Review of 5th Generation Mobile Communication Technologies

Jatinder Kaur
Asst. Prof. ,GSSDGS Khalsa College,Patiala
jkkcp17@gmail.com

Abstract
5G is the next-generation network technology which promises exponentially higher bandwidth and lower latency to serve a wide range of consumer and commercial Internet of Things applications (IoT). With its next-generation network architecture, 5G has the ability to serve hundreds of new consumer and industrial applications. When speed and throughput are exponentially higher than current networks, the potential for 5G seem almost unlimited. 5G isn't only about "larger, faster, and better" networks. It's all about enabling a wide range of new services and use cases that affect almost every part of our life. However, 5G-enabled applications must be delivered securely in order to realise their full potential, and security challenges must be addressed at the network core from the start in order to protect both networks and customers. Some of the most fundamental concerns about 5G networks are discussed in this study. The paper can enlighten its readers on what is expected of 5G network, its architecture and what are the basic security issues involved in it.

Keywords: Heterogeneity, MIMO, SDN, NFV, MEC

1. Introduction

In the 1980s, the first generation of analog-based mobile communication systems was introduced, allowing people to et rid from from the shackles of the telephone line. In the 1990s, more efficient second-generation (2G) mobile communication systems based on digital communication were introduced, and personal mobile communications grew rapidly on a global scale after that. People can enjoy quicker mobile Internet experiences, such as video telephony, after 2000, after the deployment of 3G infrastructure. In 2010, the construction of a 4G commercial network based on Long Term Evolution (LTE) improved system capacity and user experience. By the third quarter of 2015, 364 commercial LTE networks had been launched, according to the Global TD-LTE Initiative (GTI). The 5th-Generation (5G) mobile communication technologies are emerging into research domains as the IMT-Advanced (IMT-A) systems are deployed around the world. The goal of 5G wireless networks is to deliver exceptionally high data rates and coverage by deploying dense base stations with enhanced capacity, greatly improved Quality of Service (QoS), and extremely low latency [1]. The 3rd Generation Partnership Project (3GPP), which produces international standards for all mobile communications, introduced the 3GPP specifications that underpin 5G network design. The International Telecommunications Union (ITU) and its partners define the requirements and schedule for mobile communication systems, with a new generation being defined every decade or so. In a series of releases, the 3GPP develops specifications for those requirements.

The “G” in 5G stands for “generation.” Beyond 4G LTE (long-term evolution) technology, which follows 3G and 2G, 5G technological design represents substantial advancements. 5G, like its predecessors, will have to coexist with existing networks. The network architecture of 5g mobile technology is a significant improvement over previous systems. Large cell-dense networks enable massive leaps in performance. Furthermore, compared to today's 4G LTE networks, the architecture of 5G networks provides better security. The desin considerations for a 5G network architecture that supports high-demand applications is complex. For example, there is no one-size-fits-all solution; a variety of applications necessitate data transport over long distances, enormous data volumes, or a mix of the two. To realise the whole 5G vision, 5G architecture must handle low, mid, and high-band spectrum — from licenced, shared, and private sources. As a result, 5G is designed to operate at radio frequencies ranging from below 1 GHz to extremely high frequencies known as "millimetre waves" (or mmWave). The signal can go further if the frequency is lower. The more data it can transport, the higher the frequency. The core of 5G networks consists of three frequency bands:

- The highest frequencies of 5G are delivered through 5G high-band (mmWave). These frequencies extend from 24 GHz to around 100 GHz. Because high frequencies have a hard time passing past obstructions, high-band 5G has a limited range. Furthermore, mmWave coverage is restricted, necessitating additional cellular infrastructure.
- The 5G mid-band works between 2 and 6 GHz and serves as a capacity layer for urban and suburban areas. The peak rates in this frequency band are in the hundreds of megabits per second.
- The 5G low-band runs at frequencies below 2 GHz and has a wide range of coverage. This band makes use of spectrum that is now accessible and in use for 4G LTE, effectively creating an LTE 5G architecture for 5G devices that are ready now. Low-band 5G's performance is so comparable to 4G LTE, allowing it to be used with current 5G devices.

Operators must address the power requirements of 5G in addition to spectrum availability and application requirements for distance vs. bandwidth issues, as the average 5G base station design requires more than double the power of a 4G base station.

