5G security: Technologies and Challenges

Shreyas Ramesh
Cybersecurity
University at Buffalo
(State University of New York)
Buffalo, USA
Ramesh3@buffalo.edu

***Abstract*—The advent of 5G technology promises to revolutionize the way we communicate and interact with one another. However, with this new technology comes a host of challenges and requirements that must be addressed in order to ensure its successful implementation. This paper reviews the current state of 5G research and identifies key use cases and requirements as outlined by industry leaders Nokia and Huawei. Additionally, it examines the potential security implications of 5G and offers insights from experts in the field. The paper concludes by highlighting the need for further research and collaboration to fully realize the potential of 5G and ensure its secure and successful implementation.**

Keywords— Artificial Intelligence (AI), Machine Learning (ML), Internet of Things (IoT), Network Function Virtualization (NFV), Software-Defined Networking (SDN), Edge Computing, Blockchain.

I. INTRODUCTION

As the world embarks on the next generation of wireless communication, 5G, security becomes an imperative aspect that cannot be overlooked. Telecommunications bodies are working on integrating advanced networking technologies such as Software Defined Networking (SDN), Network Function Virtualization (NFV), cloud computing, Multi-access Edge Computing (MEC), Network Slicing (NS) concepts to telecommunication networks [1]. Compared to previous wireless technologies, 5G standards include more security features to tackle potential security vulnerabilities, contributing to security improvements throughout the future lifecycle of the technology.

First generation (1G) networks were prone to illegal interception, cloning and masquerading. Spread of misinformation and message spamming was the main challenge of second generation (2G) networks. Third generation (3G) networks introduced internet communications to devices and with it also introduced internet-based vulnerabilities. This network was further extended in fourth generation (4G) networks and the threat landscape was further complicated.

With the advent of 5G, new architectures, services, and technologies are being introduced, leading to new security challenges. For instance, increasing use of artificial intelligence and machine learning in 5G networks can create potential vulnerabilities if not properly secured [1]. Moreover, the growing reliance on cloud computing and virtualization can also introduce new security concerns, such as data breaches and unauthorized access.

Through a comprehensive analysis of existing literature and the latest developments in the field, this paper attempts to identify and explore potential vulnerabilities in the 5G network. With increasing dependence on digital technologies and the growing number of connected devices, the potential attack surface is expanding exponentially. Therefore, it is crucial that we address these security concerns proactively and develop effective strategies to safeguard 5G networks from threats both known and unknown.

The remainder of this paper is organized as follows:

- Main Techniques.
- Issues and Problems.
- Future Trends.
- References.

II. MAIN TECHNIQUES

A. Edge computing

According to Open Networking foundation (ONF) Edge computing can be defined as “The practice of processing data closer to where it is generated, rather than sending it to a central server or cloud for processing." This approach can significantly reduce latency and improve real-time processing capabilities, making it ideal for applications such as IoT, autonomous vehicles, and smart cities.

Four essential conditions must be met for edge computing to be successfully deployed and operated in 5G. These conditions are critical to the functioning of numerous applications. All four requirements are important, but depending on the applications involved, finding a healthy trade-off between them is crucial. First off, the rise of edge computing is largely driven by real-time interaction, which guarantees low latency to support applications that are sensitive to delays, including autonomous vehicles and remote surgery, improving Quality of Service (QoS). Furthermore, by handling data and user requests locally, edge servers with local processing capabilities improve bandwidth efficiency and lessen traffic congestion between small cells and the core network. Moreover, high-speed transmission is necessary to handle the enormous amount of data produced by various applications, such as virtual reality and remote surgery, made possible by mmWave frequency bands and edge servers installed in base stations [2]. Finally, edge computing depends on edge cloud availability to bring data and application logic closer to end users, guaranteeing continuous service delivery. For this reason, high availability of cloud services at the edge is essential.

B. Software Defined Networking (SDN)

Software-Defined Networking (SDN) refers to the ability of software applications to program individual network devices dynamically and have them work together *[3].* This model differs from that of traditional networks, which use dedicated hardware devices (i.e., routers and switches) to control

network traffic. SDN can create and control a virtual network – or control a traditional hardware – via software. This allows for greater flexibility and allows developers and programmers to manipulate data flows accordingly.

Software-Defined Networking (SDN) is a network architecture that facilitates software-based network management and control by separating the control plane from the data plane. The data plane manages packet forwarding and stays in the hardware, but the control plane, which decides how network traffic should be routed, is transferred to software. Instead of having to handle each device separately, this separation enables network administrators to program and administer the entire network using a centralized management system. The three primary parts of a typical SDN architecture are networking devices, controllers, and applications. Applications send information about network traffic and resource requests to the controllers, who utilize it to decide how to route data packets. The controller provides guidance to networking devices, whether they are virtual or physical regarding the routing of packets. Virtual switches embedded in software, consolidates the functions of physical switches improving network performance and efficiency.

