5th Generation Wireless Networks Security: Challenges and Solutions

Bashayer Ahmed Bin Siddiq
s44380317@st.uqu.edu.sa
Umm Al-Qura'a University, Computer Sciences and information Systems College, Makkah, KSA

Summary
In reason of the high capacity and low latency, the 5G wireless networks used nowadays in many of life applications such as: remote surgery and guiding vehicle. The high requirements of 5G networks makes it more vulnerable for security threats and attacks. This paper presents some challenges faced by 5G networks and presets some of the security solutions.

Keywords:
Security, 5th Generation, Wireless Network

1. Introduction

Beyond the existing 4th generation, or 4G International Mobile Telecommunications (IMT)- Advanced Systems, there is 5th generation mobile wireless communication system. The 5G is the evolution of services provided by 4G cellular network with more fulness, higher bandwidth channels to absorbs more users and device to device communication capabilities. However, the increasing of characteristics arises the security risks in the network, such as the diversity of implicit access in channel make the network more likely to contains hackers and snooping operations. As well as this diversity of interconnected devices will be mobile and dynamically communicated [1]. Another thing is the open architecture of the IP-based 5G system make it susceptible to unexpected threats [1]. In result, 5G wireless networks require security improvements in the respect to the 4th generation. One of these improvements is the flexibility and availability of the network with the threats caused by signals and malicious overload. Furthermore, some use cases of 5G require a special security design with low latency [2]. Nevertheless, one of the design goals is the capacity and data rates which needed in the use cases such as, virtual reality, augmented reality, high-definition screening which applied during today's life in vehicular communications and telesurgery [3]. Hence, every application that connected to 5G networks may face one of the security challenges that stipulated by Next Generation Mobile Networks (NGMN) as follows [4]:

- Flash network transit: elevated issues of end-user machines in addition to novel Internet of things (IoT)
- Protection applied on radio fronts: the encryption keys of radio waves fronts transmitted among unsafe routings.
- Safety scale: the user data has no cryptographic vindication of data safety.
- Delegated protection in the network: the restrictions of service-driven applied on the protection framework resulting into elective utilization of protection measurements.
- Peregrination of protection: the attributes of user-protection are not updated when it moves around different network factors.
- Denial of Service (DoS) attacks on the structure: a clear network supervision objects and unencrypted routing.
- Breaking in signals: consistency expanding supervision systems, for instance None-Access Stratum (NAS) coat of Third Partnership Project (3GPP) protocols.
- DoS attacks assault end-user appliances: no protection measurements applied on operating systems, programs, user devices, and information configuration.

This paper discusses the security of 5G wireless networks and its challenges classified based on Open Systems Interconnections (OSI) layer paradigm. The OSI is a regulation protocol for network communication using seven separated layers, that illustrated in table 1 [3].

As discussed previously, the 5G is used in many applications which leads to the importance of security in application of OSI. However, it is serious for industries or even individuals to be aware of the risks and threats in 5G. Furthermore, it is important for them know how to relive from security and privacy threats.

This paper organized as follow: part 2 presents the methodology of selecting the research papers, part 3 presents the security challenges of 5G networks, part 4 presents some solutions of 5G network and we conclude the paper at part 5.

Manuscript received June 5, 2022
Manuscript revised June 20, 2022
https://doi.org/10.22937/IJCSNS.2022.22.6.23

