International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 10 Oct. 2022, pp: 439-451 www.ijaem.net ISSN: 2395-5252

A Review of Emerging Security Issues in 5g Wireless Communication

Ogunlere S. O[1]., Oladejo D. O[2]., Onilede S. O[3]., Adeniyi B. S[4], Bamidele O.[5]

[1,3]*Department of Information Technology, Babcock University, Illishan, Nigeria;*
[2,,4,5]*Department of Computer Science, Babcock University, Illishan, Nigeria;*

Date of Submission: 01-10-2022 Date of Acceptance: 13-10-2022

ABSTRACT - Wireless communication has evolved in all areas of mobile and wireless communications and it is one of the fastest growing sectors. In the last decade, there has been a huge increase in wireless technology. Hence there is need for improved trust models that will set the pace. This paper begins with a brief on the evolution and development of different generations of mobile wireless technology and their importance and benefits among others. It also reviewed the essential aspects of the architecture and network security of 5G. Additionally, it summarized existing literature on security of 5G technologies based on enhancements to authentication, encryption, and assurance of availability, integrity, and privacy. It concluded by making a case for improved trust models among different use cases as new actors continue to emerge in 5G wireless network communications.

Keywords - 5G architecture, Wireless Communications, Security, Trust models, Enhancements.

I. INTRODUCTION

The popularization of mobile and smart devices and the innovation of technologies have introduced applications and services with requirements such as high performance, security, quality of service (QoS), and mobility. These requirements have driven the evolution of wireless communication technologies. 5G networks are expected to meet the needs of a wide range of applications, with different demands and in diverse and heterogeneous scenarios (5G Americas, 2020).

Designing a network capable of delivering these services with a single, predefined set of essential network functions would be highly complex and expensive. Faced with this situation, there is a certain consensus that 5G networks will be characterized by having a dense, heterogeneous, and shared network infrastructure between different operators, transparent use of multiple access technologies, the softwarization and virtualization of communication functions and protocols (5G Americas, 2018).

5G has a vision oriented to services consolidated in the scientific and technical community. A proposal aimed at facilitating the 5G vision is implementing the concepts of network softwarization, network virtualization, and network slicing (NS). Implementing these concepts allows the execution of new and diverse use cases and business models. The International Telecommunication Union's (ITU) 5G vision outlines use cases with a wide range of technological efficiency and system specifications, necessitating the interconnection of mobile networks with non-3rd Generation Partnership Project (3GPP) network technologies (3GPP, 2021). A single network provider in their domain would not be able to do this. There is a clear need for network-to-network interoperability that is also stable and reliable. Although the 3GPP has released 5G specifications that describe inter-network communications interfaces, further work is needed to improve interface functionality, performance, and security. The standardization for 5G communication has been completed, and the 5G networks are already becoming a commercial reality (Tataria et al., 2021). Therefore, the research community is looking beyond 5G to the sixth generation (6G) of wireless networks. 6G networks are expected to provide critical features on the communication services for future demands such as high security, secrecy, and privacy.

Also, 6G networks are expected to achieve the requirements of a fully connected world and provide ubiquitous wireless connectivity for everyone (Akyildiz, Kak, &Nie, 2020). The security infrastructure of 5G will be the foundation upon which 6G wireless network security will be built.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 10 Oct. 2022, pp: 439-451 www.ijaem.net ISSN: 2395-5252

Hence there is need for improved trust models that will set the pace.

A. Aim of the Study

The aim of this study is to review the essential aspects of the architecture and network security of 5G, summarize existing literature on security of 5G technologies and make evident the need for improved trust models among different use cases as new actors continue to emerge in 5G wireless network communications.

II. WIRELESS TECHNOLOGIES FROM 1G TO 7G

This section discusses briefly on the evolution and development of different generations of mobile wireless technology and their importance and benefits among others (Rani, Pritee, Deepak, & Umesh, 2020). In 1974, the mobile communication system introduced the first generation (1G) which was completed in 1984. At an earlier stage, it was developed primarily to communicate with mobile phones through a network of distributed transceivers. This generation is commonly referred to as the generation of wireless telecommunication technology that is popularly known as cell phones. The 1G mobile wireless communication systems is an analogue frequency modulation system and the technology that forms the basis for this generation is NMT (Nordic Mobile Telephony), AMPS (Advanced Mobile Phone Service) and CDPD (Cellular Digital Packet Data).

The second generation (2G) is based on the global system Mobile communication (GSM). It started in Finland in 1991. It was the first digital cellular network; there were many obvious advantages over analogue networks. They were flexible with improved sound quality, better Security etc. 2G technology has replaced analogue technology with digital communication by providing services such as text messaging, picture messaging and multimedia services (MMS). All text messages are digitally encrypted in this technology. This digital encryption allows data to be transferred in a way that only the recipient can receive and read.

The third generation (3G) of the mobile system provides 144 kbps high speed data transmission. Its features include high-speed transmission, advanced multimedia access and global roaming. 3G is used with mobile phones or handsets to connect to the internet or other IP networks for making voice and video calls, downloading and uploading data and surfing the net. 3G supported multimedia applications like full-motion video, video conferencing and internet access. Data is sent through a technology which is called as packet switching. Voice call is interpreted by circuit switching. This is the most sophisticated form of communication in the last decade.

The fourth generation of mobile communications upgraded existing communication networks and provided a comprehensive and secure IP-based solution where features like voice, data and streaming multimedia became available to users on "anytime, anywhere" basis and much higher data rates than previous generations. The term MAGIC is used to explain the 4G technology, which means M for mobile multimedia, A for any time anywhere, G for global mobility support, I for integrated wireless solution and C for customized personal service. 4G provided 1 Gbps speed for data transmission.

5G is the 5th generation mobile network. It is a new global wireless standard after 1G, 2G, 3G, and 4G networks. 5G enables a new kind of network that is designed to connect virtually everyone and everything together including machines, objects, and devices. 5G wireless technology is meant to deliver higher multi-Gbps peak data speeds, ultra-low latency, more reliability, massive network capacity, increased availability, and a more uniform user experience to more users. Higher performance and improved efficiency empower new user experiences and connects new industries. 5G is designed to deliver peak data rates up to 20 Gbps based on IMT-2020 requirements. In addition to higher peak data rates, 5G is designed to provide much more network capacity by expanding into new spectrum, such as millimetre Wave. 5G can also deliver much lower latency for a more immediate response and can provide an overall more uniform user experience so that the data rates stay consistently high even when users are moving around.

