5G Security Threats and Recommendations

Abdullah Bajahzar,

Majmaah University, College of Science at Zulfi, Department of Computer Science and Information, Zulfi 11932, Saudi Arabia

Summary
Security is the foundation for successful delivery of 5G networks in a variety of vertical industries. 5G (Next Generation Network) will use the novel mechanical concept to meet the full range of broadband access, high customers and different usage tools and a huge network of devices (such as the Internet of Things) in an ultra-reliable and sensible way. Software Definition Network (SDN) and Network Function Virtualization (NFV) take advantage of advances in distributed computing, such as, Mobile Edge Computing (MEC) is the most search progress to meet these needs. Still, it is a new issue to safely take advantage of these advances and provide protection to customers' in future remote systems. In these respects, this paper outlines the security challenges of cloud, SDN, and NFV, as well as the difficulties of customer protection. This paper describes the answers to these difficulties and future directions for the secure 5G systems. It aims to explain why security is the foundation of 5G, and the differences between 5G and 2G, 3G, 4G in form of security in terms of demand, threat prospects and solutions.

Key words:
5G, SDN, IoT, NFV, MEC

1. Introduction

5G is an end-to-end ecosystem that enables a fully mobile and connected society, which gives fully portable and relevant society create self-esteem for customers and accomplices through existing and developing use cases, communicate with predictable experience and enable actual action plans.

According to the 5th Generation Public-Private Partnership (5G-PPP), 5G will associate approximately 7 trillion remote devices or things, reducing the age benefit creation time from 90 hours to one and a half hours, and giving privacy to push client control. .By relates to all aspects of life, 5G is suitable for computerized society that needs high management interest and security with different technical arrangements [1]. In this way, through the flexible system activities and management, search for distributed computing, SDN and NFV ideas to meet development customers and management within the limits of capital consumption and operating costs request.

In the 5G business environment, security is an important factor affecting business development. Customers understand security and Protection is necessary and they can understand the protection benefits given to them. The degree of trust and in any case, the quality of the security components gives a clear level of security, which in any case exceeds the long-term security level. Admit that almost determined by trust, so negative changes may occur quickly. In order to increase recognized safety, it is important to ensure that safety and protection includes that exist in prior ages are additionally present [2].

A method of measuring personal life has emerged on the Internet. Individual is expanding measures to regularly collect and send personal and financial related information using mobile phones and mobile phones system. Cybercrime is growing rapidly and is affected and worried by many individuals. It is vital to remember the inevitable vertical arrangement of different industries that 5G must have strengthened [2]. These provide a wide range of business drivers for security, such as: vertical vehicle requirements Unwavering quality, honesty and accessibility to avoid deaths. Social insurance also needs Unwavering quality and will emphasize confidentiality. Smart city applications will include the ever-increasing amount of personal data has created a critical issue of confidentiality. Production line and vitality are a basic system that requires strong digital resistance assault.

In this environment, even true professional security tools may be unique. However, it is obviously not enough to give a safe inclusion in a similar inheritance system based on facts. This paper describes key security challenges that lag behind the security answers to the featured security challenges. The 5G security institutionalization exercise at the time of writing this article has been introduced.

2. Core Security Challenges for 5G

5G requires a rich set of security designs and solutions because it connects every part of life with the communication system. In this way, we conducted a survey and demonstrated key security and privacy challenges in 5G systems. The basic challenges of 5G demonstrated by the Next Generation Mobile Network (NGMN) and the in-depth research in writing are as follows:

- Edge Computing and Software-Defined Networking

Manuscript received November 5, 2019
Manuscript revised November 20, 2019

5G has test the high transmission capacity and low inertia preconditions fully convey the cost. Now confirmed 5G will be built according to NFV, MEC and SDN. From a security perspective, with key results: Relying on physical division will be harder, so there should be a fundamental, it is assumed that the information is very static and is obvious to different screen characters during travel like the hypervisor is close to the memory of the capabilities. There will be more prominent arrangements and topologies that will be even more powerful. The use of open source programming will be built.

- **Support for privacy**

Discussions about the importance of customer safety and customer safety are expanding regarding who should or should not be close to the customer's substance and its associated metadata, such as IP Addresses, gadgets and personal identifiers, as well as visited areas [3].