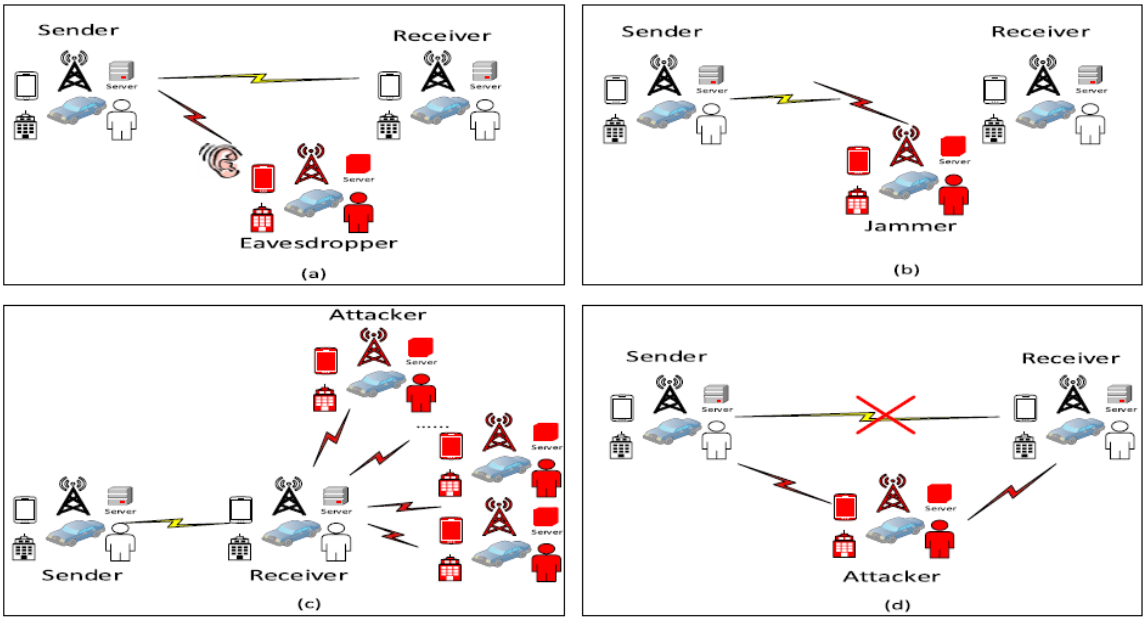

Figure 1 Attacks in 5G wireless networks (a). Eavesdropping; (b). Jamming; (c). DDoS; (d). MITM. *[2]*

2. Methodology

This paper aims to answers the following research questions:

- Had the counts of studies regarding the security challenges of 5th generation networks been growing during the last years?
- What are the 5th generation networks attacks and challenges?
- What are the solutions of increasing the security of 5th generation networks?

To process this research questions, this paper confesses the guidelines of Preferred Reporting Systematic Reviews Items and Meta-Analysis (PRSIMA) [5], which is a description methodological program for systematic literature review. The following sections demonstrates the eligibility criteria, data resources, study election and result.

Table 1 OSI Layers

Layer#	***Layer Name***
7	Application
6	Presentation
5	Session
4	Transport
3	Network
2	Data Link
1	Physical

2.1 Eligibility Criteria

This study demonstrates rival studies in journals in addition to conferences of three sciences databases which are: ScienceDirect, Google Scholar, and Association for Computing Machinery (ACM).

The chosen studies included the next criteria:

- Studies must be regarded to the security about 5th generation wireless network.
- Studies must include the solutions of security threats about 5G.

2.2 Data Resources

Each of the three electronic databases showed above has different studying fields. By the ease of searching process, ACM enables a sophisticated searching by selecting keywords in multiple fields and timeframe for released year. This paper choses studies released at English Language among 2015-2022. Furthermore, this study focused on the title and abstract at the initial phase. Since the keywords used for the search are taken from the research aims in addition to research questions. Hence, the chosen keywords contain “security”, “5G networks”, “attacks”, and “threats”.

2.3 Study election

The study election process contained due stages. At the initial phase, the papers which consist of at least due keywords in the studying areas was extracted. This for the first standard aforesaid in part 2.1. In situation that keywords identified, the chosen papers studied to review if they full under the second criteria in part 2.1. Furthermore, the papers which are unrelated to this study were rejected.

3. 5G Security Challenges

The wireless transmission nature is vulnerable to different malicious threats because of broadcast kind. This section will display the attacks that may face 5G networks such as: eavesdropping, jamming, Distributed Denial of service in addition to Denial of Service, and Man in the Middle Attack. Another thing is, there are multiple of security services provided by 5G which are: authentication, confidentiality, availability, and integrity.

3.1 Attacks

3.1.1 Eavesdropping and Traffic Analysis

In the situation of interception a message from others in an unintentional way by the receiver, that is called eavesdropping. The eavesdropping attack is shown in Figure 1 (a). The solution to assure the security against eavesdropping attack is the encryption of signals among radio channels. Thus, the encryption makes the eavesdropper cannot protest as a receiver of signals [2] [5].