The sixth-generation technology uses the latest combination of radio and fibre optics technology. Data delivery will be through the lens with reduced dependence on copper cables or bases. The 6G mobile system will integrate 5G wireless mobile systems and satellite networks for global coverage. Telecommunications satellite is used for voice, data, internet and video transmission. Earth imaging satellite network is for the collection of weather and environmental information and the Navigational Satellite Network for Global Positioning System (GPS). It is believed that 6G will make the speed of 1GB. 6G has four different standards namely Pico cell, micro cell, macro cell and satellite cell. So, these four networks must have handoffs and roaming but how that will happen is not yet answered.

7G (seventh-generation wireless) is the inevitable intelligent cellular technology. It is similar

International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 10 Oct. 2022, pp: 439-451 www.ijaem.net ISSN: 2395-5252

to 6G for global coverage but it will also define satellite functions for mobile communications.7G networks will be able to use higher frequencies and provide substantially higher capacity and much lower latency in communications.

A. 5G Network Architecture

The basic protocol that will run on the 5G is the Internet Protocol version 6 (IPv6). The physical and data link layers define the 5G wireless network technology as an Open Wireless Architecture (OWA). In order for the 5G to maintain virtual multi wireless network, the network layer is divided into upper and lower network layers. While the upper layer is for mobile terminals, the lower layer is for interface. In the network layers all the routing are based on IP addresses. The session and transport layers in the 5G network Open Systems Interconnection (OSI) layers support the open transport protocol (OTP) which is used to overcome higher bit rate losses while quality of service management across various types of networks is handled by the application layer (Idowu-Bismark, Kennedy, Idachaba, &Atayero, 2018).

The OSI (Open System Interconnection) layers for the 5G network is shown in Figure.1. In 5G network, the 5G terminal is expected to be software radio driven with modulation and error control schemes that are downloadable from the internet.

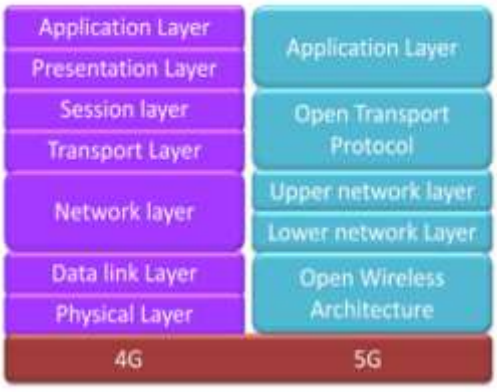

Figure 1: 4G and 5G Network OSI Layers (Idowu-Bismark, Kennedy, Idachaba, &Atayero, 2018)

B. 5G System Architecture

The 5G core network oversees functions that are not directly related to radio access but are needed to provide a full network. This involves things like authentication, billing, and setting up end-to-end connections. Managing these functions separately, rather than incorporating them into the radio-access network (RAN) is advantageous since it enables many radio-access technologies to be supported by the same core network (Dahlman, Parkyall, &Skold, 2020). The RAN oversees the overall network's radio-related features, such as scheduling, radio-resource management, re-transmission protocols, coding, and various multi-antenna schemes.

C. Core Network

Today's core network is already heavily virtualized, with core network functionality running on commodity computer hardware. The term NS is widely used in the sense of 5G. A network slice is a logical network that serves a specific business or customer need by combining the required functions from the service-based architecture. One network slice, for example, may be set up to serve mobile broadband applications with maximum mobility support, close to what Long Term Evolution (LTE) offers. Another slice can be dedicated to a non-mobile, latency-sensitive industry automation program. These slices will all run on the same underlying physical core and radio networks, but from the viewpoint of end-user applications, they will appear as separate networks. It is close in several ways to set up several virtual machines on the same physical machine. Edge computing can be used in a network slice like this. A network slice may also include sections of the end-user program that run close to the core network edge to provide low latency.

The 5G core network architecture emphasizes a control-plane/user-plane split, with separate bandwidth scaling for the two. Suppose more control plane capacity is needed, for example. In that case, it should be simple to add it without affecting the network's user plane. On a high level, the 5G core can be illustrated using a service-based representation as depicted in Figure 2.

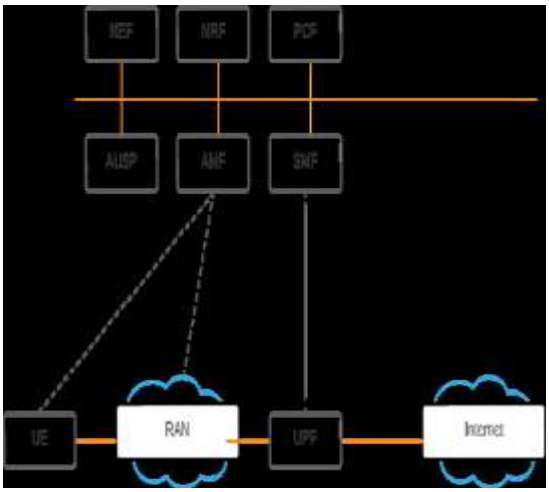

Figure 2: 5G service-based representation (Dahlman et al., 2020)

International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 10 Oct. 2022, pp: 439-451 www.ijaem.net ISSN: 2395-5252

The user-plane function (UPF) and the gateway between the RAN and external networks such as the Internet make up the user-plane function. Packet routing and forwarding, packet verification, Quality of Service (QoS) management, packet filtering, and traffic measurements are among its duties. Many components comprise the control-plane functions, such as the session management function (SMF). IP address allocation for the system (also known as user equipment (UE), policy compliance control, and general session-management functions are all handled by the SMF. The access and mobility management function (AMF) takes care of control signalling between the core network and the device, security for user data, idle-state mobility, and authentication. The functionality operating between the core network, specifically the AMF, and the device is sometimes referred to as the non-access stratum (NAS), to separate it from the access stratum (AS), which handles functionality operating between the device and the radio access network. Besides, the core network can also handle other types of functions, for example, the policy control function (PCF) responsible for policy rules, the unified data management (UDM) responsible for authentication credentials and access authorization, the network exposure function (NEF), the network repository runction (NRF), the authentication server function (AUSF) handling authentication functionality, and the application function (AF).

