Journal of IoT in Social, Mobile, Analytics, and Cloud (ISSN: 2582-1369)
www.irojournals.com/iroismac/

# Recent Security Features of 5G Protocol for Real Time Network Domain – An Overview

**S. Smys**

Professor, Department of Electrical and Electronics Engineering, RVS College of Engineering and Technology, Coimbatore, India

**E-mail:** smys375@gmail.com

## Abstract

Numerous mission-critical applications in the field of information technology will rely on fifth generation (5G) networks in the future. The 5G is projected to bring new technological improvements and innovation. Software-Defined Networking (SDN) is the present backbone of 5G. Because of the specific needs of each application that may be met by network slicing, 5G can provide this feature. In comparison to 4G Long-Term Evolution (LTE) and preceded generations, 5G is more adaptable and scalable. However, considerable advances in 5G cyber security are required to minimise the rising threats of hacking. Both the network and the devices linked to 5G are subjected to security problems. 5G communication networks' weaknesses may create many dangerous unknown attacks. However, it depends on the 5G privacy and security key protocol. In addition, several dangerous attacks may be combined to provide a wide range of attack options for hackers. For the 5G communication network, this article provides a complete framework for security analysis. The findings of this study might lead to unique 5G communication exploits. Moreover, artificial intelligence learning has been recently used to create and analyse attack graphs for software-defined and virtualized 5G communication networks.

**Keywords:** 5G edge securities, vulnerability analysis, 5G security, mobile network security, IoT, smart agriculture, agriculture robots

## 1. Introduction

In comparison to 4G LTE networks, 5G wireless networks are faster, have reduced latency, and have more capacity. From distant learning to mobile workforces, they utilise


*DOI: https://doi.org/10.36548/jismac.2021.4.003*
*Received: 06.02.2022, received in revised form: 19.03.2022, accepted: 02.04.2022, published: 12.04.2022*

dynamic spectrum sharing. The disaster reply to the wide area networks for next level attack through many entertainment channels, game application and others are nearly unlimited. With the help of 5G, services such as drone deliveries and cloud-based traffic management might realise their promise. A wider variety of radio frequencies are possible, allowing carriers to enhance their network capabilities in the ultra-high millimetre-wave bands [1 -5].

The 5G is a major shift in telecommunications, bringing new connections, capabilities and services to the table. Advancements in connectivity will open up a broad range of new markets and economic opportunities for businesses throughout the globe. It is important to keep in mind that these changes pose substantial threats to national and financial security, as well as to other global interests [6-8]. For this reason, criminal and foreign opponents will perceive 5G networks as a great source of valuable information and intelligence. Figure 1 shows threat profile evaluation.