- **Network management**

This includes network assurance and optimization. Management and Facilitate network optimization (like traffic shaping) if the carrier can be understood Key meta-data from the traffic they convey. Fraud management and network defense (DOS attacks) will require network operators to understand their meta-data and content being delivered.

- **Internet of things**

This includes organizational affirmation and progress. Administrative and encourage systems to improve (e.g. activity shaping) key meta-information from the activities they pass. Fraud management and digital protection (e.g. for DOS attacks) you need to arrange for administrators to understand their Meta information and content [4].

- **Security overheads**

Security guarantees such as encryption, hashing, and security conventions virtualization conditions are not conducive to time and computational overhead e.g. encrypted answers to security outsourcing or access management suggest key management and calculate the overhead [5].

- **Interference**

The risk of the radio frame is impedance. The Internet of Things has been supported by everyone Create capacity through the huge numbers expected. This is In general, as a matter of gratitude. In any case, the proximity of a large number of gadgets may vary Causing jams within authorized and unauthorized areas - may be called space junk or the ocean is filled with plastic packaging [5].

DOS attacks on end-user devices

There are no security measures for the working framework, application and configuration information on the client device. The 5G program criteria outlined by NGMN through radio proficiency include building a common combinable center and streamlining activities and management by mastering new calculations and organization progress [1]. The following table provides an overview of various security risks and attacks, with a focus on component or service uncertainty in the system, as well as advances that are most prone to attack or danger. These security challenges are described in the accompanying sections.

Table 1 recapitulates the security challenges in 5G technologies.

Table 1: Security Challenges in 5G Technologies

Security Threat	Network Element	Effected technology			Links	Privacy
		SDN	NFV	Cloud		
DOS Attack	Centralized control element	✓	✓	✓		
Signaling storms	SDN controller				✓	
Resource theft	Shared cloud resources		✓	✓		
Configuration attacks	SDN switches	✓	✓			
Saturation attacks	SDN controller and switches	✓				
Penetration attacks	Virtual resources	✓		✓		
Scanning attacks	Open air interfaces				✓	✓
Timing attacks	Subscriber			✓		✓
Boundary attacks	Subscriber location					✓
ISMI catching attacks	Base station				✓	✓

3. 5G Security Goals

As the 5G period approaches, the flow of information and the number of authorities will increase to unobtrusive levels. The benefits of the Internet of Things are there is only one of many. Regarding 5G, it is not just a communication medium [6]. 5G security configurations is a complete security configuration World safety insurance related to everything.

Vertical industry E2E security

- **Differentiated security protection**

The E2E security configuration takes into account various vertical enterprises.

- **Flexibility**

In order to provide better help and quick response to vertical business prerequisites, E2E security capabilities are good Business changes may occur soon. It will require adaptable and efficient end-to-end security arrangements and adaptation.

Security as a service

Faced with the convergence of IT and CT, the telecommunications industry is looking to help them improve quality and better serve vertical businesses. Remotely the communication system does a good job of ensuring customer protection, and the customer has built a general high level of trust in security.

- **Privacy protection**

5G will see the APP government enthusiastic. In addition to this boom, personal safety information is booming, including gadget identifier, client ID and client preferences.

- **Secure Infrastructure**
  - **Differentiated framework-level insurance based on IT thinking**.

    After IT innovations (such as NFV and SDN) are put into use, a large number of framework-level insurances have been established to prevent Administrative Prevention Management and other dynamic attacks that may increase.
  - **Identity management**

    Both programming and device frameworks operate under multi-vendor conditions. Have specific end goals to mitigate unauthorized organization access Assets, strict personality management is an imaginable need.

4. 5G Security Perspectives

New Trust Model and Identity Management:

In the inherited multi-function switching system, the telecommunications system is responsible for verifying the client's arrangement. Verification between customer and administration is not guaranteed system [7]. The system can work with professional cooperatives to complete safer, more efficient role management (Fig. 1).