D. Network Slicing (NS)

5G leverages the option to build virtual corporate networks within the network itself, a function known as Network Slicing (NS) (Foukas, Patounas, Elmokashfi, & Marina, 2017; Afolabi, Taleb, Samdanis, Kasentini, &Flinck, 2018). Each of these slices is created with guaranteed service quality parameters and customized according to the specific needs of each company or organization (Kaloxylos, 2018). Their customization, i.e., their creation as private networks, ensures a good quality of service, increasing their reliability (Su et al., 2019). Any facility will have its own 5G node, which will provide a specific network segment adapted to its particularities and QoS (Laghrissi&Taleb, 2018).

This adaptive network model can be attributed to two technologies: network virtualization and edge computing. With the development of edge computing, or cloud computing, companies can process data and apply decision algorithms close to the internet of things (IoT) devices that generate the information. This new approach to transmitting information also opens up new possibilities across the board, especially compared to the long distances that data has to travel today with the need to send it to processing environments.

E. NS Basic Design Principles

The NS architecture is based on three principles: isolation, elasticity, and end to end (E2E) optimization (Kaloxylos, 2018):

1. **Isolation:** This is a NS feature that can separate and impose limits on network resource use. This feature is supported by network virtualization. It also ensures the performance of different users (Mobile vendors, Network operators, Vertical industries) through an equitable distribution of resources. Isolation can be deployed:

(I) By using a different physical resource

(II) When separating a shared resource via virtualization

(III) Through sharing a resource with the guidance of a respective policy that defines the access rights for each tenant.

2. **Elasticity:** This is an essential operation related to the resource allocated to a particular network slice. Specifically, elasticity allows the dynamic management of resources allocated to network segments according to different users' demands to use them efficiently. Fixed availability of resources on a network segment can lead to under, and over-utilization of resources due to user demands variations (Abdulghaffar, Mahmoud, Abu-Amara, &Sheltami, 2021). Therefore, NS is designed with an elastic nature to simultaneously satisfy the users QoS and optimize the overall network overhead. The main challenge in the elasticity application is the negotiation policy between network segments so that the performance of the network segments is not affected by an increase in the number of users or an increase in QoS. However, this process requires an inter-slice negotiation since it may influence the performance of other slices that share the same resources.
3. **Customization E2E**: NS's inherent property is for facilitating service delivery from the service providers to the end-user(s)/customer(s). Network segments ensure that the network operator’s shared resources are efficiently utilized between different users. Network segments customization in NS is performed at all layers of the network topology using the technical features provided by Software Defined Networks(SDN) and supported by the advantages of Network Function Virtualization **(**NFV). As described by (Lin, Tseng, & Wang (2021), E2E property has two extensions:

International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 10 Oct. 2022, pp: 439-451 www.ijaem.net ISSN: 2395-5252

(I) A slice that combines resources that belong to distinct infrastructure providers
(II) It unifies various network layers and heterogeneous technologies,

F. Technologies enabling NS

The key virtualization technologies for NS are listed below:

1. **Software Defined Networks:** It provides key characters such as flexibility, service-oriented robustness adaptation and scalability. SDN creates a virtualized control plane that enables intelligent management between network functions, eliminating the gap between service provisioning and network management, i.e., with SDN network control becomes directly programmable using standardized interfaces (Prabakaran, Nizar, & Kumar, 2021). The SDN controller manages network slices applying rules when necessary and following the corresponding network policy. Furthermore, SDN permits flexibility into control and data planes in 5G networks.
2. **Network Function Virtualization:** It allows the deployment of originally based in hardware network functions (NF) on virtual environments leveraging benefits of cloud computing. With NFV, NFs can be easily deployed and dynamically allocated, as well as NFs can be assigned to service providers (SPs) so that mobile network operators (MNOs) can share their infrastructure (Prabakaran et al., 2021).
3. **Edge computing:** technologies as cloud and edge computing offer computational, storage, and networking facilities within single or multiple platforms for enabling a network slice. Specifically, edge computing enables data acquisition and provides services close to end-users allowing a form of edge-centric networking, which facilitates data proximity, assuring ultra-low latency, high data rates, and intelligence and control.

III. CYBERSECURITY IN 5G

The services and applications offered by the connectivity of emerging 5G networks will introduce new security requirements to mitigate vulnerabilities and attacks. These must be addressed in the deployment of 5G networks. The transition to 5G networks according to the 3GPP is divided into two parts:

a) Standalone networks, where a 5G core (5GC) network is introduced
b) Non-standalone networks, which will take advantage of the same protocols of the plane of LTE control and the LTE evolved packet core (EPC) network (5G Americas, 2020).

A. Threats, Vulnerabilities, and Attacks

This section highlights the threats, vulnerabilities and attacks in 5G networks.

B. 5G Non-standalone (NSA)

The operation of the 5G NSA architecture is based on LTE control plane protocols (see Figure 2), so the initial 5G NSA launches will only offer Mobile Broadbandimprovements. Threats and vulnerabilities presented in LTE will also affect the 5G NSA network (Tataria et al., 2021). For a proper transition to 5G, the threats that occur in 4G must be considered.

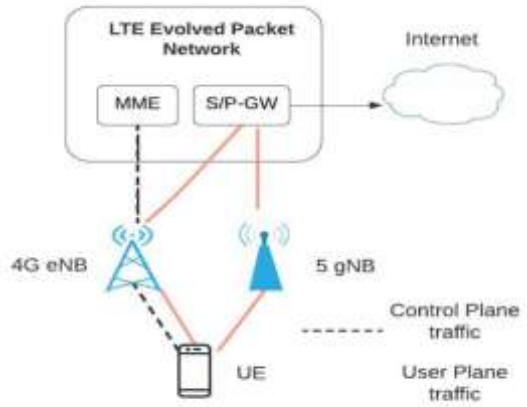

Figure 3: Non-standalone architecture (Tataria et al., 2021)

The main security threats to the 5G NSA network are described below:

1. **Downgrade attack:** This attack forces a User Equipment LTE connection to connect to 2G or 3G, even though the end-user can do so with higher technology.
2. **Data modification attacks:**Universal Mobile Telecommunications System (**UMTS**) and LTEcommunications integrity are not protected by any security method to intercept the information flow. This could lead to data injection or modification, such as man in the middle (MITM) (5G Americas, 2018). Mutual authentication between the mobile device and the base station can prevent a MITM-type attack.
3. The 5G Extensible Authentication Protocol - Authentication and Key Agreement EAP-AKA protocols are emerging solution to enable connection requests and then initiate the authentication process in 5G networks.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 10 Oct. 2022, pp: 439-451 www.ijaem.net ISSN: 2395-5252