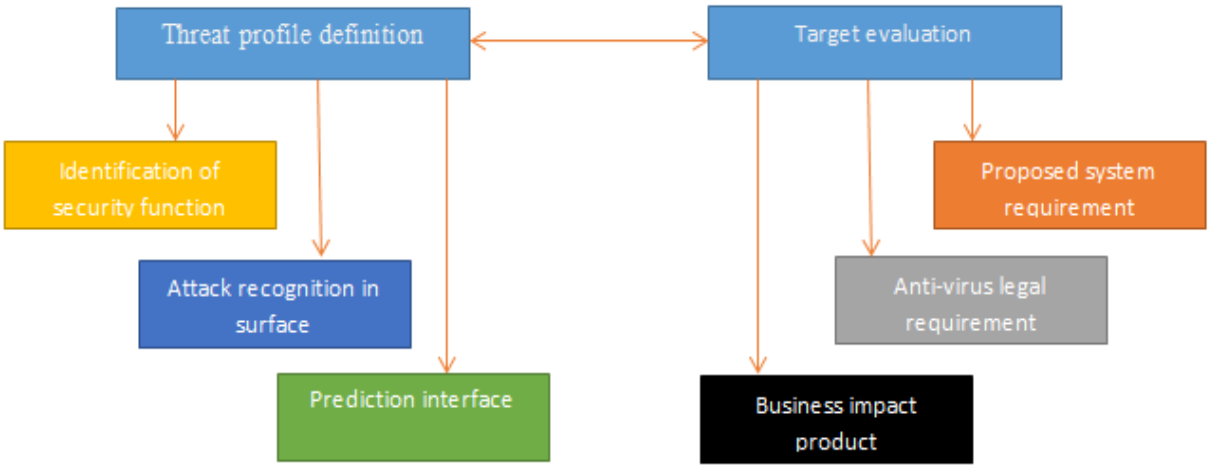


**Figure 1.** Threat profile evaluation

There are many advantages and benefits to moving to the 5G network, but it also brings new risks and challenges. An early list of dangers across the 5G domains has been established by the Working Panel on 5G Threat Models. In addition to the three main dangers, there are other sub-threats that may be exploited by criminals. Even if these risks aren't comprehensive, they may impede the developed world's move to 5G.

As a result, unlike previous generations of cellular networks, 5G networks need complicated security systems. Several threats based on entertainment channels and gaming application networks, were not taken into consideration in the design of prior cellular network

generations. 5G has a lot of new features that haven't been seen before. There is a shared mobile network for multi-tenancy and virtualization infrastructure [9-12].

In terms of speed, protocols, and network settings, 5G mobile communication is superior to 4G mobile communications. Because it is 20 times faster than the current LTE, the 5G wireless network is set up as a soft-defined network with a 20 Gbps speed, while the 5G core network is now decentralised to reduce traffic transmission latency [13, 14].

### 1.1 Motivation

A new set of trust models emerge as a consequence of the decrease in face-to-face engagement. In the 5G standard, privacy issues that were previously unaddressed in 4G, have been addressed. Unlike previous generations of standards, academics are already concerned about the security of the 5G system before the standard is widely deployed. The recent security protocols have been examined in a formal manner, revealing flaws that may now be addressed before 5G equipment is implemented.

### 1.2 Statement of the issue

All standard characteristics, not only the radio interface, are included in this study, which is a standalone scenario that also includes the 5G core network architecture. To further understand the 5G architecture, the security policies that are compatible with it are considered. After that, the different use cases and the security measures connected with their implementation are examined in further depth. Finally, some of the assumptions stated in this paper are verified and how 5G-compliant devices and networks implement recent security measures are evaluated.

## 2. Organization of the Research

It is separated into parts that summarizes 5G security studies, with Section 3 including the most current research on 5G security. Section 4 explores several threat assessment approaches in further detail. Section 5 discusses the conclusion, as well as possible future enhancements.

## 3. Recent Works

### 3.1 Artificial Intelligent approach

Analysis of LTE and 5G technologies' cyber security vulnerabilities utilising the Support Vector Machine (SVM) was proposed by Park et al. [15]. There are four categories that the technique categorised assaults under:

1. DDoS (Distributed Denial of Service),
2. Man-in-the-middle,
3. Phishing,
4. Bogus data injection.

Security difficulties in the real 5G local network were revealed by Holtrup et al., [16] who also offered mitigating measures. An attack tree and 15 test cases were also created by the researchers, and they discovered eight basic weaknesses in the system.

### 3.2 Standard security context

A risk matrix was developed by Sullivan et al., [17] using the recent threat categorization model, which took into account the possibility and effect of 12 different attack scenarios on radio access and the network's core. The Open Systems Interconnection (OSI) concept was used to arrange security technology into layers. Security solutions, gaps and outstanding research topics were discussed for each layer in detail by the authors [18, 19].

New control-aware attack analytics were developed in [20], to secure IoT-based 5G networks. They also revealed new methods for assessing and detecting threats to 5G core networks' vulnerabilities and attacks. They also looked at the specific vulnerabilities in the SDN, *Network* Functions Virtualization (NFV), and Radio Access Network (RAN) components of the 5G network. Finally, they devised novel security issues discussions and its direction analysis approaches based on artificial intelligent method.