Another type of passive attack is traffic analysis which means that the receiver protests the information transmitted such as location and identity of one of the communicated parts without recognizing the signals content [2].

The encryption technique depends on the using of a strong encryption algorithm to fight against eavesdropping. However, some technologies may assist the eavesdroppers in their attacks. The 5G wireless network implement Heterogeneous Networks HetNet to raise the difficulty on the eavesdroppers. HetNet is the network with devices that contains operating systems and protocols with big differences for each device [6].

3.1.2 Jamming

Jamming is an active attack which obstruct connection of two valid users. A designed interface generated by malicious side to damage the connection between the valid users [2]. Jamming attack is shown is Figure 1(b). When talking about 5G wireless connection, it uses the radio interface to control channels which may disrupted by jamming attackers. Furthermore, the attacker uses high powered attacks to close the control channels which resulting to encumber the frequency bands [7].

Some of the techniques for secure communication to prevent jamming attacks at physical coat are direct sequence spread spectrum (DSSS) and frequency hopping spread spectrum (FHSS). These methods work by signals pervasion through boarder spectral bandwidth [2].

3.1.3 DoS and DDoS

This type of attacks overstrains the communicated resources. As shown in Figure 1(c), these attacks are active attacks and can be defect the 5G network at different layers. In addition, these attacks can descent a very large numerical devices from accessing the 5G networks [2]. DoS and DDoS threatening the 5G networks at different levels which are: signals, user management, backup frameworks, radio sources, logical and physical sources [8].

3.1.4 MITM

As shown in Figure 1(d), this type of attack, the attacker can manage the communication among duo valid users and modify, protest and exchange the messages between them. The attacker can impose the valid user to make a communication channel for sham base transceiver station, this is called mendacity base station based on MITM offensive [9]. In order to prevent this attack a reciprocal authentication used in the communication between the base station with mobile appliance [2].

3.2 Security Services

3.2.1 Authentication

Authentication is required to prevent the previous attacks which threatening 5G wireless networks. The authentication consist entity authentication as well as message authentication. Apart from that, entity authentication occur when a contacting side is alleges that he is the right user. According to the cellular networks, the reciprocal authentication implemented after the duo contacted sides create a connection through user kit and mobility management entity (MME). Hence, the 5G demands the authentication between other third entities like service providores in addition to user kit and MME. An Authentication and Key Agreement (AKA) protocol is applied for the sake of authenticating the communicated entities in the network and setting up the keys to protect the data follow in the network [10]. However, the released version of AKA by 3GPP has many securities concerned in 5G regarding about user localization, weakness of activity, active attackers' effect and roaming malicious. The updated

Table 2: Summery of some existing security solutions in 5G *[7]*

Security solution	Target component	Technological impact								Privacy
		MEC	Blockchain	AI	SDN	NFV	CPS	Cloud	Cryptography	
ENDER	Centralized server	No	No	No	No	No	Yes	Yes	No	Yes
SIPDAS attack simulator	Physical cloud	No	No	No	No	No	Yes	Yes	No	No
APG-BFT algorithm	Centralized server	No	Yes	No	No	No	No	No	No	Yes
Deep learning framework	Wireless Android-based devices	No	No	Yes	No	No	No	No	No	No
Machine learning-based algorithm	Physical layer authentication	No	No	Yes	No	No	No	No	No	Yes
Elliptic-ElGamal-based authentication scheme	Secret key-based authentication	No	No	No	No	No	No	No	Yes	Yes
SDN-guard	Centralized server	No	No	No	Yes	Yes	No	Yes	No	Yes
Blood filter method	Fog layer	No	No	No	Yes	Yes	No	No	No	Yes
NFV method	Edge computing	No	No	No	Yes	Yes	No	Yes	No	Yes
SDN-5G	Centralized server	No	No	No	Yes	No	No	No	Yes	Yes
Deep Q-networklearning	Edge server	Yes	No	No	No	No	No	No	No	Yes
SDN-SC	Core network	No	No	Yes	Yes	No	No	No	No	No

version of AKA protocol proposed in [10] which resolve the vulnerabilities 5G networks when it implement this protocol.

Then there is the message authentication which is a substantial requirement of security in 5G due to the increasing of 5G applications [2]. The research [11] proposed Cyclic Redundancy Check (CRC) for 5G message authentication that discover the virulent error but it is excluding bandwidth increasing.