With the advent of fifth-generation (5G) wireless networks, security threat vectors will be larger than ever before, with increased privacy concerns. As a result, it's critical to emphasise the security risks that exist not just owing to the wireless nature of mobile networks, but also in the future technologies that will be critical for 5G.

2. 5G Mobile Communication Technologies

5G cellular networks are based on a number of different technologies, which we review below:

- **Millimeter waves:** These are electromagnetic waves with a frequency range of 30 to 300 GHz, as opposed to the spectrum used for 4G LTE, which is below 6 GHz [2]. The microwave band is located slightly below the millimetre wave band, and it typically covers the frequencies of 3–30 GHz. Millimeter waves enable 5G networks to send enormous amounts of data over short distances and to utilise unlicensed frequencies, such as those used by Wi-Fi, without interfering with Wi-Fi networks, due to the utilisation of tiny cells to complement existing cellular networks.
- **Small cells:** These cells are portable base stations that supplement traditional macro cells by enhancing network capacity on demand and offering extended coverage. Small cells also improve energy efficiency due to the shorter transmitter-receiver distance [3]. Their primary application is in dense environments such as stadiums and indoors. As a result, 5G networks will rely on a complex architecture that includes macro and small ultra dense cells. Small cells' portability will allow for dynamic infrastructure.
- **Massive MIMO:** Massive multiple-input, multiple-output, or massive MIMO, is an expansion of MIMO in which antennas at the transmitter and receiver are grouped together on a greater scale to improve throughput and spectrum efficiency. A 128-antenna array in a 64-transmit/64-receive configuration is an example of large MIMO. Massive MIMO

improves spectral efficiency[4] in two ways: (a) by allowing a base station (BS) to connect with numerous devices at the same time, frequency, and location, and (b) by permitting multiple data streams between the BS and each device.

- **Beam forming:** Beam forming is another breaktrough technology crucial for 5G's success. Signals from traditional base stations were broadcast in many directions, regardless of the location of targeted users or devices. Signal processing algorithms can be used to determine the most efficient transmission path to each user, while individual packets can be sent in multiple directions and choreographed to reach the end user in a predetermined sequence, using multiple-input, multiple-output (MIMO) arrays with dozens of small antennas combined in a single formation. With 5G data transmission occupying the millimetre wave, free space propagation loss, proportional to the smaller antenna size, and diffraction loss, inherent to higher frequencies and lack of wall penetration, are significantly greater. The smaller antenna size, on the other hand, allows far larger arrays to fit into the same physical space. Massive beam formation to accommodate the challenges of 5G bandwidth becomes more realistic with each of these smaller antennas potentially reassigning beam forming many times per millisecond. With massive MIMO, narrower beams can be achieved with a higher antenna density in the same physical space, allowing for higher throughput. It is a technology that concentrates a wireless signal on a single receiving device rather than broadcasting it in all directions. It is, in other words, a method of directing the majority of signals generated by an array of transmitting antennas in a desired angular direction [4]. The use of beam shaping allows high-quality signals to be delivered to the receiver, lowering transmission latency and error rates.
- **Full duplex:** Today's BSs and mobile devices rely on transceivers that must take turns broadcasting and receiving data over the same frequency, or operate on various frequencies if a device needs to transmit and receive data simultaneously[5]. A device that uses full-duplex technology may transmit and receive data at the same time and on the same frequency. Wireless networks' capacity can be doubled with such technologies.
- **Software defined networks (SDN):** SDNs were created to increase network flexibility by separating the network control and forwarding planes and allowing the control plane and data to be directly programmable. 5G SDN, in conjunction with network functions virtualization technologies, will enable the establishment of several hierarchies that make up the network topology, allowing 5G cellular networks to fulfil a variety of application needs. The examples above demonstrate how combining different technologies can significantly enhance communication capacity, minimise transmission latency, and save energy. It does, however, demonstrate the complex and decentralised architecture of 5G cellular networks, which widens the cyber risks.
- **Multi-Access Edge Computing (MEC)**
  MEC (Multi-Access Edge Computing) is a key component in 5G design. MEC is a cloud computing evolution that brings applications from centralised data centres to the network edge, bringing them closer to end users and devices. This effectively eliminates the long network path that previously separated the user and the host in terms of content delivery. This technology isn't unique to 5G, but it is critical to its effectiveness. Low latency, high bandwidth, and real-time access to RAN information are features of the MEC that separate 5G design from its predecessors. Operators will need to use new ways to network testing and validation as a result of the convergence of the RAN and core networks. 5G networks that follow the 3GPP 5G specifications are suited for MEC implementation. The 5G specifications define the edge computing enablers that allow MEC and 5G to work together to transport data. The MEC architecture's distributed processing capability will better enable

the enormous volume of connected devices inherent in 5G deployments and the advent of the Internet of Things, in addition to the latency and bandwidth benefits (IoT).

