Chapter 2

History of security and privacy in wireless communication systems: open research issues and future directions

Abdulwaheed Musa[1,2]

Abstract

Wireless communication is one of the most successful technologies that have found application in various sectors of our daily lives. However, one of the major issues and challenges of wireless communication is security. To provide a holistic view of this crucial issue, this chapter presents a historical description of the evolution of the cellular network and provides a general overview of different attacks and vulnerabilities in the wireless network based on the Open System Interconnection (OSI) layered protocol architecture. The chapter further presents a brief review of the security and privacy issues for each cellular generation. The various emerging wireless communication systems as well as the application of artificial intelligence (AI) and machine learning (ML) to wireless security system design. The security issues and challenges in the key technology of 6G wireless network were identified and discussed. Finally, open research issues have been identified and discussed, giving a path for further research direction for security in 5G wireless networks and beyond.

Keywords: Wireless communication; Cellular network; Open System Interconnection; Security; Privacy

2.1 Introduction

Communication is the exchange of information between people or nodes separated by a short or long distance. Wireless communication is simply the communication between one or more devices without any physical connection between them. It utilizes radio frequency transmission to transmit information from source to destination [1]. It is one of the most popular modes of communication today due to its numerous advantages such as its cost-effectiveness, minimal power consumption, flexibility, lack of physical

[1]Department of Electrical and Computer Engineering, Kwara State University, Nigeria
[2]Institute for Intelligence Systems, University of Johannesburg, South Africa

infrastructure, and ease of deployment, among others, over its wired counterpart [2]. This has led to an exponential increase in the number of wireless users, especially with the provision and implementation of wireless networks systems and telecommunication services, including cordless, cellular, and satellite phones as well as wireless local area networks (WLANs), which have found extensive applications in various sectors such as in business, government, and military. Over the past few decades, wireless communication systems have evolved progressively from the first to the fifth generation which has benefitted various stakeholders, including standard bodies, end-users, commercial service providers, academic research groups, etc. [3]. The recent 5G network included several novel technologies such as ultra-densification, network function virtualization, the adoption of small cells, referred to as heterogenous network (HetNet) as well as the utilization of new frequency bands (millimeter wave bands) which enabled the development of the different emerging applications such as machine to machine (M2M) communication, enhanced mobile broadband (eMBB), and virtual and augmented reality (VAR). This thus has demonstrated the vast potential of the 5G wireless network and beyond [3]. However, security is one of the major issues faced by these developments and applications of wireless communication systems.

Security is a critical issue in every aspect of our daily lives, such as in banking, finance, e-commerce, and medical data, especially with the increased number of hackers and hacking tools that could be used to break into networks and systems to steal users' data [4]. Similarly, security is a crucial concern in wireless communication networks due to their dynamic nature and the utilization of radio frequency for the transmission of signals over unprotected media, referred to as open-air transmission, where any attacker that is in proximity to the signal can easily attack and steal confidential information by eavesdropping, modifying, tracking or perform any other malicious attacks on the information. This has drawn the interest and attention of researchers over the years, and there have been various developed algorithms to combat these security threats and vulnerabilities. However, these techniques and algorithms, for example, cryptographic algorithms, failed to meet up with the requirements of the future wireless communication systems challenges [5]. Hence, the need for new, dynamic, and robust security algorithms that would meet the requirements of the 5G and beyond networks. This chapter aims to present the security issues and challenges in wireless communication across all the developed cellular technologies (1G to 5G), as well as to review these security challenges in the 6G wireless network showing the trends and recommendations for further research directions. The key contributions of this chapter are as follows:

- The historical description as well as a comparison between the developed cellular generations is presented.
- General security issues in wireless communication based on the OSI reference model and a tabular summary of these attacks are provided.
- The security and privacy challenges across all cellular generations are presented, including a taxonomy of these attacks.
- The security issues in 5G technology, URLLC, eMBB, and mMTC are presented and discussed.

- The contributions of artificial intelligence (AI) and machine learning (ML) to security system design in wireless communication are also reviewed.
- The security issues and challenges of future wireless communication, particularly the 6G network, are presented and reviewed.
- Critical open research issues for security in 5G networks and beyond have been identified and elaborated.

The rest of the chapter is organized as follows: Section 2.2 presents the history and evolution of wireless communication. The general security issues are provided in Section 2.3. Section 2.4 presents and discusses security and privacy in wireless communication from the first to the fifth generation. The emerging wireless communication system is discussed in Section 2.5. Section 2.6 presents the application of AI and ML to wireless security system design. The security issues and challenges in future wireless communication system are presented and discussed in Section 2.7. Finally, Section 2.8 concludes the chapter and provides some recommendations.

