminal and the application server.
- Use anti-DDoS tools to guard against network clogging, wireless interference, and broken communication links.
- Using the security tools implemented in edge computing, along with data integrity protection, timestamp, serial number, and other techniques, to guard against tampering with, falsifying, or replaying application data and guarantee the accuracy of data transmission [7].

iii. **mMTC Scenario:** In the massive Machine-Type Communication (mMTC) environment, major security threats include counterfeit devices, data tampering, eavesdropping, and unauthorized remote control. The following countermeasures are recommended:

- **Establish two-way authentication** between IoT devices and the network using lightweight encryption algorithms and streamlined security protocols to ensure only trusted devices gain access.
- **Protect the integrity and confidentiality** of sensitive data generated by IoT terminals by encrypting it, preventing attackers from intercepting, modifying, forging, or replaying critical information during transmission.
- **Deploy security monitoring mechanisms** to quickly detect and prevent the misuse of large-scale IoT devices. This helps mitigate potential threats such as Distributed Denial of Service (DDoS) attacks targeting air interfaces or service platforms, which could lead to network congestion and service disruption in mMTC environments.

6. CONCLUSIONS AND FUTURE SCOPE

The solution can be provided to the problems which are mobility management and secure channel establishment from source to destination. In the past time various techniques are designed which provide solution to mobility management and security issue. This research is to improve handoff mechanism and increase security of the network.

1. Mobility Management Problem

The 5G network is the most advanced network which needs to deal with high mobility due to which handoff is the major concern to maintain quality of service. In the existing technique proxy models is applied to handle mobility management which leads to hard handoff in the network. In this research, the technique of angle of trajectory will be applied which leads to soft handoff in the network.

2. **Secure Channel Establishment**

The 5G network is type of network which needs to deal with active and passive attacks. The secure channel establishment is the technique which provides end-to-end encryption to the data which is transmitted over the secure channel. The authentication algorithms are the complex algorithm which provides end-to-end authentications. This research elliptic curve cryptography technique is implemented which is secure and less complex.

1. The schemes which are already designed for the secure handoff are unable to make hard handoff efficiently which affect network performance.

2. The authentication mechanism needs to propose so that less information needs to be exchanged at the time of handoff.

3. The data transmission in the 5g network needs to be secure so that security attacks needs to be reduced which directly increase network performance in terms of latency.

7. REFERENCES

[1] J. Cao *et al.*, "A Survey on Security Aspects for 3GPP 5G Networks," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 1, pp. 170–195, Firstquarter 2020.

[2] S. Park, S. Kwon, Y. Park, D. Kim, and I. You, "Session Management for Security Systems in 5G Standalone Network," *IEEE Access*, vol. 10, pp. 73421–73436, 2022.

[3] P. Wright *et al.*, "5G network slicing with QKD and quantum-safe security," *Journal of Optical Communications and Networking*, vol. 13, no. 3, pp. 33–40.

[4] Q. Tang, O. Ermis, C. D. Nguyen, A. D. Oliveira, and A. Hirtzig, "A Systematic Analysis of 5G Networks with a Focus on 5G Core Security," *IEEE Access*, vol. 10, pp. 18298–18319, 2022.

[5] K. Saleem *et al.*, "Bio-Inspired Network Security for 5G-Enabled IoT Applications," *IEEE Access*, vol. 8, pp. 229152–229160, 2020.

[6] Y. Wu *et al.*, "A Survey of Physical Layer Security Techniques for 5G Wireless Networks and Challenges Ahead," *IEEE Journal on Selected Areas in Communications*, vol. 36, no. 4, pp. 679–695, Apr. 2018.

[7] G. Arfaoui *et al.*, "A Security Architecture for 5G Networks," *IEEE Access*, vol. 6, pp. 22466–22479, 2018.

[8] Z. Zou, T. Chen, J. Chen, Y. Hou, and R. Yang, "Research on Network Security Risk and Security Countermeasures of 5G Technology in Power System Application," *Proc. 2021 IEEE 5th Advanced Information Technology, Electronic and Automation Control Conference (IAEAC)*, pp. 102–105, 2021.

[9] L. Zhijie, "Research on communication security of power system based on 5G Technology," *Proc. 2021 IEEE International Conference on Data Science and Computer Application (ICDSCA)*, pp. 866–871, 2021.