3.2.2 Confidentiality

Confidentiality covers two portions, first is data confidentiality and privacy. Data confidentiality is the meaning of limitation of data access to desired users in order to protect data transference in addition to the blocking of the unauthorized users to access the data. Privacy means that blocking valid users to reach their information [2]. Privacy protection is an important aspect related to 5G due to the using of sensitive information, e.g., sender/receiver location which used in many 5G applications such as: vehicle routing and health monitoring [novel].

To secure the data confidentiality cryptography is used to prevent the attacker from eliciting any valuable information [2]. When talking about 5G, the encryption materials managed using a Universal Subscriber Identity Module (USIM). In USIM, any user kit assigned to an identifier that named Subscription Permanent Identifier (SUPI) which globally unrivalled. This identifier and other participated items are integrity protected in the USIM. In the primary authentication, the user must demonstrate its identity by forwarding its identifier. This SUPI is concealing with the public key from base station and produce a tentative identifier which called Subscription Concealed Identifier SUCI. This identifier will be conveyed to home network to authenticate user identity. The home network contains Subscription Identifier De-Concealing Function (SIDF) which keep a proper private key. This identifier will hide the SUCI which return a specified SUPI then there is a user identification [12]. However, the 5G uses elliptic curve integrated encryption schemes (ECIESs) in concealment process [13]. The concealment process illustrated in [13].

3.2.3 Availability

Availability is the meaning of the valid users can access the service at anytime and anywhere they need. Availability detects how powerful the system when encounter any attacks which detect the performance of 5G networks [2]. The famous attack in the availability is Denial of Service attack [14]. However, to defense against DoS attacks a proposed scheme called IEWA in [2]. Apart from that, the researcher analyzed the security improvement of the scheme according to steady-state availability and it is increased by 5 precent.

3.2.4 Integrity

Integrity means the preventing of information from modification or alteration by active attacks caused by unauthorized entities. When talking about 5G, 5G has the objective to provide the connection for anyone in anytime and anyplace, in order to shore implementations that react

as individuals. Furthermore, the data integrity is the security requirement in certain application [2] [15].

4. Solutions of 5G security

This section will discuss solutions that protect 5G wireless network systems. The major security solutions for 5G networks are cryptography and physical layer security (PLS) [16]. However, the security of 5G depend on the strength of encryption algorithm which implemented using machine learning-based algorithm. The machine learning-based algorithms resolve the spoofing attacks in 5G networks by authenticate the communication at physical layer [7].

To understand PLS, two equations must be recognized that used to estimate the security performance. The first equation is secrecy capacity, and it is calculated as [17]:

$$Cs = Cm - Ce; \quad (1)$$

Cm: the main channel capacity for a valid user,
Ce: the channel capacity for eavesdropper [18].
The secrecy outage probability is determined by instant secrecy space which is the minimum goal of secrecy rate *RT*, which indicate that *RT* must be less than 0, and:

$$POUT\ (RS) = P\ (Cs < RT)\ ; \quad (2)$$

As well the previous equations in addition to consumed power, the secrecy EE is determined by the proportion among the obtained secrecy rate of the application with the related wasted energy [19].

Table 2 shows some security solutions for 5G networks.

Deep learning framework is designed to qualify jamming attacks which depend on AI-based deep learning. Some proposed deep learning algorithms learns the desired characteristics from diverse wireless connected devices [20].

As some attacks prevented by cryptography-based models, the Elliptic-ElGamal based authentication model is cryptography-based framework. This model is a create a pair of secret keys using Elliptic curve cryptography. In addition, it exchanges the key by users using ElGamal [21].

To defense against MIMA attacks, Blood Filter method is used, and it depends on two major aspects: flooding controller and Open v-Switch (OVS) to supervise the system.

In the other hand, there are some techniques used to secure 5G applications at physical layer. Fingerprints used to simplify user authentication process. Furthermore, Radio frequency identification (RFID) used as a single tag that secure multiple applications. In some situation of poor RFID should uses efficient encryption algorithms and authentication mechanisms [2]. In [22], an Attack and Failures Prediction Agent (AFPA) is proposed for 5G mobile networks. The proposed framework takes into the account the correlation between cyber-attacks and networks failures prediction.