4. **IMSI Tracking:** when IMSI (International Mobile Subscriber Identity) requests are made. The international mobile sub-scriber identity (IMSI) is sent unencrypted over the radio, thus allowing the attacker to find out which SIM card is using the connected user.
5. **Base station spoofing:** "fake" base stations are capable of unknowingly tracking and collecting their personal data.
6. **LTE roaming**: The use of old signalling protocols such Signaling System 7 (SS7) (an international telecommunication protocol standard that defines how the network elements in a public switched telephone network (PSTN) exchange information and control signals) with vulnerabilities in 2G, 3G / 4G could expose users to listening to voice conversations, reading or transmitting messages, and tracking phones (IT Pro Portal, 2019).

IV. REVIEW OF EXISTING SECURITY SERVICES IN 5G WIRELESS NETWORKS

The new architecture and new technologies in 5G wireless networks ushered in new features and requirements of security services. This section, primarily introduces four types of security services: authentication (entity authentication and message authentication), confidentiality (data confidentiality and privacy), availability, and integrity.

A. Authentication

There are two kinds of authentications, namely, entity authentication and message authentication. Both entity authentication and message authentication are important in 5G wireless networks. Entity authentication is used to ensure the communicating entity is the one that it claims to be. The authentication and key agreement (AKA) in 4G LTE cellular networks is symmetric-key based. However, 5G requires authentication not only between user equipment (UE) and mobility management entity (MME) but also between other third parties such as service providers. Since the trust model differs from that used in the traditional cellular networks, hybrid and flexible authentication management is needed in 5G. The hybrid and flexible authentication of UE can be implemented in three different ways: authentication by network only, authentication by service provider only, and authentication by both network and service provider (Huawei White Paper, 2015).

Due to the very high speed data rate and extremely low latency requirement in 5G wireless networks, authentication in 5G is expected to be much faster than ever. Moreover, the multi-tier architecture of the 5G may encounter very frequent handovers and authentications between different tiers in 5G. This frequency causes unnecessary latency between different tiers.

Abualhaol and Muegge (2019) proposed a security scoring based on continuous authenticity developed to evaluate and improve the security of 5G wireless systems. The principle of legitimacy patterns is proposed to implement continuous authenticity, which enables attack detection and system security scoring measurement. For the legitimacy pattern, a redundant sequence of bits is inserted into a packet to enable the attack detection. The simulation results show the feasibility of implementing the proposed security scoring using legitimacy patterns. The authors pointed out that legitimacy patterns considering technical perspectives and human behaviours could improve the performance.

Combining the high security and utmost efficiency in bandwidth utilization and energy consumption in 5G, Dubrova, Naslund and Selander (2018), proposed a new cyclic redundancy check (CRC) based message authentication which can detect any double-bit errors in a single message. The CRC codes based cryptographic hash functions are defined. A linear feedback shift register (LFSR) is used to efficiently implement the CRC encoding and decoding. The message authentication algorithm outputs an authentication tag based on a secret key and the message.

Fan, Gong, Du, Li, and Yang (2018), proposed a revocation method in the Radio Frequency Identification (RFID) secure authentication scheme in 5G use cases. A hash function and a random number are used to generate the corresponding module through a typical challenge-response mechanism. The reader contains a pseudo-random number generator (PNG) and the server holds a hash function database. The server establishes a tag record for each legitimate tag and a group of corresponding application records. After receiving the authentication request, the tag generates the second random number and calculates two hash authentication messages which are used to determine whether to revoke or to certify the application. The security and complexity results are presented, which show that the proposed scheme has a higher level of security and the same level of complexity compared with existing ones.

Zhang, Wang, Ye, and Lin (2021) proposed a light-weight and robust security-aware (LRSA) data transmission protocol in an mobile-health system utilizing certificate-less generalized signcryption (CLGSC) technique, The anonymous and mutual authentication is implemented between

International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 10 Oct. 2022, pp: 439-451 www.ijaem.net ISSN: 2395-5252

the client and the physician in a wireless body area network to protect the privacy of both the data source and the intended destination. A certificate-less signature algorithm is applied to the source client data before it is sent out. The source data identity can only be recovered by the intended physician who has the private key. The cipher text should be decrypted after the source identity is recovered with the right session key. Therefore, even the private key is leaked out, without the session key, the ciphertext is still safe. On the other hand, by verifying the signcryption, the physician can authenticate the source client. The computational and communication overheads of the proposed CLGSC are compared with other four schemes. Simulation results show that the proposed CLGSC scheme has a lower computational overhead than the other four schemes.

Eiza, Ni, and Shi (2016) proposed a novel system model for a 5G-enabled vehicular network that facilitates a reliable, secure, and privacy-aware real-time video reporting service. This service is designed for participating vehicles to instantly report the videos of traffic accidents to guarantee a timely response from official vehicles and/or ambulances toward accidents. While it provides strong security and privacy guarantees for the participating vehicle's identity and the video contents, the proposed service ensures traceability of misbehaving participants through a cooperation scheme among different authorities.

B. Availability

Availability is a key metric to ensure the ultra-reliable communications in 5G. However, by emitting wireless noise signals randomly, a jammer can degrade the performance of the mobile users significantly and can even block the availability of services. Jamming is one of the typical mechanisms used by Denial-of-Service (DoS) attacks. Most of the anti-jamming schemes use the frequency-hopping technique, in which users hop over multiple channels to avoid the jamming attack and to ensure the availability of services.

Li, Kaur, and Andersen (2017) proposed a secret adaptive frequency hopping scheme as a possible 5G technique against DoS based on a software defined radio platform. The proposed bit error rate (BER) estimator based on physical layer information is applied to decide frequency blacklisting under DoS attack. Since the frequency hopping technique requires that users have access to multiple channels, it may not work efficiently for dynamic spectrum access users due to the high switching rate and high probability of jamming.