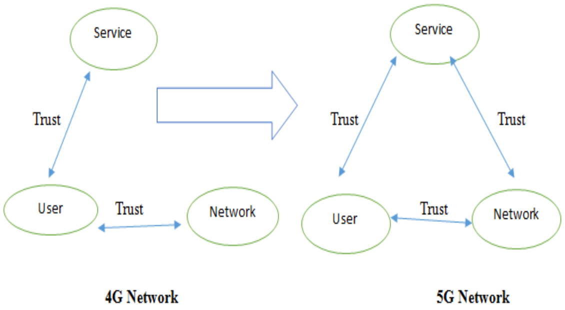

Fig. 1 Comparison of 4G and 5G networks.

5. Hybrid Authentication Management

The 5G system is open and has a lot of management. Smart transportation, a brilliant matrix, and a modern Internet of Things are some of them [8]. These two systems in addition, professional organizations face the challenge of making access and management validation more difficult and cheaper. Three verification models may coexist in 5G to meet the needs of various organizations.

- **Authenticate by system**

Management verification brings key spending metrics to professional cooperatives. Expert organization can provide a welfare payment system once confirmed the customer will be able to reach a large number of authorities after completing a separate verification.

- **Authenticated by a professional organization**

Then, the system may rely on the vertical verification of the vertical business and the excluded gadgets the radio system is verified, which can reduce the cost of the system.

- **Authenticated by two systems and professional organizations**

For some administrations, the inheritance model can be accepted. System processing arrangement visit, expert cooperative management benefits are obtained.

- **Diversified Identity Management**

The legacy cell system relies on a SIM card to monitor the customer's personality and key. In 5G, gear types, such as sensors, wearable devices Gadgets and savvy home gadgets may be too little or too modest to force SIM.

- **Combination of device identification and service identification**

In the new identity management framework, identity consists of device identity and service identity. Each device identification (also known as physical identity) is globally unique and can be assigned to devices at the manufacturing stage. Service identity is assigned by the service provider or network.

- **From device-based management to user-based management**

It allows the user to decide which devices are allowed to access the network and which services are allowed as devices of the same user can share bandwidth quotas with each other online or offline.

6. Service-Oriented Security

Build E2E Security

Differentiated security for different services

The 5G system will benefit from it. This means that special attention will be paid to safety necessities.

Adaptable safety design that contributes to the safety attributes of various system slices

Regarding the opportunity to provide separation of separation security, adaptive safety engineering is expected to help E2E assurance based on various management Arrange the cutting design [9].

A Uniformed security management system for multi-vendor environment

In the cloud state, system-based programming and types of gears originate from more than one hardware seller.

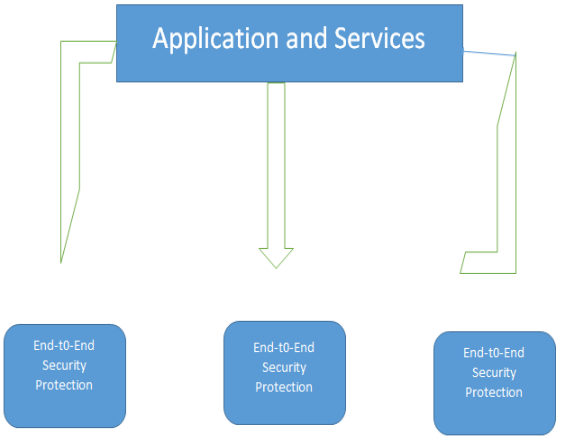
Application and Services
End-t0-End Security Protection
End-t0-End Security Protection
End-t0-End Security Protection

Fig. 2 E2E Security Protection.

Security Assessment

5G needs an open phase to help with the massive management of vertical business, for example, telemedicine services, the Internet Vehicles and the Internet of Things. Depending on the capacity, the platform can be further divided into units.

All system work units may need to verify each other if they are safe, so when they merge entering a phase, you can complete the phase of the abnormal state of security [10].

A common method of investigating the quality of its safety is the signature of the seller. Trust the combination and then test each other's secure execution. In this way, it seems like a universally popular evaluation system and equipment closer, all sellers can test their system work units using standard methods. A safety assessment can be obtained as long as specific and quantifiable safety measures are meaningful for each system work unit.

7. Security Solutions for Privacy in 5G

5G must exemplify the safeguards that protect the planned and bad habits. In order to protect client security in the 5G framework, there should be shared understanding and trust models with different partners, such as clients, scheduling administrators, stakeholders, application designers, and information utilization and capacity manufacturers [1]. In this way, 5G will need better tools to achieve accountability, information minimization, directness, acceptance and access control. Also requiring a cloud-based semi-converged approach, portable administrators can store and process very sensitive information locally and store less subtle information in a wide range of daylight fog.