- **Network function virtualization (NFV) and 5G**
  Network function virtualization (NFV) decouples software from hardware by virtualizing network functions such as firewalls, load balancers, and routers and operating them as software. This reduces the need for many expensive hardware components and can also accelerate installation timeframes, allowing customers to receive revenue-generating services sooner. By virtualizing appliances within the 5G network, NFV allows the 5G infrastructure. This includes network slicing, which allows multiple virtual networks to run at the same time. NFV can address other 5G challenges through virtualized computing, storage, and network resources that are customized based on the applications and customer segments.
- **5G RAN Architecture**
  NFV extends to the RAN, for example, through network disaggregation promoted by coalitions like O-RAN. This allows for more flexibility and competitiveness, as well as open interfaces and open source development, which makes it easier to roll out new features and technology on a large scale. The goal of the O-RAN ALLIANCE is to enable multi-vendor deployment with off-the-shelf hardware enabling easier and faster interoperability. Network disaggregation also enables the virtualization of network components, enabling the network to scale and improve user experience as capacity grows. The benefits of virtualsing components of the RAN provide a means to be more cost effective from a hardware and software viewpoint especially for IoT applications where the number of devices is in the millions.
- **Network Slicing**
  Network slicing may be the most important component in realising the full potential of 5G architecture. This technique expands the NFV area by allowing many logical networks to run on top of a shared physical network infrastructure at the same time. By constructing end-to-end virtual networks that incorporate both networking and storage capabilities, this becomes a key component of 5G design. By allocating network resources to different users or "tenants," operators may effectively manage a variety of 5G use cases with varying throughput, latency, and availability demands. Network slicing becomes extremely useful for applications like the IoT where the number of users may be extremely high, but the overall bandwidth demand is low. Because each 5G vertical will have unique requirements, network slicing will be a key design issue for 5G network architecture. With this level of customization now available, costs, resource management, and network configuration flexibility may all be improved. Furthermore, network slicing allows for faster time-to-market and speedier trials for prospective new 5G services.

3. Core Network And 5G Architecture Diagram

We will give an overview of the 5G core architecture and describe the 5G core components in this part. One of the three key components of the 5G System, commonly abbreviated as 5GS[6], is the 5G core network, which provides the expanded functionality of 5G networks. The 5G Access Network (5G-AN) and User Equipment are the other two components (UE). As demonstrated in the 5G core diagram, the 5G core uses a cloud-aligned service-based architecture (SBA) to enable authentication, security, session management, and traffic aggregation from connected devices, all of which requires the complex interconnection of network operations. The components of the 5G core architecture include:

- User plane Function (UPF)
- Data network (DN), e.g. operator services, Internet access or 3rd party services
- Core Access and Mobility Management Function (AMF)
- Authentication Server Function (AUSF)

- Session Management Function (SMF)
- Network Slice Selection Function (NSSF)
- Network Exposure Function (NEF)
- NF Repository Function (NRF)
- Policy Control function (PCF)
- Unified Data Management (UDM)
- Application Function (AF)

The 5G network architecture diagram below illustrates how these components are associated.