To reduce the switching rate and probability of jamming, Adem, Hamdaoui, and Yavuz (2018) proposed a pseudorandom time hopping anti-jamming scheme.The authors pointed out that the proposed time-hopping technique is a strong candidate for links in 5G wireless networks due to its good performance as well as its capability in providing jamming resilience with a small communication overhead. However, a pre-shared key is required for the time-hopping anti-jamming technique. Both frequency hopping and time hopping require a pre-shared key to determine the hopping sequence.

Considering the limited computational capabilities at certain nodes, Labib, Ha, and Saad, and Reed (2018) proposed a fusion centre is used to defend these nodes from a malicious radio jamming attack over 5G wireless networks. A non-cooperative Colonel Blotto game is formulated between the jammer and the fusion centre as an exercise in strategic resource distribution. The jammer aims to jeopardize the network without getting detected by distributing its power among the nodes intelligently. On the other hand, the fusion centre as a defender aims to detect such an attack by a decentralized detection scheme at a certain set of nodes. The fusion centre can allocate more bits to these nodes for reporting the measured interference. A hierarchical degree is assigned to each node based on its betweenness centrality. Once the attack is detected, the fusion centre will instruct the target node to increase its transmit power to maintain a proper (signal-to-noise ratio) SNR for normal communications. The simulation results show that error rate performance improves significantly with the fusion centre having more bits to allocate among the nodes. The proposed resource allocation mechanism outperforms the mechanism that allocates the available bits in a random manner.

C. Data Confidentiality

Data confidentiality service is commonly required to tackle eavesdropping attacks. This subsection discussed data confidentiality based on power control, relay, artificial noise, signal processing, and cryptographic methods.

D. Power Control

Power control for security aims to control the transmit power to ensure that the eavesdropper cannot recover the signal. Based on the most simple eavesdropping attack model with a single eavesdropper armed with a single antenna, Ghanem and Ara (2018) proposed a distributed algorithm to secure D2D communications in 5G, which allows two legitimate senders to select whether to cooperate

International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 10 Oct. 2022, pp: 439-451 www.ijaem.net ISSN: 2395-5252

or not and to adapt their optimal power allocation based on the selected cooperation framework. In the system model each user has a single antenna. A shared bi-directional link is presented for comparison. The distance between the legitimate transmitter and the eavesdropper is given a constraint to avoid distance attacks as the eavesdropper may have a better received signal quality on the transmitted message than the legitimate receiver. Simulation results show that achievable secrecy rates are improved by relaying data for each other. With the increase of distance between the transmitter and the receiver, the benefit from cooperation decreases and at some point non-cooperation could become more beneficial to the legitimate transmitter.

Bernardo and De Leon (2019) presented an optimization model to minimize the total power consumption of the network while satisfying the security level against eavesdroppers by assuming that the base station (BS) has imperfect channel knowledge on the eavesdroppers. The simulation results show that a highly dense network topology can be an effective solution to achieve high capacity, and reliable and secure communication channels.

D. Relay

Cooperation with relay can be used to help the sender to secure the signal transmission.

Nguyen, Duong, Ngo, Velkov, and Shu (2019) proposed two relay selection protocols, namely optimal relay selection (ORS) and partial relay selection (PRS), to secure an energy harvesting relay system in 5G wireless networks. The system model which consists of multiple relay nodes and assumes there is no direct link between sender and receiver. The power beacon is armed with multiple antennas, which can be used to strengthen the energy harvested. The ORS chooses the aiding relay to maximize the secrecy capacity of the system by assuming the source has full knowledge of channel state information (CSI) on each link. The PRS selects the helping relay based on partial CSI. The system includes a power beacon with multiple antennas, several relays, a destination node and an eavesdropper with a single antenna. Two energy harvesting scenarios that aim to maximize energy harvesting for source and selected relay are investigated. The analytical and asymptotic expressions of secrecy outage probability for both relay selections protocols are presented. The numerical results show that ORS can significantly enhance the security of the proposed system model and can achieve full secrecy diversity order while PRS can only achieve unit secrecy diversity order regardless of the energy harvest strategies. PRS that maximizes energy harvesting for relay strategy has a better secrecy performance than the one based on the maximizing energy harvesting for source. Moreover, the results show that the secrecy performance of the considered system is impacted significantly by the duration of energy harvest process.

To tackle the complexity issue of relay selection in 5G largescale secure two-way relay amplify-and-forward (TWR-AF) systems with massive relays and eavesdroppers, Zhang, Ge, Li, Gong, and Ding (2021) proposed a distributed relay selection criterion that does not require the information of sources signal to noise ratio (SNR), channel estimation, or the knowledge of relay eavesdropper links. The proposed relay selection is done based on the received power of relays and knowledge of the average channel information between the source and the eavesdropper. The system model includes two source nodes, a number of legitimate relay nodes and multiple passive eavesdroppers. Each node has a single antenna. The cooperation of eavesdroppers is considered. In TWR-AF, the received signals from the two sources at the eavesdropper in each time slot are overlapped, where one source's signal acts as the jamming noise. The analytical results show that the number of eavesdroppers has a severe impact on the secrecy performance. The simulation results show that the performance of the proposed low-complexity criterion is very close to that of the optimal selection counterpart.

Considering eavesdroppers and relay with single and multiple antennas, Xu, Ren, Song, and Du (2019) studied the transmission design for secure relay communications in 5G networks by assuming no knowledge on the number or the locations of eavesdroppers. The locations of eavesdroppers form a homogeneous Poisson Point Process. A randomize-and-forward relay strategy is proposed to secure multi-hop communications. Secrecy outage probability of the two-hop transmission is derived. A secrecy rate maximization problem is formulated with a secrecy outage probability constraint. It gives the optimal power allocation and code word rate. Simulation results show that the secrecy outage probability can be improved by equipping each relay with multiple antennas. The secrecy throughput is enhanced and secure coverage is extended by appropriately using relaying strategies.

E. Artificial Noise

Artificial noise can be introduced to secure the intended signal transmission. With the artificial-noise aided multi-antenna secure transmission under a stochastic geometry framework, Wang, Zheng, Yuan, Towsley, and Lee (2019) proposed an

International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 10 Oct. 2022, pp: 439-451 www.ijaem.net ISSN: 2395-5252

association policy that uses an access threshold for each user to associate with the base station BS so that the truncated average received signal power beyond the threshold is maximized and it can tackle randomly located eavesdroppers in a heterogeneous cellular network. The tractable expression of connection probability and secrecy probability for a randomly located legitimate user are investigated. Under the constraints of connection and secrecy probabilities, the network secrecy throughput and minimum secrecy throughput of each user are presented. Numerical results are presented to verify the analytical accuracy.