[10] Y. Jiang, Y. Cong, and A. Hu, "Power 5G Hybrid Networking and Security Risk Analysis," *Frontiers in Energy Research*, vol. 12, Feb. 2022.

[11] B. Li *et al.*, "Technical System and Top-Level Frame Design for Energy Internet-Oriented Integrated 5G Power Communication Network," *Proc. 2021 IEEE 5th Information Technology, Networking, Electronic and Automation Control Conference (ITNEC)*, pp. 1434–1437, 2021.

[12] Y. Zou *et al.*, "Electric Load Profile of 5G Base Station in Distribution Systems Based on Data Flow Analysis," *IEEE Transactions on Smart Grid*, vol. 13, no. 3, pp. 2452–2466, May 2022.

[13] L. Guo, C. Ye, Y. Ding, and P. Wang, "Allocation of Centrally Switched Fault Current Limiters Enabled by 5G in Transmission System," *IEEE Transactions on Power Delivery*, vol. 36, no. 5, pp. 3231–3241, Oct. 2021.

[14] J. M. Hamamreh, Z. E. Ankarali, and H. Arslan, "CP-Less OFDM With Alignment Signals for Enhancing Spectral Efficiency, Reducing Latency, and Improving PHY Security of 5G Services," *IEEE Access*, vol. 6, pp. 63649–63663, 2018.

[15] Z. Ai, Y. Liu, F. Song, and H. Zhang, "A Smart Collaborative Charging Algorithm for Mobile Power Distribution in 5G Networks," *IEEE Access*, vol. 6, pp. 28668–28679, 2018.

[16] C. Zhang, J. Ge, J. Li, F. Gong, and H. Ding, "Complexity-Aware Relay Selection for 5G Large-Scale Secure Two-Way Relay Systems," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 6, pp. 5461–5465, Jun. 2017.

[17] I. H. Abdulqadder, D. Zou, I. T. Aziz, B. Yuan, and W. Dai, "Deployment of Robust Security Scheme in SDN Based 5G Network over NFV Enabled Cloud Environment," *IEEE Transactions on Emerging Topics in Computing*, vol. 9, no. 2, pp. 866–877, Apr.–Jun. 2021.

[18] S. Ahmadzadeh, G. Parr, and W. Zhao, "A Review on Communication Aspects of Demand Response Management for Future 5G IoT-Based Smart Grids," *IEEE Access*, vol. 9, pp. 77555–77571, 2021.

[19] X. Ma, Y. Duan, and S. Zhu, "Optimal configuration for photovoltaic storage system capacity in 5G base station microgrids," *Global Energy Interconnection*, vol. 10, no. 7, pp. 29731–29740, Oct. 2021.

[20] Y. Zhang, J. Li, and Y. Tian, "Privacy-preserving communication and power injection over vehicle networks and 5G smart grid slice," *Journal of Network and Computer Applications*, vol. 7, no. 31, pp. 12–19, Aug. 2018.

[21] M. Humayun *et al.*, "Privacy Protection and Energy Optimization for 5G-Aided Industrial Internet of Things," *IEEE Access*, vol. 8, pp. 183665–183677, 2020.

[22] X. Zhang, J. Fei, H. Jiang, and X. Huang, "Research on Power 5G Business Security Architecture and Protection Technologies," *Proc. 2021 6th International Conference on Power and Renewable Energy (ICPRE)*, pp. 913–917, 2021.

[23] T. A. Zerihun, M. Garau, and B. E. Helvik, "Effect of Communication Failures on State Estimation of 5G-Enabled Smart Grid," *IEEE Access*, vol. 8, pp. 112642–112658, 2020.

[24] X. Ma, Q. Zhu, and Z. Wang, "Optimal configuration of 5G base station energy storage considering sleep mechanism," *Global Energy Interconnection*, vol. 1, no. 9, pp. 611–619, Feb. 2022.

[25] B. D. Deebak and F. Al-Turjman, "A robust and distributed architecture for 5G-enabled networks in the smart blockchain era," *Computer Communications*, vol. 9, no. 4, pp. 469–473, Oct. 2021.

[26] C. R. Kumar J., A. Almasarani, and M. A. Majid, "5G-Wireless Sensor Networks for Smart Grid—Accelerating technology's progress and innovation in the Kingdom of Saudi Arabia," *Procedia Computer Science*, vol. 5, no. 13, pp. 9887–9896, Mar. 2021.