5G Architecture Diagram

Network functions are divided by service in 5G, which was built specifically. This architecture is also known as the 5G core Service-Based Architecture (SBA). The major components of a 5G core network are depicted in the 5G network topology diagram below:

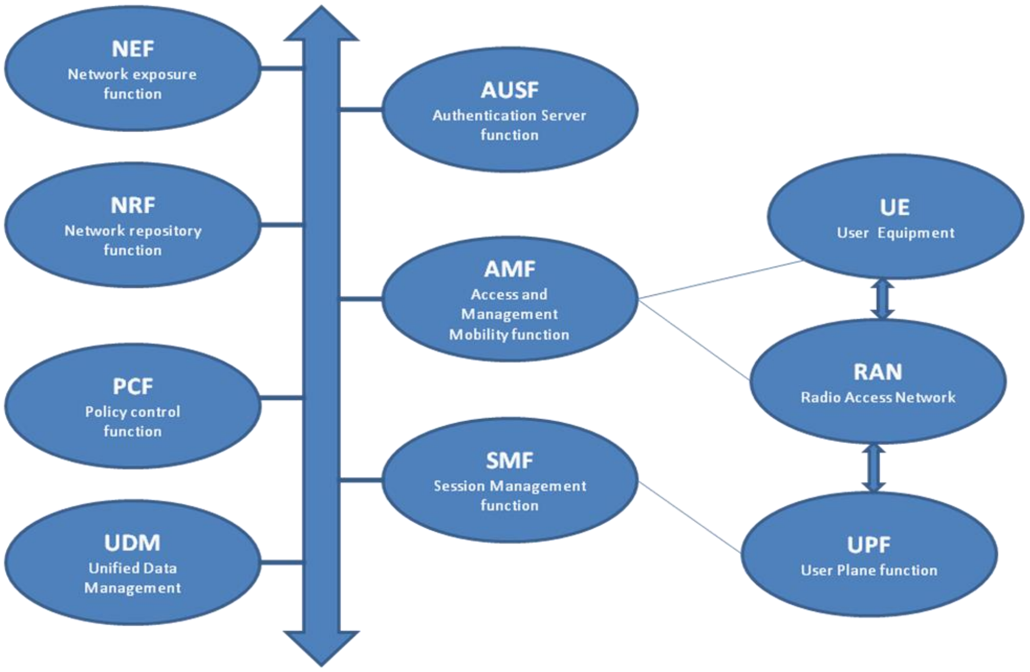

Figure 1. Network Topology of 5G [6]

Working

- User Equipment (UE), such as 5G smartphones or cellular devices, connects to the 5G core and then to Data Networks (DN), such as the Internet, via the 5G New Radio Access Network.
- The Access and Mobility Management Function (AMF) serves as the UE connection's single point of entry. The AMF picks the appropriate Session Management Function (SMF) for managing the user session based on the service requested by the UE.
- Between the User Equipment (UE) and the external networks, the User Plane Function (UPF) transfers IP data flow (user plane).
- The AMF uses the Authentication Server Function (AUSF) to authenticate the UE and gain access to 5G core services. Other functions such as the Session Management Function (SMF), Policy Control Function (PCF), Application Function (AF), and Unified Data Management (UDM) offer the policy control framework for governing network activity by applying policy decisions and obtaining subscription information.

Behind the scenes, the 5G network architecture is more complicated, but this complexity is required to deliver superior service that can be adjusted to a wide range of 5G use cases.

4. Security Issues In 5G

Engineering, Software, Intrusion detection and prevention, Malwares, Physical layer, Privacy, Native security, Identity management, Digital Forensic, Account management, Financial management, Authorization and authentication, Trust and reputation, Lightweight security, and many other aspects of telecommunication security are all required. 'Network access security, Network domain security, User domain security, Application domain security, Service Based Architecture, Visibility and configurability of security, Future Heterogeneous access, privacy' are the primary domains where security is necessary and more vulnerable [14]. Security will be crucial in 5G because it will handle not just basic packet transmission traffic but also a wide range of applications. Connecting industries and business applications to the internet; with 5G, a new paradigm of communication facilities for users and industry is expected [7].