2.2 History and evolution of wireless communication

This section presents a historical description of wireless communication with a binocular focus on cellular technologies from the first generation (1G) to the fifth generation (5G) and compares these different technologies.

Wireless communication can be historically classified into three eras which include the following: the Pioneer era, which lasted till 1920, the pre-Cellular era which spanned between 1920 and 1979, and the Cellular era which started beyond 1979. In the Pioneer era, information was transmitted using smoke, torches, flares, mirrors, semaphore flags, etc., categorized under the first wireless networks, all of which were superseded by the first telegraph network developed by Samuel Morse in 1838 and thereafter, by telephones. A few decades after, Guglielmo Marconi, in 1895, demonstrated the first radio transmission which led to the advent of the wireless communication network [6]. The cellular system has advanced from the first to the fifth generation over the past few decades.

First generation (1G): the first generation of cellular network, launched by Nippon Telephone and Telegraph (NTT) in Tokyo, Japan in 1979, utilized analog transmission and operated at 800 MHz frequency band for speech services. Two years after the successful implementation of the network in Japan, two cellular networks were developed and deployed in Europe: Nordic Mobile Telephone (NMT) and Total Access Communication System (TACS). Afterward, another 1G network was developed and deployed in the United States of America (USA) in 1983 which was called the Advanced Mobile Phone System (AMPS). Although these systems were implemented differently, they still have similar disadvantages such as incompatibility issues, limitation to only voice communication, limited roaming services, limited coverage area, and low capacity. In addition, it is frequency modulation (FM)-based and used frequency division multiple access (FDMA) multiplexing scheme, which reduced the capacity of the network [7].

Second generation (2G): This cellular network, based on the Global System for Mobile Communication (GSM) standard, was developed in Finland in 1991 and utilized digital transmission. As an improvement over 1G, the 2G network was based on both the FDMA and time division multiple access (TDMA). This enhanced the system capacity. The GSM system employed a 25 MHz frequency spectrum in a 900 MHz range with a speed of 14.4 kbps. In 2G, circuit switching was used, and the core network was known as the public switched telephone network (PSTN). The general packet radio service (GPRS) was then developed as the demand to transmit data on air interface increased where an optimal speed of up to 150 kbps was achieved [8]. As the demand further increased, the Enhanced Data GSM Environment was developed which can be considered as 2.5G. This also increased the data rate amount to increase further up to 500 kbps. The major aim of this cellular network was to use digital signals for transmission and to provide several services such as web access facilities, digital voice calling, and short message services [9]. However, there are still some deficiencies experienced with the network such as the inability to support video communication and the dependency on strong digital signals. This means there is usually no network coverage if the digital signal is weak.

Third generation (3G): This cellular network was launched by the NTT DoCoMo in Japan in 2001 and was based on the International Mobile Telecommunication standard, precisely the IMT-2000 standard. The system utilized both the Code Division Multiple Access (CDMA) and WideBand Code Division Multiple Access (WCDMA) multiplexing schemes. Compared to the FDMA and TDMA utilized in the previous networks, the CDMA is a multiplexing scheme where each user utilizing the channel at a particular period is given a different code. This allowed for a significant number of users to utilize the network simultaneously. The 3G system utilized a 15–20 MHz frequency spectrum with 1,800–2,500 MHz, with a speed of up to 2 Mbps. WCDMA, the air interface for the Universal Mobile Telecommunication System (UMTS), utilized larger carrier frequency due to the increased number of users it can support as compared to the CDMA. The core network for the 3G system was a combination of circuit and packet switching [8]. The 3G system was known as the UMTS in Europe, CDMA2000 in America and the time division-synchronous code multiple access (TD-SCDMA) in China. As an advancement from the 3G network, the 3.5G and 3.75G networks were developed and deployed in the form of high-speed packet access (HSPA) and HSPA+, respectively to further increase the data rate. The HSPA+ enabled the first introduction of the multiple input multiple output (MIMO) technology where an optimal speed of up to 42 Mbps was achieved using a modulation scheme of 64-bit quadrature amplitude modulation (QAM) [7]. This system has numerous advantages such as supporting both voice and video communication. However, it also has some notable disadvantages such as expensive terminals, and high power consumption.

Fourth generation (4G): The cellular network, sometimes called the long-term evolution (LTE) was first launched in Oslo, Norway and Stockholm, Sweden in 2009. It was based on the ITU-defined capabilities in the IMT-advanced standard. The 4G network uses orthogonal frequency division multiplexing (OFDM) technique and utilized 5–20 MHz in a frequency band of 2,000–8,000 MHz where a

speed of up to 100 Mbps and 500 Mbps was achieved for downlink and uplink, respectively. This allowed the system to support high data rate applications such as online gaming, voice as well as video over IP, and high-quality online streaming. The 4G core network was IP-based and has low latency as well as wider channel and carrier aggregation of up to 100 MHz. The 4G network operates in both frequency division duplex and time division duplex (TDD) modes and also supports the TD-SCDMA evolution. Although the LTE had numerous advantages such as high throughput and simpler architecture, it is however limited in terms of security threats, cost, battery life of mobile phones, etc. [10].