Encryption based practices can be used in this case; for example, messages can be scrambled before being sent to a Region-based Service Provider. Systems are equally important, where the nature of the regional data is reduced to ensure location protection. For the IMSI to obtain an attack, an improved answer to ensure the identity of the supporter is to utilize TMSI, which is arbitrarily created and assigned to the UE in a general temp. The long-term use of IMSI is only due to blame recovery and the fact that TMSI has not been assigned. Another approach might be to employ a separation technique that would allow the identification of a fake base station that captures the spokesperson's IMSI.

5G Security Standardization

The institutionalization of 5G security is still in the drafting stage, and different key associations are making unremitting commitments to their rapid improvement. In March 2015, 3GPP determined the expiration date of the 5G specification features around 2020. At that time, NGMN distributed 5G white papers to ensure a variety of topics, including virtualization, protection, radio design, accessibility and the Internet of Things [11]. The real task is to propose 5G security engineering by checking for hazards and prerequisites. The 3GPP's SA3 collection covers all security perspectives, including RAN security, authentication components, and system cutting.

The Open Network Foundation (ONF) is committed to accelerating the use of SDN and NFV and distributing specialized decisions, including specifications for these technologies. Similarly, the NFV-secured ETSI Industry Specification Group (ISG) and (ISG NFV SEC) is responsible for the safety details of the NFV phase. The ISG NFV SEC sets out requirements for standard interfaces in the ETSI NFV design, including safety work that can gradually address potential safety hazards. In 2014, the ESTI MEC ISG was designed to handle the MEC security model and implement NFV functionality within the RAN to convey security and power [13]. The International Telecommunication Union (ITU) continues to bring together commitments from provincial associations such as ETSI and ARIB and advises institutionalized associations.

User Privacy Protection

As the 5G system will serve a large number of vertical services. This shows the extraordinary measures of customer protection data [14]. In addition, adhere to the 5G organization. Any data interruption can lead to serious consequences.

Usage management of privacy information in 5G network

5G arranges to provide customers with system management changes through inspection management (counting cut customization or selection) emphasize. Still, protecting data (for example, client benefit data and regions) can be used to manage component detection deal with [15]. In order to protect the client, the 5G system must clearly characterize the management testing standards to solve the customer's worries protection.

8. 5G: Future of Communications Networks

The fifth generation of wireless technology is causing great enthusiasm in the broadcasting and communication industry and contrasting. Some people think that 5G is the following development in telematics, promises higher transmission speeds and information rates, and transmission delays are basically less. Others, to the extent possible, innovation will be progressive, giving a large number of new applications, including humanoid robots, related cars and the Internet of things, with billions of gadgets associated with installed sensors.

Through the historical background of multi-functional exchange, the speed of information gradually jumps in every era of the system [16]. This will also be the case for 5G, but more scenarios are expected, including enhanced execution, limits and speed, and a system that works globally, regardless of where the client is or from which gadget interface.

The carrier will reduce the delay in transmission time. 5G idle depends on less than 1 millisecond; 4G system has 25 milliseconds of inactivity. Inactivity is a measure of the time it takes for a piece of information to start from one point of transmission and then to another.

Still, just updating the device and programming with the latest innovations is not enough. The new system should handle the billions of devices expected by the Internet of Things and other new applications. It must provide an association that is 100 times faster than the current system.

9. Methodology

5G networks can be simulated in OPNET using LTE-A model along with IEEE 802.15c Model. Basically, OPNET is a high level event based network level simulator used for the simulation of 5G network hardware and protocols.

Advantages of 5G using OPNET simulator:

- Generalized handling
- Awesome management in the team
- Super persistent and solid association
- Many simple gadgets
- Bit rate delay
- Postponed, reliability advertising new mechanical applications.

It is planned to set the correspondence between at least two spatially isolated clients by electronic means, wherein the customer can send/acquire a wide range of data classifications as voice and video information (Fig. 3).