Network Architecture and Infrastructure

The architecture and infrastructure of a network are critical components of security implementation. 5G requires a robust network architecture that can support enhanced security features in order to support a wide range of applications with high end security requirements. For 5G, two primary network infrastructure approaches are being considered: one is to virtualize the network infrastructure, and the other is to physically transform the network access point. Virtualization and advanced technologies such as Network Functions Virtualization (NFV)/Software Defined Network (SDN) are seen as ways to make 5G networks more efficient. While keeping a low investment cost. The security of network elements (NEs) in traditional networks is determined by how well their physical units can be isolated from one another. In 5G, however, the isolation will be considerably different because virtual NEs would be on cloud-based infrastructure. SDN is beneficial in terms of improving transmission efficiency and resource use, but it's also crucial to remember the 5G security design. In a cloud based architecture, security in term of isolation of nodes could be achieved by enforcement of the SDN flow table[8]. When considering traditional infrastructure, it's important to remember that each network access (BTS/Node B) has a unique structure. Some network access antennas are high powered, while others are low powered; each antenna would most likely have its own amplifier. Not to mention the varying levels of protection, identified management, and data protection needs dependent on the services given to end users. With the potential introduction of the Internet of Things (IoT), there is a strong likelihood that DDOS attacks will become more common. Similar active assaults can cause network disruption by granting unauthorised access or denying access to the network and its resources. So if 5G implies physical isolation of nodes for its services, it would be a nightmare in term of scalability, antenna correlations and mutual coupling. Cost will be among the issues that must be sorted out before deciding physical network access point alterations [8][9].

Robust and Rigid authentication

In a vertically integrated environment, security needs for various applications may differ significantly. The desire for lightweight security with high-speed mobile services necessitates a high-capability security method in the case of Internet of Things (IoT) devices. The traditional hop-by-hop security strategy, which is based on the network, may not be effective enough to create separate end-to-end (E2E) protection for different types of services. As the Internet of Things (IoT) becomes more widely adopted, IoT devices will require a more robust and stringent authentication technique. In order to prevent unauthorized access for example, biometric based identification could be a very suitable authentication method for smart phones [8].

Privacy Protection

Due to the large range of applications, it is essential to provide differentiated QoS (Quality of service). There should be a method or ability within networks to detect the sort of service being utilised by the user in order to provide better privacy. Because of recent major security and privacy vulnerabilities involving cellular networks, such as mass surveillance and face network access points, The telecommunication standardisation bodies, such as the 3GPP and the IETF (Internet Engineering Task Force), are being questioned [10]. Over here one must not forget that adding enhanced privacy methods makes implementation of 5G a greater challenge[8].

Application programming interfaces (APIs) and Drivers

The security drivers have continued to provide a reliable and simple connectivity service. To a certain extent, telecom operators and roamers will have to reveal application programming interfaces (APIs) to users and third-party developers or service providers. For instance, to achieve the goal of improved delivery through the use of position awareness, caching, and content adaptation. Third-party software parties on mutual hardware platforms with committed telecom software may occasionally support such optimization facilities [10].

Threat of Landscape

5G networks will serve as a core infrastructure for communication and a variety of additional applications, according to the scope or concept. The users have a major worry with this central architecture approach. If the central architecture goes down due to a disaster or for any other reason, it will have an impact on a wide spectrum of communication and daily activities for users and businesses. As a result, 5G requires well-defined protocols that are resilient to various types of attacks and disasters [10].

Energy efficiency aspects of 5G wireless systems

In the last four to five years, the advancement and growth of wireless technology has accelerated dramatically. Massive MIMO is a new technique that claims to be capable of meeting 5G criteria. Massive MIMO technology outperforms 4G technologies in terms of overall efficiency by employing principles such as having more antennas than devices, which means that some of the devices will operate as network access points (device to device and machine to machine concept). Small cells with a bandwidth of 30 to 300 GHz and a wavelength of 1 to 10 mm will be employed to improve area spectral efficacy. Massive MIMO can use relatively simple multiplexing and encoding methods with the aforementioned approach, allowing these approaches to be implemented with very simple hardware. As a result, resources are underutilised, particularly in terms of power [9].

Heterogeneous environment

As data consumption and the number of online devices grow at a rapid rate, heterogeneous access becomes a critical component of the 5G network [11]. A heterogeneous environment allows many access technologies to be used at the same time [12]. Different access technologies, on the other hand, must work together to create an architecture that meets the security needs of 5G networks [8]. However, the difficulties connected with diverse networks continue to be a source of worry. Inter-cell interference, distributed interference coordination, poor medium access control, device detection, and link setup are examples of such issues [11].

Blockchain

Because of its features like as decentralisation, immutability, interoperability, transparency, and cryptographic security, blockchain technology could be linked with IoT to provide a great solution for the aforementioned IoT challenges. Interoperability is becoming a key challenge in the IoT platform due to device heterogeneity and a lack of standards.Blockchain is principally a linked list of blocks. As a result, blockchain consists of two components: blocks and links or chains of blocks. Every block in the blockchain consists of a set of transactions and a hash value, and the chain is a collection of these cryptographically secure blocks linked together by the hash values of previous blocks [13].