## 4. Recent 5G Threats and Security

Defining what constitutes a threat in the context of information security may be a difficult task. The threat agent's capacity to carry out a successful assault, as well as the threat agent's motive, determines the chance of a risk event. The attacking categorization of threats will be used as the basis for the technique. The threat analysis approach necessitates the formalisation of data amongst various components [21]. To describe and categorise computer

security risks, Microsoft has created many approaches. The purpose of the attacker is used to determine the nature of a threat:

1. User or device identity faking
2. Tampering
3. Repudiation
4. Publication of relevant data
5. Non-performance of an essential function
6. Privilege being elevated.

It's important to understand the danger categories that are relevant to each of the many parts of a system. There are threats of new classified features as follows.

### 4.1 New security features in 5G compared to 4G

Some new security elements have been incorporated in 5G standalone implementations in order to prevent previously discovered vulnerabilities. Despite this, most of the security protections that were previously in place in 4G remain in place [22-25].

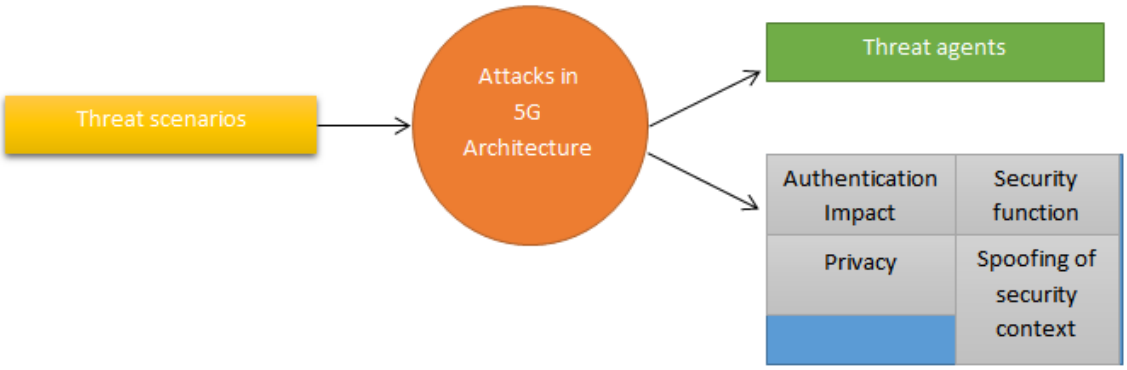


**Figure 2.** Attacks handling in 5G architecture

New 3GPP standards include the home network's public key, which is used for elliptic curve algorithms in U-SIM, in contrast to prior standards. It is possible for transaction between the sensitive data in the networks without first negotiating a key with that network when using (limited) asymmetric cryptographic techniques. As the exposed International

Mobile Subscriber Identity (IMSI) in the first attach request is replaced by initial registration request, past IMSI catcher attacks are avoided. In a similar way, other permanent identifiers enable to immediately link one person to another. Threat scenarios are scheduled in various agents through security parameters that are shown in figure 2.

### 4.2 Standard context

If the User Equipment (UE) and the network have formed a security context, then the messages can only be protected either in integrity or in confidentiality. As a result, earlier assaults on the attach request/attach reject process are still applicable to the analogous registration request/registration reject of the method. But it should be noted that rejecting is no longer allowed throughout the 5G registration process [24]. Even though 5G is not flawless, if the operator follows all 3GPP standards, it is more secure against IMSI catchers than prior protocols.

### 4.3 Spoofing of a device

The radio interface of a given parameter might be used by an attacker to launch an attack on the network. In contrast, the long-term UE key is kept in the USIM container, which is situated in a local real time network. This part is subjected to strict security standards designed to ensure that even a determined and competent attacker utilising sophisticated hardware assaults would be unable to retrieve a key. Keys are not required in the first phases of network registration, but they are required later on. The risk identification procedure is mentioned and shown in figure 3.