Fifth generation (5G): This is the latest developed and deployed cellular network that was first largely adopted by South Korea in 2018. Unlike 4G which depends on high-power cell towers to transfer data over long distances, 5G wireless signals are provided by a vast number of small cell stations placed on light poles or building roofs [7]. Many small cell stations are required because the 5G frequency band (millimeter wave bands) is suitable only for short-distance transmission. The 5G is completely wireless making it suitable for the World Wide Wireless Web (WWWW) and to be supported by different technologies such as large area synchronized code-division multiple access (LAS-CDMA), multi-carrier code division multiple access (MC-CDMA), OFDM, ultrawideband (UWB), network-local multipoint distribution service (NLMDS) and Internet Protocol version 6 (IPv6) [11]. The 5G wireless network would operate in two primary categories of frequencies: Frequency Range 1 (FR1) or simply sub-6 GHz and Frequency Range (FR2) or simply millimeter wave (mmWave) band. Unlike the previous, this network offers many advantageous benefits, but it is quite limited in terms of cost of deployment since small cells are required.

A summary of the evolution of cellular communication technology showing the years of the initial launch and key characteristics is given in Figure 2.1 and a comparison of the generation in terms of their features is given in Table 2.1.

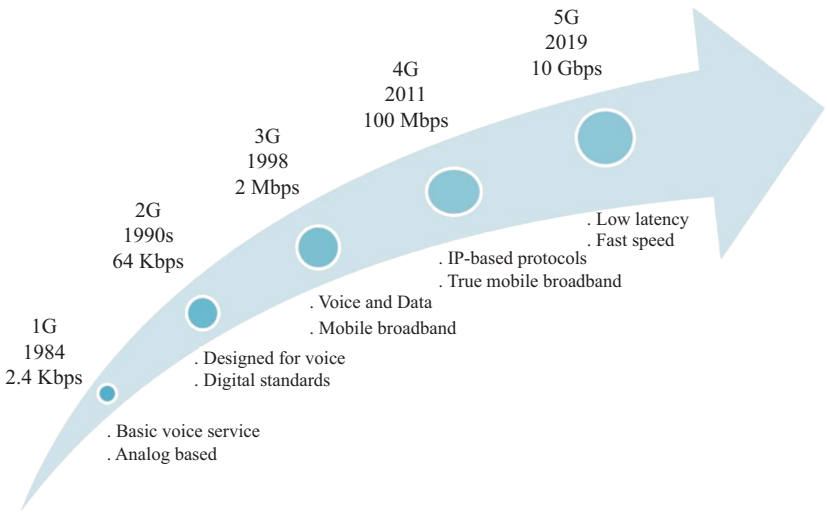


Figure 2.1 Evolution of cellular communication [12]

Table 2.1 Comparative analysis of cellular generations

Generations	1G	2G	3G	4G	5G
Deployment	1979	1991	2001	2009	2018
Switching techniques	Circuit switching	Circuit switching	Circuit and packet switching	Packet switching	Packet switching
Access techniques	FDMA	GSM, TDMA, CDMA	WCDMA, UMTS, CDMA 2000, HSUPA/HSDPA	LTEA, OFDMA, SC-FDMA, WiMAX	BDMA, NOMA FBMC
Application	Voice	Voice and data	Voice, data, and video calling	Voice, data, video calling, HD television, etc.	Voice, data, video calling, ultra HD video, VR application
Core network	PSTN	PSTN & packet	Internet	Internet	Internet
Data rate	2.4 kbps	14.4 kbps	384 kbps to 2 Mbps	100 Mbps to 500 Mbps	10 Gbps to 50 Gbps
Frequency band	800 MHz	800 MHz, 900 MHz, 1,800 MHz, 1,900 MHz	800 MHz, 900 MHz, 1,800 MHz, 1,900 MHz, 2,100 MHz	2–8 GHz	1.8 GHz, 2.6 GHz, 30–300 GHz
Advantages	Mobility	Digital voice calling, mass adoption, low power consumption	Better internet experience, support of both voice and video calling	High data rate, body area network	Low latency, higher data rate, wider coverage
Disadvantages	Poor security, low capacity, low coverage	Low data rate, inability to support video transmission	Expensive terminals and high-power consumption	Expensive and high-power consumption	Requires many small cell antennas

2.3 General security issues

This section provides a general overview of various security threats and attacks in wireless networks. Network security, either wireless or wired, refers to the prevention of unauthorized access, modification, destruction, or disclosure of information to ensure that the network's critical functions are executed properly and that there are no detrimental impacts.