C. Network virtualization functions (NVF)

NVF is the replacement of traditional hardware devices with virtual machines. The virtual machines are run on a hypervisor on which networking software such as routers and load balancers are run on. One of the main advantages of using NVF is that it allows for separation of different software's, and it replaces the manual and cumbersome installation of physical hardware devices. This saves on costs and allows for additional customization of the software as it is decoupled with the underlying physical hardware. NVF gained further popularity and its usage increased due to the elastic scaling nature of virtual appliances. By being able to increase or decrease resources based on demand, telecommunications vendors can optimise costs.

A framework, software programs, and a centralized virtual network infrastructure are the main elements of an NFV architecture. A hypervisor that abstracts the network, storage, and processing resources, or a container management platform, can serve as the foundation for the virtual network infrastructure. To provide the required network functionality, software programs—also referred to as virtualized network functions—supplant the actual hardware elements of a conventional network [3]. The infrastructure is managed and network services are provided using a framework known as MANO (Management, Automation, and Network Orchestration). This allows for more flexibility in the infrastructure and lower capital and operating costs by utilizing off-the-shelf hardware and software.

D. mmWave Technology

The millimetre-wave (mmWave) frequency spectrum, which runs at 24-100 GHz and can handle enormous amounts of data, is what the 5G network uses. Thanks to developments in coding techniques, it is possible to transmit thousands of times more data than with low-band signals. mmWave technology can be used by mobile network operators to expand network capacity, attain multi-gigabit speeds, and achieve very low latencies both indoors and outdoors. This is accomplished by expanding network capacity in outdoor metropolitan areas and enabling high-throughput services in indoor sites including sports arenas, train stations, airports, and event venues. This technology has been adopted globally by several first world countries including but not limited to US, China, Japan and Germany.

With a few key distinctions, 5G mmWave transmission functions similarly to existing radio frequency (RF) communications. 5G mmWave transmissions have a limited transmission range and frequently need a straight line of sight to the antenna since signals are more easily blocked by objects. Compared to lower frequency transmissions (e.g., 2G, 3G, or 4G), the equipment needed for 5G mmWave transmission and reception is smaller. Beamforming technology, which focuses the radio signal on a particular region rather than using conventional antennas that cover a large area like a floodlight, is one prominent aspect of 5G mmWave transmission. Like a torch, this targeted coverage enables stronger signals and less interference in the intended area, but the signal becomes weaker a few meters away [4].

The convergence of these different technologies allows 5G networks to power devices globally.

III. ISSUES AND PROBLEMS

While 5G networks provide enormous speeds to users, there exists a security trade-off that has to be taken into consideration. Documented below are the security issues and problems that arise due to 5G networks.

A. Network slicing

A crucial component of 5G networks is network slicing, which permits the development of several virtual networks on a single physical infrastructure. This makes it possible to tailor network services to meet needs, such as throughput, latency, and security. The isolation of network slices, which is essential for limiting unwanted access and safeguarding sensitive data, is one of the main security concerns [5]. There's a chance that a breach in one slice could propagate to others, which would have a larger effect on the network. Additionally, additional security flaws including those relating to software faults and configuration problems are introduced by the virtualization of network operations as part of network slicing.

The possibility for attackers to take advantage of network slicing's flexibility for malevolent intent is another security concern. An attacker could exploit a network slice to start a denial-of-service attack or to intercept private information. Furthermore, because network slicing uses shared infrastructure, it is challenging to track down malicious behaviour because an attacker can simply move across slices to evade detection.

B. Software defined networking SDN

The centralized control plane is a significant security issue related to SDN in 5G networks. With network intelligence contained in a controller entity, SDN topologies divorce the control plane from the data plane. A possible target for attackers and a single point of failure are introduced by this

centralized control approach. Unauthorized access, disruptions to the control plane, or network-wide outages could be caused by a compromised SDN controller, which could cause service interruptions and data breaches [3]. Furthermore, depending too much on a centralized controller introduces a crucial security dependency whereby the network's overall security is at risk from the controller's penetration.

SDN's larger attack surface and possibility for network spying present another security risk for 5G networks. Through software-defined policies, network managers may now dynamically set and manage network resources thanks to SDN's programmability and automation features. But this programmability also opens up new avenues for attack and ways for bad actors to take advantage of weaknesses in protocols, switches, or SDN controllers. Attackers may try to perform denial-of-service (DoS) attacks, spy on network traffic, create false controller orders, or modify SDN control messages to obtain unauthorized access [6]. Furthermore, attackers may be able to carry out network reconnaissance more quickly and effectively thanks to SDN's visibility and control, obtaining information on traffic patterns, network architecture, and security measures that they might use to plan and carry out focused assaults.

C. Privacy concerns

The possibility of widespread spying is one of the main issues with 5G security. Governments and businesses can effortlessly monitor and track people's behavior with previously unheard-of precision thanks to the capacity to gather and analyze massive volumes of data from billions of linked devices [7]. This brings up important moral issues about civil liberties and privacy, as well as the possibility of power abuse by people in positions of influence. Furthermore, these worries may be exacerbated by the use of AI and machine learning in 5G security systems, since autonomous algorithms may decide with biases built into them.