Assuming the sender is armed with multiple antennas Wang, Zheng, and Yin (2019) proposed an artificial noise transmission strategy to secure the transmission against an eavesdropper with a single antenna in millimetre wave systems. Millimetre wave channel is modelled with a ray cluster based spatial channel model. The sender has partial CSI knowledge on the eavesdropper. The proposed transmission strategy depends on directions of the destination and the propagation paths of the eavesdropper. The secrecy outage probability is used to analyse the transmission scheme. An optimization problem based on minimizing the secrecy outage probability with a secrecy rate constraint is presented. To solve the optimization problem, a closed-form optimal power allocation between the information signal and artificial noise is derived. The secrecy performance of the millimetre wave system is significantly influenced by the relationship between the propagation paths of destination and eavesdropper. The numerical results show that the secrecy outage is mostly occurred if the common paths are large or the eavesdropper is close to the transmitter.

Zappone, Lin, and Jorswieck (2019) proposed an optimization problem formulated to maximize the secrecy by assuming imperfect CSI of eavesdropper at transmitter. The system is modelled with one legitimate transmitter with multiple antennas, and one legitimate receiver and one eavesdropper, each with a single antenna. Artificial noise is used at the transmitter. Resource allocation algorithms are used to solve the optimization problem with correlation between transmit antennas. With the combination of fractional programming and sequential convex optimization, the first order optimal solutions are computed with a polynomial complexity.

F. Signal Processing

Besides the three methods above to provide data confidentiality Chen, Zhu, Li, Wei, Leung, and Yang (2019) proposed an original symbol phase rotated (OSPR) secure transmission scheme to defend against eavesdroppers armed with unlimited number of antennas in a single cell. Perfect CSI and perfect channel estimation are assumed. The BS randomly rotates the phase of original symbols before they are sent to legitimate user terminals. The eavesdropper cannot intercept signals, only the legitimate users are able to infer the correct phase rotations recover the original symbols. Symbol error rate of the eavesdropper is studied, which proves that the eavesdropper cannot intercept the signal properly as long as the base station is equipped with a sufficient number of antennas.

Considering multiple eavesdroppers Qin, Liu, Ding, Gao, and Elkashlan (2019) analysed the secure performance on a large-scale downlink system using non-orthogonal multiple access (NOMA). The system considered contains one base station (BS), multiple NOMA users and eavesdroppers randomly deployed in a finite zone. A protected zone around the source node is adopted for enhancing the security of the random network. Channel statistics for legitimate receivers and eavesdroppers and secrecy outage probability are presented. User pair technique is adopted among the NOMA users. Analytical results show that the secrecy outage probability of NOMA pairs is determined by the NOMA users with poorer channel conditions. Simulation results show that secrecy outage probability decreases when the radius of the protected zone increases and secrecy outage probability can be improved by reducing the scope of the user zone as the path loss decreases.

G. Cryptographic Methods

Cryptographic methods are also used for implementing data confidentiality by encrypting data with secret keys. Asymmetric cryptography can be applied to key distributions. To reduce the cost of encryption, symmetric cryptography is adopted for data encryption.

Eiza, Ni, and Shi (2019) proposed a participating vehicle can send its random symmetric key, which is encrypted using public key. The symmetric key is used to encrypt the message between participating vehicles. A one-time encryption key is also encrypted by a public key. The one-time encryption key is used to encrypt the video. Zhang, Wang, Ye, and Lin (2021) proposed an initial symmetric session key is negotiated between the client and a physician after they establish the client/server relationship. The symmetric key is then used for the data transmission between the client and the physician.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 10 Oct. 2022, pp: 439-451 www.ijaem.net ISSN: 2395-5252

I. Key Management

Key management is the procedure or technique that supports the establishment and maintenance of keying relationships between authorized parties, where the keying relationship is the way common data is shared between communication entities. The common data can be public or secret keys, initialization values, and other non-secret parameters.

To provide flexible security, Sedidi and Kumar (2019) proposed three novel key exchange protocols, which have different levels of computational time, computational complexity, and security, for device-to-device (D2D) communications based on the Diffie-Hellman (DH) scheme. The threat analysis of all three proposed protocols under common brute force and MITM attacks is presented. Performance study is provided for the proposed protocols to evaluate the confidentiality, integrity, authentication, and nonrepudiation of security services based on theoretical analysis. The analysis proves that the proposed protocols are feasible with reasonable communication overhead and computational time.

For D2D group use cases, Elrahman, Khedher, and Afifi (2018) proposed a group key management (GKM) mechanism to secure the exchanged D2D message during the discovery and communication phases is proposed. There are five security requirements in the proposed GKM, namely forward secrecy (users that have left the group should not have access to the future key), backward secrecy (new users joining the session should not have access to the old key), collusion freedom (fraudulent users could not deduce the current traffic encryption), key independence (keys in one group should not be able to discover keys in another group), and trust relationship (do not reveal the keys to any other part in the same domain or any part in a different domain). ID-based cryptography (IBC) scheme based on Elliptic Curve Cryptography (ECC) for securing multicast group communications is presented. The steps of the proposed protocol include secret key generation, elliptic curve digital signature algorithm, signature verification, group formation procedure, and key generation, join process, and leave process. The master key and private key generations are based on IBC and ECC schemes. The overhead for communications, re-keying message, and key storage are assessed. The weakness of the IBC scheme and the ways of creating and using GKM are compared. The overall performance comparisons show that the proposed GKM has an enhancement in both the protocol complexity and security level compared with other works.

ECC was also adopted for the proposed LRSA protocol by Zhang, Wang, Ye, and Lin in 2021. The network manager generates a partially private and partially public key for the client and the physician after the registration. And once the client and the physician establish the client/server relationship, an initial systematic session key can be set up for the data transmission.

J. Privacy

5G wireless networks raise serious concerns on privacy leakage when supporting more and more vertical industries such as m-health care and smart transportation. The data flows in 5G wireless networks carry extensive personal privacy information such as identity, position, and private contents. In some cases, privacy leakage may cause serious consequences. Depending on the privacy requirements of the applications, privacy protection is a big challenge in 5G wireless networks. A number of existing studies have considered location privacy and identity privacy.