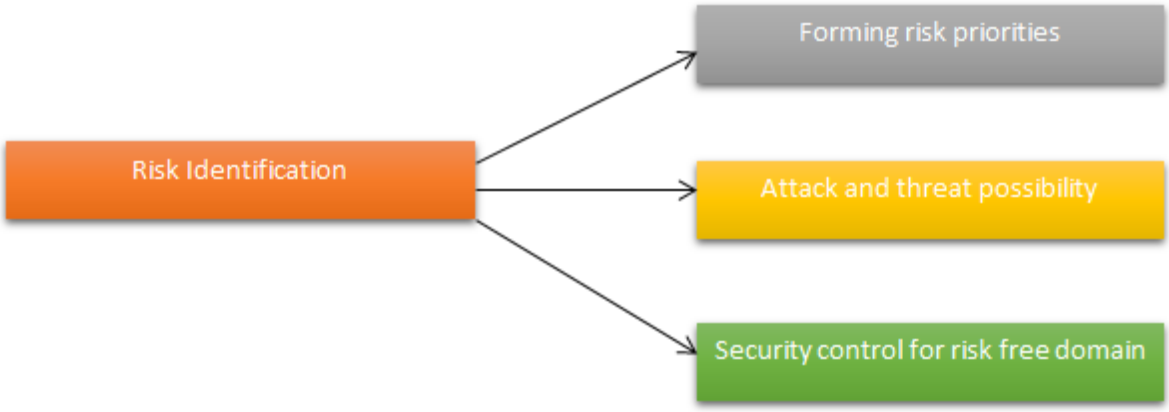


**Figure 3.** Risk identification procedures in 5G domain

### 4.4 Spoofing of a security edge protection proxy

To authenticate requests from a roaming network, the home network holds long-term keys and does so at the Security Edge Protection Proxy (SEPP) level. Because of this, the two SEPPs will be able to verify one another. SEPPs are anticipated to carry all control plane data between the server and the network at home, as is the case for all other network traffic. Additionally, it stipulates that communication between the SEPPs should be secured using Transport Layer Security (TLS). The spoofed network can imitate only one network, which is why the serving network name is included in the first authentication request from a UE to the home network. Aside from that, the SEPP of the home network should be able to verify that both the SEPP certificate and the network name acquired in separate operations are consistent with each other [26].

### 4.5 Spoofing of a security context

According to the enhanced paradigm of trust, many additional security measures guarantee that subscriber and network interactions are verifiable and authenticated:

#### 4.5.1 Interoperability protection

Multiple security risks in 2G, 3G, and 4G networks have been discovered as a result of flaws in the diameter protocols' underlying architecture. 6–8 security proxy servers, which are basically an extension of the signaling firewalls of 2G, 3G, and 4G, will enable inter-operator security in 5G.

#### 4.5.2 Privacy

In 5G networks, the public key of the home network will be utilized for asymmetric encryption to prevent the leakage of subscriber identification. In order to verify a user's identity, 5G networks and devices authenticate each other.

#### 4.5.3 Authentication

Authentication for data transmissions in various routers through Wi-Fi communication is required.

### 4.5.4 Fundamental Hierarchy

5G utilizes crucial separation in order to execute the revised concept of trust. Data communicated by a user is protected against tampering by this method, which reduces the impact of an attack on infrastructure.

### 4.5.5 The safety of the radio network

At the architectural level, the 5G base station separates the data handling units (Central Unit) from the radio module (Distributed Unit). A secure interface connects the central unit and distributed unit together and allows them to communicate. Even if the intruder process to obtain the central and distributed unit, the network will remain safe because of this isolation. As 5G networks are supposed to be more secure than previous generation networks, several modifications have been implemented. In 5G, known security vulnerabilities in large diameter signaling networks have been addressed. However, this does not rule out the possibility of 5G networks being breached [25]. There are 5G's possible security risks now. The 5G networks become more tempting targets when they're used in new contexts, such as remote surgery, self-driving automobiles, and automated manufacturing.

## 4.6 Communication security

An act of security is an ongoing activity, and not a one-time process. Despite extensive work on 5G security at the standard level, there are still major unknowns. 5G networks must be protected by operators constantly studying and implementing the 3GPP and Group Special Mobile Association (GSMA) guidelines. It is necessary to adopt recommendations with care. However, each network has its own distinct characteristics [26]. Changes in security rules must be a part of an entire process, regardless of whether they are based on suggestions, audits, or monitoring. Before and after installation, testing must be carried out. As a result, 5G security isn't simply about having top-notch architecture or cutting-edge security technology. It necessitates the development of processes, procedures, and cross-team communication.