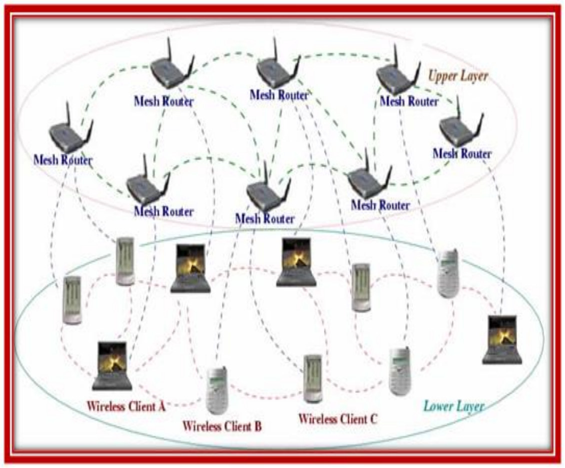

Fig. 3 Advantages of 5G using OPNET simulator.

The 5G library for the LTE System Toolbox enables us to study the implementation and implementation of 5G wireless access innovations featuring the Release 15 3GPP NR standard V15.0 (Fig. 4).

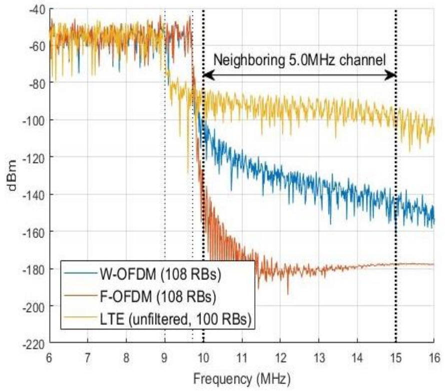

Fig. 4 LTE spectra

5G NR PDSCH Transport Channel:

- Code square division and de-allocation
- LDPC channel
- coding Assessment coordination and recovery

5G NR polar coordinate coding:

- CRC supported polar (CA-Polar) coding for control and communication channels
- Evaluation and recovery rate

TR 38.901 Communication Channel:

- Tapped Delay Line (TDL) Channel Demo

- Launched a delayed line (CDL) channel program.

5G will use mobile clouds, SDN and NFV to address the challenges of large-scale connectivity, flexibility and cost. Beneficially, these technologies also have inherent security challenges. Therefore, in this paper, the main security challenges that may become more threatening in 5G have been described, unless properly addressed. These security mechanisms and solutions for these challenges have been proposed.

However, due to the limited integration and integration of these technologies in 5G, security threat vectors cannot be fully implemented at this time. Similarly, more user devices such as communication security and privacy challenges will become more apparent. The Internet of Things is connected to each other, and 5G provides new services. All in all, new security threats and challenges are equally desirable with the deployment of new 5G technologies and services. However, from the initial design phase to deployment, considering these challenges will minimize the potential for potential security and privacy errors.

5G will have complex environments including automaton and air traffic control, cloud-driven virtual reality, related vehicles, intelligent production lines, cloud-driven robots, transportation and electronic health. Therefore, applications need a secure communication system to help more regularly verify and exchange finer information. In addition, many new players, such as open professional organizations, MNOs and cloud administrators, will be included in these administrations.

10. Simulations

Based on the comparison and results above, the simulation criteria to term as:

In light of these studies, the security conditions of information correspondence in the UDN incorporate the accompanying:

(i) Each organize element ought to be commonly confirmed, and the reciprocal elements should utilize their particular private keys. The security instrument ought to be connected to guarantee that the two sides can get applicable data.

(ii) Each correspondence element ought to have the capacity to get the common keys in information interchanges. The distinctive correspondence sessions utilize diverse shared keys.

(iii) The security instruments for information scrambled in view of shared keys should bolster the dynamic joining or leaving of correspondence elements.

(iv) All elements ought to get brought together administration from the system administrator. The age of shared keys between correspondence elements ought to be as per the significant directions.

(v) The security component should bolster numerous consistent channels between similar sources or goals and maintain a strategic distance from the duplication of the key stream.

(vi) The security instrument ought to be productive to guarantee snappy reactions and adjust to the substance's execution and system transfer speed in various correspondence forms.

11. Simulation algorithm

To set up a safe information correspondence session among the system substances, the security arrangement in view of the IC can be actualized in four stages.