Regarding location privacy, Farhang, Hayel, and Zhu (2018) proposed a decentralized algorithm for access point selection based on a matching game framework, which is established to measure the preferences of mobile users and base stations with physical layer system parameters.to protect the location and preferences of users that can be revealed with associated algorithms in heterogeneous networks (HetNets). Differentially private Gale-Shapley matching algorithm was developed based on differential privacy. Utilities of mobile users and access points were proposed based on packet success rate. Simulation results show that the differentially private algorithm can protect location privacy with a good quality of service based on utility of the mobile users. Ulltveit-Moe, Oleshchuk, and Kien (2017) proposed a location-aware mobile intrusion prevention system (mIPS) architecture with privacy enhancement. The authors presented the mIPS requirements, possible privacy leakage from managed security services.

In the study by Zhang, Wang, Ye, and Lin (2021), contextual privacy is defined as the privacy of data source and destination. The identity of the source client is encrypted by a pseudo identity of the source client with the public key of the physician using certificate less encryption mode. Meanwhile, the identity of the intended physician is also encrypted with the public key of the network manager. Through these two encryption steps, the contextual privacy can be achieved.

For the proposed reporting service in the study by Eiza, Ni, and Shi (2019), privacy is an essential requirement to gain acceptance and participation of people. The identity and location information of a vehicle should be preserved against illegal tracing. Meanwhile, a reporting vehicle should be able to reveal its identity to the authorities for special circumstances. The pseudonymous authentication schemes are applied to achieve the conditional anonymity and privacy.

V. THE NEED FOR A NEW TRUST MODELS

With the advanced services offered by 5G wireless networks, not only new types of functions are provided to people and society, but also new services are applied to vertical industries, such as smart grid, smart home, vehicular networks and mobile-health networks, etc.

Trust models vary among different use cases with emerging new actors in 5G wireless networks. For some applications, there are various types of devices connected to the same network, some of which may be used only to gather data and some of which may be used only to access internet. The trust requirements of different devices are therefore different.

For different security demands, the corresponding trust model may have different security requirements. As an example, a high security level demand may require both password and biometric authentication simultaneously. With the massive number of devices over 5G wireless networks, new trust models are needed to improve the performance of security services such as IoT use cases authentication. These new trust models will affect the security services.

VI. CONCLUSION

5G wireless networks are expected to provide advanced performance to enable many new applications. In this paper, we presented a comprehensive study on recent development of 5G wireless security. The current security solutions mainly based on the security services provided such as authentication, availability, data confidentiality and key management. Many new security aspects in 5G are expected due to the applications of technologies such as HetNets, D2D, massive MIMO, SDN and IoT. Some existing literature on security of these technologies has been summarized. It is expected that this study will be helpful in addressing the security concerns from both industry and academia to provide research directions for implementing security on 5G wireless networks.

ACKNOWLEDGMENT

We would like to sincerely appreciate the anonymous reviewers for their comments which has improved the work.

REFERENCES

[1]. 3GPP. (2021). 5G Release https://www.3gpp.org/release-16
[2]. 3GPP. (2021). About 3GPP. https://www.3gpp.org/about-3gpp
[3]. 5G Americas. (2018). The evolution on security in 5G. https://www.5gamericas.org/the-evolution-of-security-in-5g-2/
[4]. 5G Americas. (2020). Security considerations for the 5G era. https://www.5gamericas.org/security-considerations-for-the-5g-era/
[5]. Abdulghaffar, A., Mahmoud, A., Abu-Amara, M., & Sheltami, T. (2021). Modeling and evaluation of software defined networking based 5G core network architecture. IEEE Access, 9, 10179-10198.
[6]. Afolabi, I., Taleb, T., Samdanis, K., Kasentini, A., & Flinck, H. (2018). Network slicing and softwarization: A survey on principles, enabling technologies, and solutions. IEEE Communications Surveys Tutorials, 20(3), 2429-2453.
[7]. Akyildiz, I., Kak, A., & Nie, S. (2020). 6G and Beyond: The Future of Wireless Communications Systems. IEEE Access, 8, 133995-134030.
[8]. Dahlman, E., Parkyall, S., & Skold, J. (2020). 5G NR: The next generation wireless access technology. Elsevier Science.
[9]. Foukas, X., Patounas, G., Elmokashfi, A., & Marina, M. (2017). Network slicing in 5G: Survey and challenges. IEEE Communications Magazine, 55(5), 94-100.
[10]. Idowu-Bismark, O., Kennedy, O., Idachaba, F., & Atayero, A. A. (2018). Primer on MIMO Detection Algorithms for 5G Communication Network. International Journal on Communications Antenna and Propagation (IRECAP), 8(3), 194-205.
[11]. IT Pro Portal. (2019). Old vulnerabilities could majorly impact 5G security. https://www.itproportal.com/news/old-vulnerabilities-could-majorly-impact-5g-security/
[12]. Kaloxylos, A. (2018). A survey and an analysis of network slicing in 5G networks.

IEEE Communications Standards Magazine, 2(1), 60-65.

[13]. Koumaras, H., Tsolkas, D., Gardikis, G., Gomez, P., Frascolla, V., Triantafyllopoulou, D., & Bosneag, A. (2018). 5genesis: The genesis of a flexible 5G facility. IEEE 23rd international workshop on computer aided modeling and design of communication links and networks (camad), 1-6.

[14]. Laghrissi, A., & Taleb , T. (2018). A survey on the placement of virtual resources and virtual network functions. IEEE Communications Surveys & Tutorials, 21(2), 1409-1434.

[15]. Lin, Y.B., Tseng, C.C., & Wang, M.H. (2021). Effects of transport network slicing on 5G applications. Future Internet, 13(3), 69.

[16]. Prabakaran, D., Nizar, S. M., & Kumar, K. S. (2021). Software-defined network (SDN) architecture and security considerations for 5G communications. In Design methodologies and tools for 5G network development and application, 28-43.

[17]. Selvi, K., & Thamiselvan, R. (2021). Dynamic resource allocation for SDN and edge computing based 5G network. Third international conference on intelligent communication technologies and virtual mobile networks (icicv), 19-22.

[18]. Su, R., Zhang, D., Venkatesan, R., Gong, Z., Li, C., Ding, F., & Zhu, Z. (2019). Resource allocation for network slicing in 5G telecommunication networks. A survey of principles and models. IEEE Network, 33(6), 172-179.