## 5. Conclusion

The security threats associated with mobile networks have been steadily decreased with each subsequent iteration in the construction of the 5G network architecture. Despite

this, a new type of threat in the 5G domain is based on common local networks and, in many cases, poses significant dangers for network providers. The security of 5G networks will require significant effort on the part of telecom suppliers and operators, despite the fact that many elements are already in place. This is due to the fact that they are responsible for ensuring that standards are implemented and operators adhere to suggestions. The self-sustained networks consist of automatic response systems and intrusion response systems to assess the vulnerability. Recent threats will be employed in future work to deploy countermeasures against cyber-attacks using the vulnerability analysis approach. They also utilize the model in conjunction with the safest network domain to identify the local response by its own autonomous assessment or response system/procedure that is under recent attacks in 5G dynamic architecture.

## References

[1] Park, S.; Kim, S.; Son, K.; Kim, H. Security threats and countermeasure frame using a session control mechanism on volte. In Proceedings of the 2015 10th International Conference on Broadband andWireless Computing, Communication and Applications (BWCCA), Krakow, Poland, 4–6 November 2015; pp. 532–537.

[2] Makris, N.; Zarafetas, C.; Valantasis, A.; Korakis, T. Service Orchestratidoion OverWireless Network Slices: Testbed Setup and Integration. IEEE Trans. Netw. Serv. Manag. 2021, 18, 482–497.

[3] Kholidy, H.A.; Karam, A.; Sidoran, J.L.; Rahman, M.A. 5G Core Security in Edge Networks: A Vulnerability Assessment Approach. In Proceedings of the 26th IEEE Symposium on Computers and Communications (ISCC), Athens, Greece, 5–8 September 2021;pp. 1–6.

[4] Rodrigo, R.; Javier Lopez, M.M. Mobile edge computing, Fog et al.: A survey and analysis of security threats and challenges. Future Gener. Comput. Syst. 2018, 78, 680–698.

[5] Ghosh, A.; Ghorui, N.; Mondal, S.P.; Kumari, S.; Mondal, B.K.; Das, A.; Gupta, M.S. Application of Hexagonal Fuzzy MCDM Methodology for Site Selection of Electric Vehicle Charging Station. Mathematics 2021, 9, 393.

[6] Fan, Z.; Xiao, Y.; Nayak, A.; Tan, C. An improved network security situation assessment approach in software defined networks. Peer-to-Peer Netw. Appl. 2019, 12, 295–309.

[7] Kholidy, H.A. Towards A Scalable Symmetric Key Cryptographic Scheme: Performance Evaluation and Security Analysis. In Proceedings of the 2019 2nd International Conference on Computer Applications & Information Security (ICCAIS), Riyadh, Saudi Arabia, 1–3 May 2019; IEEE: Piscataway Township, NJ, USA, 2019.

[8] Khan, R.; Kumar, P.; Jayakody, D.N.K.; Liyanage, M. A survey on security and privacy of 5g technologies: Potential solutions, recent advancements and future directions. IEEE Commun. Surv. Tutor. 2019, 22, 196–248.

[9] Kholidy, H.A. Detecting impersonation attacks in cloud computing environments using a centric user profiling approach. Gener. Comput. Syst. 2021, 117, 299–320.

[10] Abdulqadder, I.; Zou, D.; Aziz, I.; Yuan, B.; Dai, W. Deployment of robust security scheme in sdn based 5g network over nfv enabled cloud environment. IEEE Trans. Emerg. Top. Comput. 2018, 9, 866–877.

[11] Kholidy, H.A. Correlation-based sequence alignment models for detecting masquerades in cloud computing. IET Inf. Secur. 2020, 14, 39–50.

[12] Tian, Z.; Sun, Y.; Su, S.; Li, M.; Du, X.; Guizani, M. Automated attack and defense framework for 5g security on physical and logical layers. arXiv 2019, arXiv:1902.04009.

[13] Kholidy, H.A.; Baiardi, F.; Hariri, S. DDSGA: A Data-Driven Semi-Global Alignment Approach for Detecting Masquerade Attacks. IEEE Trans. Depend. Sec. Comput. 2015, 12, 164–178.