Stage 1 (verifiable endorsement age). Prior to setting up the safe information correspondence, the elements should dispatch an IC ask for to the CA. For instance, another AP (indicated as Ent_UID endeavors to join the APG, where another element (signified as Ent_) is enlisted. The substance Ent_UID must speak with the element Ent_ and trade basic data. At that point, Ent_UID sends an IC asks for message.

The substance Ent_UID with a one of a kind personality creates an irregular number and processes. Simultaneously, to maintain a strategic distance from a replay assault, Ent_ produces a cryptographic arbitrary number and figures HMAC. At that point, Ent_UID sends and also the estimation of HMAC to the CA. The HMAC is a keyed-hash message validation code calculation in cryptography.

Stage 2 After the demand is gotten, the CA (private key is, open key is, and) checks the character and relating HMAC of Ent_UID. On the off chance that the approval is affirmed, an arbitrary number will be created. The CA starts to register the accompanying:

(i) The reproduced information of people in general key.

(ii) The scrambled endorsement with the substance's character, where is the element's personality and Encrypt is an encoding capacity for the personality data security.

(iii) The segment information of the private key: , where . is a Secure Hash Algorithm (SHA, for example, SHA-1.

(iv) Similarly, a succession code is created by the CA, and afterward the CA sends back to the requester Ent_ with, and HMAC.

Ent_ at that point confirms the message got from the CA. On the off chance that the confirmation is affirmed, Ent_ processes the accompanying keys utilizing the reproduction information:

Ent_ private key (pKey): E * Ru + s (mod) n
Ent_ open key (PKey): E * CERTu + Qca

The confirmation of Ent_ can likewise be comparably led.
In the UDN, a shared test reaction among the APs can be handled utilizing the confirmation equation technique.
Stage 3 (shared key age amongst Ent_ and Ent_). After the personalities are affirmed, the elements can concur with the common key for the correspondence session to ensure the privacy of information transmission. The sender needs to encode the information before transmission, while the beneficiary needs to unscramble the information. In like manner, both of the correspondence accomplices must have a similar key, to be specific, the "common" key (sKey), in this paper. Be that as it may, since any information with the common key can be blocked and have high hazard, it is difficult to transmit the key as plaintext in the system. Besides, every correspondence session is impermanent and unverifiable. The dynamic sessions require the way to be persistently revived and refreshed. It is hard to preload distinctive encryption keys for every correspondence session in the genuine administrator.

12. Results and Discussion

5G must include a planned approach to protection, where privacy is considered from the earliest starting point of the system, and many of the necessary features must be inherent. In the case where portable administrators can process highly sensitive data in a wide range of daylight [17]. In these areas, administrators can access and control information more and choose where to share. 5G will require better accountability, information minimization, directness, acceptance and access control.

In the process of institutionalizing 5G, the direction and formulation of quantity protection should be considered. Administrative methods can be divided into three categories [7]. The first is the administrative direction, the government mainly through state-specific protection control, and through multinational associations such as the United Nations (UN) and the European Union (EU). Second is the business level, where different companies and gatherings, such as 3GPP, ETSI and ONF, collaborate to draft best standards and practices to ensure protection. The third is the direction of the shopper level, which ensures the required security by considering the buyer's prerequisites.

For zone protection, anonymity based techniques must be connected, where the true role of the supporter can be overridden and replace the alias. The practice based on encryption is additionally useful for this situation, such as, the message can be sent before being sent to the location based service (LBS) provider. Encode. For example, a confusing approach is also valuable, which reduces the nature of regional data while keeping in mind the ultimate goal of ensuring regional protection. In addition, area-based coverage calculations are useful for handling some important regional security attacks, such as timing and limiting attacks.

In addition, 5G networks have different participants, such as virtual MNOs (VMNOs), communication service providers (CSPs), and network infrastructure providers.

All of these participants have different security and privacy priorities. The synchronization of inconsistent privacy policies between these participants will be a challenge in 5G networks. In previous generations, mobile operators had direct access to and control of all system components [2]. Therefore, 5G operators will lose their comprehensive governance of security and privacy. In a shared environment, user and data privacy are severely challenged, with the same infrastructure being shared among the various participants, such as VMNO and other competitors.

In addition, 5G networks have no physical boundaries because they use cloud-based data storage and NFV capabilities.