5. Conclusion

The main contribution of this paper is the discussion of 5G mobile technology concepts and architecture. A new revolution of 5G technology is about to begin because 5G technology going to give tough completion to normal computer and laptops whose marketplace value will be effected. In the field of telecommunications, there have been numerous advancements from 1G to 2G to 3G to 4G to 5G. The new 5G technology will be offered in the market at a lower cost, with a higher peak speed and higher reliability than previous technologies. 5G is an emerging technology that give benefits to rural and remote communities. In this paper, main focus is on the security issues 5G will face now and in future. Since the service and network architecture of 5G is going through dramatic remodeling, 5G network features and strength can be improved if already security protection and privacy is considered. In future, 5G security challenges can be handle in easy way with capability to handle the increasing number of heterogeneous sources and devices, capability to secure the user's data and organizations tools software, detection and imaging.

References

[1] M. Agiwal, A. Roy, and N. Saxena, "Next Generation 5G Wireless Networks: A Comprehensive Survey," IEEE Communications Surveys Tutorials, vol. 18, no. 3, pp. 1617–1655, thirdquarter 2016.

[2] T.E. Bogale, X. Wang, L.B. Le, "mmWave Communication Enabling Techniques for 5G Wireless Systems: A Link Level Perspective", in mmWave Massive MIMO – A Paradigm for 5G (S. Mumtaz, J. Rodriguez, L. Dai, eds.), Elsevier 2017.

[3]Q. Wu, G. Ye Li, W. Chen, D. K. Ng, R. Schober, "An Overview of Sustainable Green 5G Networks", IEEE Wireless Commun. 24(4): 72-80 (2017).

[4] I. Ahmed, H. Khammari, A. Shahid, A.Musa, K.S. Kim, E. De Poorter, I. Moerman, "A Survey on Hybrid Beamforming Techniques in 5G: Architecture and System Model Perspectives", IEEE Communications Surveys and Tutorials 20(4): 3060-3097 (2018).

[5] https://spectrum.ieee.org/video/telecom/wireless/5gbytes-full-duplex-explained

[6] 5G Core Network - a Short Overview - Grandmetric

[7] K. Karthik ,Sobharani kuracha "SECURITY IN WIRELESS CELLULAR," vol. 4, no. 4, pp. 190–197, 2015, IJAIEM.

[8]"5G Security: Forward Thinking Huawei White Paper." (http://www.huawei.com/minisite/5g/img/5G_Security_Whitepaper_en.pdf)

[9] P. K. Hirani, "Special issues on 5g technologies," International Journal of Engineering Technology and Management (IJETM). Volume 2: Issue 2: Page No. 01- 07.

[10]ERICSSON, "Mobility Report," June, 2015 (https://www.ericsson.com/res/docs/2015/ericssonmobility- report-june-2015.pdf).

[11] W. H. Chin, Z. Fan, and R. Haines, “Emerging technologies and research challenges for 5G wireless networks,” IEEE Wireless Communications 21(2):106-112 · April 2014.
[12] A. Ghosh, J. Andrews, R. Ratasuk, E. Ratasuk, B. Mondal, P. Xia, N. Mangalvedhe, Han-Shin Jo, T. Thomas, H. Dhillon, T. Novlan, M. Cudak "Heterogeneous Cellular Networks: From Theory to Practice", IEEE Communications Magazine Volume: 50, Issue: 6, Page No. 54-64, June 2012.
[13] V. Sharma and N. Lal, "A Detail Dominant Approach for IoT and Blockchain with their Research Challenges," 2020 International Conference on Emerging Trends in Communication, Control and Computing (ICONC3), Lakshmangarh, Sikar, India, 2020, pp. 1-6, doi: 10.1109/ICONC345789.2020.9117533.
[14] I. Ahmad, S. Shahabuddin, T. Kumar, J. Okwuibe, A. Gurtov and M. Ylianttila, "Security for 5G and Beyond," in IEEE Communications Surveys & Tutorials, vol. 21, no. 4, pp. 3682-3722, Fourthquarter 2019, doi: 10.1109/COMST.2019.2916180.