[14] Luo, S.; Wu, J.; Li, J.; Guo, L.; Pei, B. Toward Vulnerability Assessment for 5G Mobile Communication Networks. In Proceedings of the 2015 IEEE International Conference on Smart City/SocialCom/SustainCom (SmartCity), Chengdu, China, 19–21 December 2015; pp. 72–76.

[15] Park, S.; Kim, D.; Park, Y.; Cho, H.; Kim, D.; Kwon, S. 5G Security Threat Assessment in Real Networks. Sensors 2021, 21, 5524.

[16] Holtrup, G.; Lacube, W.; David, D.P.; Mermoud, A.; Bovet, G.; Lenders, V. 5G System Security Analysis. arXiv 2021, arXiv:2108.08700.

[17] Sullivan, S.; Brighente, A.; Kumar, S.A.P. 5G Security Challenges and Solutions: A Review by SI Layers. IEEE Access 2021, 9, 116294–116314.

[18] Li,W; Wang, N.; Jiao, L.; Zang, K. Physical Layer Spoofing Attack Detection in MmWave Massive MIMO 5G Networks. IEEE Access 2021, 9, 60419–60432.

[19] Singh, R.; Kumar, H.; Singla, R.K. TOPSIS Based Multi-Criteria Decision Making of Feature Selection Techniques for Network Traffic Dataset. Int. J. Eng. Technol. 2013, 5, 4598–4604.

[20] Haque, N.; Rahman, M.; Chen, D.; Kholidy, H. BIoTA: Control-Aware Attack Analytics for Building Internet of Things. In Proceedings of the 18th IEEE International Conference on Sensing, Communication and Networking (SECON), Rome, Italy, 6–9 July 2021.

[21] Park, S.; Cho, H.; Park, Y.; Choi, B.; Kim, D.; Yim, K. Security Problems of 5G Voice Communication. In Information Security Applications; You, I., Ed.; WISA: Jeju Island, Korea, 2020.

[22] Fernandez, J.-M.; Vidal, I.; Valera, F. Enabling the Orchestration of IoT Slices through Edge and Cloud Microservice Platforms. Sensors 2019, 19, 2980.

[23] Batalla, J.M.; Andrukiewicz, E.; Gomez, G.P.; Sapiecha, P.; Mavromoustakis, C.X.; Mastorakis, G.; Zurek, J.; Imran, M. Security Risk Assessment for 5G Networks: National Perspective. IEEE Wirel. Commun. 2020, 27, 16–22.

[24] Haque, N.; Rahman, M.; Chen, D.; Kholidy, H. BIoTA: Control-Aware Attack Analytics for Building Internet of Things. In Proceedings of the 18th IEEE International Conference on Sensing, Communication and Networking (SECON), Rome, Italy, 6–9 July 2021.

[25] Khan, J.A.; Chowdhury, M.M. Security Analysis of 5G Network. In Proceedings of the 2021 IEEE International Conference on Electro Information Technology (EIT), Mt. Pleasant, MI, USA, 14–15 May 2021.

[26] Subedi, P.; Alsadoon, A.; Prasad, P.W.C.; Rehman, S.; Giweli, N.; Imran, M.; Arif, S. Network slicing: A next generation 5G perspective. J. Wirel. Commun. Netw. 2021, 2021, 102.

## Author's biography

**S. Smys** received his M.E. and Ph.D. degrees in Wireless Communication and Networking from Anna University and Karunya University, India. His main area of research activity is localization and routing architecture in wireless networks. He serves as Associate Editor of Computers and Electrical Engineering (C&EE) Journal, Elsevier, and Guest Editor of MONET Journal, Springer. He served as Reviewer for IET, Springer, Inderscience and Elsevier journals. He has published many research articles in refereed journals and IEEE

conferences. He has been General chair, Session Chair, TPC Chair and Panelist in several conferences. He is Member of IEEE and Senior Member of IACSIT wireless research group. He has been serving as Organizing Chair and Program Chair of several International conferences and in the Program Committees of several International conferences. Currently, he is working as Professor in the Department of Information Technology at RVS technical Campus, Coimbatore, India.