These are some of the solutions of 5G security networks. There is much research conducted until now to solve 5G security challenges and improve the security of it.

5. Conclusion

The security of 5G wireless networks is an important topic in the recent years. Many of IoT application depends on 5G because it provides a high bandwidth and low latency.

In the future work of this paper is to conduct more studies and papers to analyze the security of 5G networks. Not only that, but we will also develop a secure framework for 5G security and study the security of different 5G applications.

References

[1] M. T. OMERANI Hanane, "4G and 5G: Security and privacy analysis".

[2] Y. Q. a. R. Q. H. DONGFENG FANG, "Security for 5G Mobile Wireless Networks," IEEE, 2017.

[3] A. B. S. A. P. K. M. C. S. SULLIVAN, "5G Security Challenges and Solutions: A Review by OSI Layers," IEEE, 2021.

[4] T. K. M. L. J. O. M. Y. A. G. Ijaz Ahmad, "Overview of 5G Security Challenges and Solutions," ResearchGate, 2018.

[5] D. Q. H. a. A. D. Areej Alsini, "Hashtag Recommendation Methods for Twitter and Sina Weibo:A Review," MDPI, 2021.

[6] M. L. X. L. Xiaoling Xu, "Key technology and application ofmillimeter wave communications for 5G: a survey," Springer, 2018.

[7] WIKIPEDIA, "Heterogeneous network," [Online]. Available: https://en.wikipedia.org/wiki/Heterogeneous_network. [Accessed 19 4 2022].

[8] S. R. S. K. S. M. M. S. A. E. A. T. W. K. Y. P. a. J. H. P. Jin Ho Park, "A Comprehensive Survey on Core Technologies and Services for 5G Security: Taxonomies, Issues, and Solutions," hcisijournal, 2021.

[9] G. NGMN Alliance, "5G Security Recommendations Package #1," 2016.

[10] N. D. a. V. L. M. Conti, "A survey of man in the middle attacks," IEEE, 2016.

[11] M. L. ,. K. J. M. AN BRAEKEN, "Novel 5G Authentication Protocol to Improve the Resistance Against Active Attacks and Malicious Serving Networks," IEEE, 2019.

[12] M. N. a. G. S. E. Dubrova, "CRC-based message authentication for 5G mobile technology," IEEE, 2015.

[13] T. J. Jing YANG, "An overview of cryptographic primitives for possible use in 5G and beyond," SCIENCE CHINA, 2020.

[14] M. B. Nicholas J H, "Secure human identification protocols," Springer, 2001.

[15] L. H. J. C. A. X. C. HAIOU HUANG, "An Authentication Scheme to Defend Against UDP DrDoS Attacks in 5G Networks," IEEE, 2019.

[16] Z. Z. D. Z. F. P. &. L. H. MA Zheng, "Key techniques for 5G wireless communications:network architecture, physical layer,and MAC layer perspectives," SCIENCE CHINA, 2015.

[17] Y. L. Jingfeng Zhao, "Supply chain security evaluation model and index system based on a 5G information system," Springer, 2021.

[18] P. M. S. S. A. L. J. F. H. M. G. P. S. S. H. C. G. M. P. José María Jorquera Valero, "Design of a Security and Trust Framework for 5G," Journal of Network and Systems Management, 2021.

[19] S. A. Alghamdi, "Novel trust-aware intrusion detection and prevention system for 5G," Springer, 2021.

[20] P.-H. L. a. E. J. A. Zappone, IEEE, 2016.

[21] Y. S. J. a. J. H. P. S. K. Singh, "A deep learning-based IoT-oriented infrastructure for secure smart City," Sustainable Cities and Society, 2020.

[22] Z. D. a. K. A. M. A. Abro, "A Lightweight elliptic-ElGamal-based authentication scheme for secure device-to-device communication," Future Internet, 2019.

[23] H. S.-C. M. Yosra Benslimen, "Attacks and failures prediction framework for acollaborative 5G mobile network," Springer, 2021.

Bashayer Bin Siddiq received the B.E. degree, from Umm Alqura Univ. in 2018. Her research interest includes Data Analysis, Machine Learning, and their application.