Therefore, 5G operators cannot directly control the data storage location in the cloud environment. Since different countries have different levels of data privacy mechanisms depending on their preferred environment, privacy is questioned if user data is stored in a cloud in a different country. For example, the UE keeps moving for 30 minutes with the particular paces of 3 km/h, 30 km/h, and 60 km/h as indicated by Table 2. The required stockpiling limit can be ascertained utilizing the equation above. The outcomes are appeared as takes after (accepting the SIM card limit is 32 kB) [18]:

$$128\,\text{bit}\times30\times60\times0.731 = 168422\,\text{bits} = 20\,\text{kB} < 32\,\text{kB}.$$
$$128\,\text{bit}\times30\times60\times1.421 = 327398\,\text{bits} = 40\,\text{kB} > 32\,\text{kB}.$$
$$128\,\text{bit}\times30\times60\times2.018 = 464947\,\text{bits} = 56\,\text{kB} > 32\,\text{kB}.$$
$$128\,\text{bit}\times30\times60\times0.771 = 177638\,\text{bits} = 22\,\text{kB} < 32\,\text{kB}.$$
$$128\,\text{bit}\times30\times60\times1.425 = 328320\,\text{bits} = 40\,\text{kB} > 32\,\text{kB}.$$
$$128\,\text{bit}\times30\times60\times2.034 = 468634\,\text{bits} = 57\,\text{kB} > 32\,\text{kB}.$$
$$128\,\text{bit}\times30\times60\times0.579 = 133402\,\text{bits} = 16\,\text{kB} < 32\,\text{kB}.$$
$$128\,\text{bit}\times30\times60\times1.228 = 282931\,\text{bits} = 35\,\text{kB} > 32\,\text{kB}.$$
$$128\,\text{bit}\times30\times60\times1.796 = 413798\,\text{bits} = 51\,\text{kB} > 32\,\text{kB}.$$

In any case, in our answer for secure information correspondence, the pairwise key that incorporates people in general key and private key is an irregular age utilizing the rebuilt parameters. The pairwise key ought to be spared by the system elements, while the mutual keys are immediately figured. The common keys can be created ordinarily and don't require capacity. Subsequently, the keys' stockpiling limit will be essentially steady, and the keys' storage room can be computed by recipe (6):
225ece 2 256 = 115200 bits = 14 kB.

13. Conclusions

For the security and protection of a huge system, it does not work after 5G the different parts of the system configuration have just been completed. Instead, security In addition, protection features should be included in the system plan. This goal requires a Security and protection between the dynamic discourse between the network and every other party who Contribute to 5G innovation.

Now, many parts of 5G are still unverifiable but there is still some abnormal state. Choices about safety and protection standards can now be agreed partner. For example, whether you have 5G security or not, you can agree the security device will still cover the management layer despite the entry level. The time is generally correct to determine whether to extend the end-to-end portion.

Therefore, it may now be agreed whether to expand security. If you receive each of these standards, it will affect the 5G system outline and they can be considered in the early stages of planning, and Words can begin. All the issues we discuss in this article will be understood as some stage of the discourse, once started.

Safety and protection prerequisites are often seen as obstacles or weight However, in the long run, the system configuration will ignore them anyway. The features included since then are less successful and are usually more expensive than including it. In the long run, security is a driving factor Management and system development. Management and systems engineering from 5G is undergoing a sensational redesign that will enhance elements and concentration if safety insurance and protection ideas are incorporated on time, the quality of 5G.

References

[1] I. Ahmad, T. Kumar,” Overview of 5G Security Challenges and Solutions” pp. 229-233, 2018. DOI: 10.1109/MCOMSTD.2018.1700063

[2] Madhusanka Liyanage, Ijaz Ahmed, Raimo Kantola, "Enhancing Security of Software Defined Mobile Networks", Access IEEE, vol. 5, pp. 9422-9438, 2017. doi: 10.1109/ACCESS.2017.2701416

[3] G.B Satrya, "Security enhancement to successive interference cancellation algorithm for non-orthogonal multiple access (NOMA)", Personal Indoor and Mobile Radio Communications 2017 IEEE 28th Annual International Symposium on, pp. 1-5, 2017. doi: 10.1109/PIMRC.2017.8292165