[19]. Tataria, H., Shafi, M., Molisch, A., Dohler, M., Sioland, H., & Tufvesson, F. (2021). 6G Wireless Systems: Vision, Requirements, Challenges, Insights, and Opportunities. Proceedings of the IEEE, 1-34.

[20]. Huawei. (2015). 5G Security: Forward Thinking. HUAWEI WHITE PAPER.

[21]. Wang, H., Zheng, T., Yuan, J., Towsley, D., & Lee, M.H. (2019). Physical Layer Security in Heterogeneous Cellular Networks. IEEE Transactions on Communications, 64(3), 1204-1219.

[22]. Ulltveit-Moe, N., Oleshchuk, V.A., & Kien, G.M. (2017). Location-aware mobile intrusion detection with enhanced privacy in a 5G context. Wireless Personal Communications, 57(3), 317-338.

[23]. Chen, B., Zhu, C., Li, W., Wei, J., Leung, V.C., & Yang, L.T. (2019). Original Symbol Phase Rotated Secure Transmission Against Powerful Massive MIMO Eavesdropper. IEEE Access, 4, 3016-3025.

[24]. Rani, P. T., Pritee, S. U., Deepak, S.D, & Umesh, J. T. (2020). A literature review on: wireless technologies from 0g to 7g. Ire Iconic Research and Engineering Journals, 4(6).

[25]. Adem, N., Hamdaoui, B., & Yavuz, A. (2018). Pseudorandom Time-Hopping Anti-Jamming Technique for Mobile Cognitive Users. IEEE Globecom Workshops (GC Wkshps), 1-6.

[26]. Labib, M., Ha, S., Saad, W., & Reed, J.H. (2018). A Colonel Blotto Game for Anti-jamming in the Internet of Things. IEEE Global Communications Conference (GLOBECOM), 1-6.

[27]. Duan, X., & Wang, X. (2019). Fast Authentication in 5G HetNet through SDN Enabled Weighted Secure-Context-Information Transfer. IEEE International Conference on Communications (ICC), 1-6.

[28]. Eiza, M.H., Ni,W., & Shi, Q. (2016). Secure and Privacy-Aware Cloud-Assisted Video Reporting Service in 5G Enabled Vehicular Networks. IEEE Transactions on Vehicular Technology, 65(10), 7868-7881.

[29]. Zhang, A., Wang, L., Ye, X., & Lin, X. (2021). Light-weight and Robust Security-Aware D2D-assist Data Transmission Protocol for Mobile-Health Systems. IEEE Transactions on Information Forensics and Security, 12(3), 662-675.

[30]. Dubrova, E., Naslund, M., & Selander, G. (2018). CRC-Based Message Authentication for 5G Mobile Technology. IEEE Trustcom/BigDataSE/ISPA, 1186-1191.

[31]. Farhang, S., Hayel, Y., & Zhu, Q. (2018). PHY-Layer Location Privacy Privacy-Preserving Access Point Selection Mechanism in Next-Generation Wireless Networks. IEEE Conference on Communications and Network Security (CNS), 263-271.

[32]. Elrahman, E.A., Khedher, H.L., & Afifi, H. (2018). D2D Group Communications Security. International Conference on Protocol Engineering (ICPE) and International Conference on New Technologies of Distributed Systems (NTDS), 1-6.

[33]. Zappone, A., Lin, P.H & Jorswieck, E. (2019). Artificial-noise-assisted energy-efficient secure transmission in 5G with imperfect CSIT and antenna correlation. IEEE 17th International Workshop on Signal Processing Advances in Wireless Communications (SPAWC), 1-5.

[34]. Abualhaol, I., & Muegge, S. (2019). Securing D2D Wireless Links by Continuous Authenticity with Legitimacy Patterns. 49th Hawaii International Conference on System Sciences (HICSS), 5763-5771.

[35]. Fan, K., Gong, Y., Du, Z., Li, H & Yang, Y. (2018). RFID Secure Application Revocation for IoT in 5G. IEEE Trustcom/BigDataSE/ISPA, 175-181.

[36]. Li, Y., Kaur, B., & Andersen, B. (2017). Denial of service prevention for 5G. Wireless Personal Communications, 57(3), 365-376.

[37]. Ghanem, S.A., & Ara, M. (2018). Secure Communications with D2D cooperation. Communications, Signal Processing, and their Applications (ICCSPA), 1204-1219.

[38]. Luo, Y., Cui, L., Yang, Y & Gao, B. (2018). Power control and channel access for physical-layer security of D2D underlay communication. International Conference on Wireless Communications & Signal Processing (WCSP), 1-5.

[39]. Bernardo, N.I., & De Leon, F. (2019). On the trade-off between physical layer security and energy efficiency of massive MIMO with small cells. International Conference on Advanced Technologies for Communications (ATC), 135-140.

[40]. Nguyen, N.P., Duong, T.Q., Ngo, H.Q., Velkov, Z.H., & Shu, L. (2019). Huawei White Paper Secure 5G Wireless Communications: A Joint Relay Selection and Wireless Power Transfer Approach. IEEE, 4, 3349-3359.

[41]. Zhang, C., Ge, J., Li, J., Gong, F., & Ding, H. (2018). Complexity-Aware Relay Selection for 5G Large-Scale Secure Two-Way Relay Systems. IEEE Transactions on Vehicular Technology, 66(6), 5461-5465.

[42]. Xu, Q., Ren, P., Song, H., & Du, Q. (2019). Security Enhancement for IoT Communications Exposed to Eavesdroppers With Uncertain Locations. IEEE Access, 4, 2840-2853.

[43]. Ju, Y., Wang, H.M., Zheng, T.X., & Yin, Q. (2019). Secure transmission with artificial noise in millimeter wave systems. IEEE Wireless Communications and Networking Conference, 1-6.

[44]. Qin, Z., Liu, Y., Ding, Z., Gao, Y., & Elkashlan, M. (2019). Physical Layer Security for 5G Non-orthogonal Multiple Access in Large-scale Networks. IEEE International Conference on Communications (ICC), 1-6.

[45]. Sedidi, R & Kumar, A. (2019). Key Exchange Protocols for Secure Device-to-Device (D2D) Communication in 5G. Wireless Days (WD), 1-6.