The risk of fraud and identity theft is a serious privacy problem. People's personal information may be more susceptible to cyberattacks, data breaches, and other types of crimes as 5G networks spread [7]. The capacity to gather and preserve enormous volumes of information about people, such as their whereabouts, communication preferences, and financial particulars, may make it simpler than ever for criminals to pose as someone else or take advantage of people for destructive ends. Apart from these worries, there's a chance that 5G security technologies will reinforce current societal injustices. For example, minority communities who are already susceptible to discrimination and oppression may be disproportionately impacted by the deployment of biometric authentication techniques like fingerprint scanning or facial recognition.

D. Artificial Intelligence:

AI can be used to enhance the performance of 5G networks by optimizing resource allocation, improving network efficiency, and enhancing security. However, the use of AI in 5G networks also raises privacy and security concerns.

One of the main issues with 5G networks is bias in AI models. Certain types of traffic may be given priority over others by AI-based network management systems, which could result in unjust resource allocation, network congestion, and decreased performance. The utilization of skewed or insufficient data may be the source of this bias, which can lead to biased decision-making. Furthermore, security flaws and possible abuse of network resources are brought up by the opaqueness of AI-based network management systems. Because these systems are opaque, it can be challenging for network operators to comprehend the choices the system is making, which could result in security lapses.

AI-based network management systems also pose privacy issues due to their massive data collection and processing processes. Sensitive data about users, such as their location, surfing preferences, and communication styles, may be included in the data collection. Users' privacy rights may be violated as a result of the use of this data. Furthermore, new security flaws like distributed denial-of-service (DDoS) and denial-of-service (DoS) attacks may be introduced by AI-based network management systems. These assaults have the potential to impede network functions or allow unwanted access to network resources. These worries are made worse by the absence of set security norms and regulations. In the absence of such standards, network operators find it difficult to guarantee the security and privacy of their networks.

E. MEC and Cloud Related Security Issues

The utilization of edge devices like routers, switches, gateways, and Internet of Things devices characterizes 5G edge computing environments, which provide particular security challenges. As the cornerstone of the edge computing infrastructure, edge devices frequently have security flaws, such as weak default passwords, insecure firmware, a lack of encryption, and inadequate access controls. These flaws may give attackers access to private information without authorization [7].

IV. FUTURE TRENDS

5G technology has just started being adopted globally and many telecommunications vendors are actively working on securing the technology. One of the methods currently being researched is the implementation of blockchain within 5G to ensure transparency.

By utilizing blockchain for network security, a decentralized and immutable ledger is established, recording network transactions, security events, and access control policies, thus enhancing network security and trust. Moreover, blockchain-based identity management solutions enable self-sovereign identity, allowing users to control and manage their digital identities. This grants users full control over their identity information, enhances privacy, and streamlines authentication and authorization processes in 5G applications and services. Lastly, decentralized applications can be developed on distributed networks, enabling secure and transparent services, such as decentralized communication platforms, peer-to-peer content sharing, and DeFi applications [8]. The integration of blockchain technology into 5G networks provides a promising avenue for addressing security and privacy concerns and unlocking new potential in the field.

In conclusion, 5G technology exists to make virtual life faster and more accessible but it has its flaws.

V. REFERENCES

[1] P. Zhang, X. Yang, J. Chen, and Y. Huang, "A Survey of Testing for 5G: Solutions, Opportunities, and Challenges," China Communications, vol. 16, no. 1, pp. 69–85, 2019.

[2] Najmul Hassan, Kok-Lim Alvin Yau, Celimuge Wu, "Edge Computing in 5G: A Review", Retrieved from: https://ieeexplore.ieee.org/abstract/document/8821283

[3] Haleplidis, E., et al. (2015). "SDN: Layers and Architecture Terminology." RFC 7426, January 2015.

[4] GSMA (2022). "5G mmWave – Unlocking the Full Potential of 5G". Retrieved from: https://www.gsma.com/futurenetworks/wp-content/uploads/2022/04/GSMA-5G-mmWave-Factsheet-Unlocking-the-Full-Potential-of-5G.pdf

[5] Shunliang Zhang (2019). "An Overview of Network Slicing for 5G". Retrieved from: https://ieeexplore.ieee.org/abstract/document/8685766

[6] Yifan Liu; Bo Zhao; Pengyuan Zhao; Peiru Fan; Hui Liu (2019). "A survey: Typical security issues of software-defined networking". Retrieved from: https://ieeexplore.ieee.org/abstract/document/8766905

[7] Rabia Khan, Pradeep Kumar, Dush Nalin K Jayakody, Madhusanka Liyanage (2019). "A Survey on Security and Privacy of 5G Technologies: Potential Solutions, Recent Advancements and Future Directions". Retrieved from: https://www.researchgate.net/publication/334644935

[8] Dinh C. Nguyen, Pubudu N. Pathirana, Ming Ding, Aruna Seneviratne (2019). "Blockchain for 5G and Beyond Networks: A State-of-the-Art Survey". Retrieved from: https://arxiv.org/pdf/1912.05062.pdf