[4] M. S. Parwez, A. Imran, Continuous time markov chain based reliability analysis for future cellular 5G networks, IEEE Global Communications Conference (GLOBECOM), pp. 1-6, 2015. doi: 10.1109/GLOCOM.2015.7417594

[5] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, “A Survey on Wireless Security: Technical Challenges, Recent Advances, and Future Trends”, Proceedings of the IEEE, vol. 104, no. 9, pp. 1727-1765, 2016. https://arxiv.org/pdf/1505.07919

[6] J. Prados-Garzon, J. Navarro-Ortiz, J. Lopez-Soler, "Link-level access cloud architecture design based on SDN for 5G networks", IEEE Networks, vol. 29, no. 2, pp. 24-31, 2015. DOI: 10.1109/MNET.2015.7064899

[7] I. Ahmad, “5G security: Analysis of Threats and Solutions,” 2017 IEEE Conf. Standards for Common. And Net-working, Sept 2017, pp. 193–99. DOI: 10.1109/CSCN.2017.8088621

[8] T. S. Rappaport, S. Sun, R. Mayzus, H. Zhao, "Millimeter wave mobile communications for 5G cellular: It will work!", IEEE Access, vol. 1, pp. 335-349, May 2013. doi: 10.1109/ACCESS.2013.2260813

[9] Dongfeng Fang, Yi Qian, Rose Qingyang Hu, Security for 5G Mobile Wireless Networks, Access IEEE, vol. 6, pp. 4850-4874, 2018. doi: 10.1109/ACCESS.2017.2779146

[10] Yi Qian, Rose Qingyang Hu, "Security for 5G Mobile Wireless Networks", Access IEEE, vol. 6, pp. 4850-4874, 2018. doi: 10.1109/ACCESS.2017.2779146

[11] Ghada Arfaoui, Jean-Philippe Wary, "Security and Resilience in 5G: Current Challenges and Future Directions", Trustcom/BigDataSE/ICESS 2017 IEEE, pp. 1010-1015, 2017. DOI:10.1109/Trustcom/BigDataSE/ICESS.2017.345

[12] Ghada Arfaoui, Pascal Bisson, Mike Surridge, Jean-Philippe Wary, Alexander Zahariev, "A Security Architecture for 5G Networks", Access IEEE, vol. 6, pp. 22466-22479, 2018. doi: 10.1109/ACCESS.2018.2827419

[13] P. Schneider, “Towards 5G Security Threats”, Trustcom/BigDataSE/ISPA, 2015 IEEE, Volume 1, pp. 1165-1170. doi: 10.1109/CSCN.2017.8088621

[14] Fang, Qian, QingYang "Security and DoS framework for 5G and next generation mobile broadband networks", Smart Technologies IEEE EUROCON 2017 -17th International Conference on, pp. 104-109, 2017. doi:10.1109/ACCESS.2017.2779146

[15] Akhil Gupta, Sanjeev Jain, Bandwidth Spoofing and Intrusion Detection System for Multistage 5G Wireless Communication Network, Vehicular Technology IEEE Transactions on, vol. 67, no. 1, pp. 618-632, 2018. doi: 10.1109/TVT.2017.2745110

[16] E. Hossain and M. Hasan, "5G cellular: key enabling technologies and research challenges," IEEE Instrumentation & Measurement Magazine, vol. 18, pp. 11-21, 2015. DOI: 10.1109/MIM.2015.7108393

[17] Madhusanka Liyanage, Ijaz Ahmed, Raimo Kantola, "Enhancing Security of Software Defined Mobile Networks", Access IEEE, vol. 5, pp. 9422-9438, 2017. doi: 10.1109/ACCESS.2017.2701416

[18] Z. Chen, S. Chen, H. Xu, B. Hu, “A Security Scheme of 5G Ultradense Network Based on the Implicit Certificate”, Wireless Communications and Mobile Computing, 2018, Article ID 8562904, https://doi.org/10.1155/2018/856290

Abdullah Bajahzar received a PhD in Computer Science and Software Engineering degree from De Montfort University, United Kingdom, in 2014 and MSc Software Engineering degree from De Montfort University, United Kingdom, in 2008. He is currently working as an Assistant Professor at Majmaah University, Saudi Arabia. His research interest includes data mining, big data, IoT and data science.