Wireless and wired communication networks have some similarities, notwithstanding their differences. For instance, both utilize the open system interconnection (OSI) layered protocol architecture for their transmission, consisting of seven layers. However, this section would focus on five layers namely: the Physical, the Media Access Control (MAC), the Network, the Transport, and finally, the Application layers. Figure 2.2 shows how the data transmission from Node A to Node B occurs based on the OSI layers over a wireless medium.

Different protocols exist in the different layers of the OSI model. For instance, the application layer includes protocols such as hypertext transfer protocol (HTTP) and file transfer protocol (FTP) for providing web services and transporting large data files, respectively. The transport layer includes protocols such as the transmission control protocol (TCP) and user datagram protocol (UDP). Because each layer of the OSI model supports different protocols, they are vulnerable to various threats and attacks discussed below.

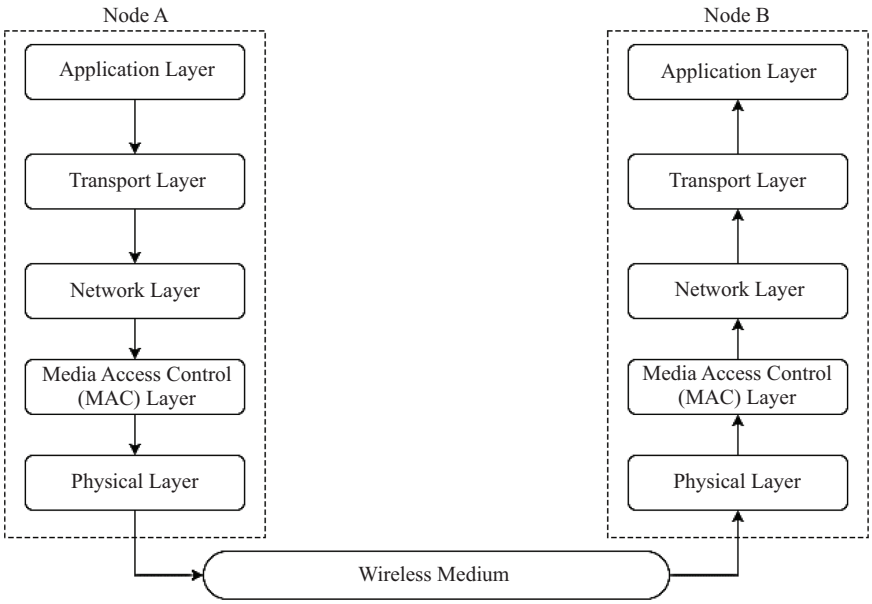


Figure 2.2 OSI-layered protocol architecture [13]

2.3.1 Physical layer attacks

The first layer of the OSI model architecture is known as the physical layer and it determines the physical characteristics of signal transmission. Signals sent through a wireless network are broadcast over the open air, making the physical layer of a wireless network susceptible to two major types of attacks which include eavesdropping attacks and jamming attacks [13]. An eavesdropping attack is a form of passive attack and it refers to an unauthorized interception of transmitted signal between the source and destination. It is a major threat to the wireless network as it is the prerequisite to all other attacks [14]. An eavesdropper situated within the coverage of the transmitter of a wireless network can overhear the communication sessions. To prevent this and maintain confidential communication, various methods have been developed, but one of the oldest of them all is known as cryptography, that is, the art and science of concealing meaning through the means of encryption. In that case, the receiver has a private key which would be utilized to decrypt the transmitted encrypted message. This will prevent the eavesdropper from understanding the message even after the interception. Jamming, on the other hand, is a type of denial of service (DoS) attack where a malicious node in the wireless network sends a large amount of radio signal to flood the channel with the intent of preventing legitimate users from utilizing the resources of the network, thus causing reduction in the network availability [15]. Jamming attacks are classified into four major types which include: deceptive, random, constant, and reactive jammers [16]. The constant jammers launch an attack by sending a continuous high-powered noise sweep from one communication channel to another based on a predetermined approach and then repeating this procedure over and over. For the random jammers, they work at random and switches from one communication channel to the other without any precise plan. The deceptive jammers transmit unauthorized packets via wireless networks making them busy. Finally, the reactive jammers consistently monitor the status of frequency channels and attack only those utilized for communication [16]. Various techniques have been developed to prevent jamming attacks. Among all of them, spread spectrum techniques have been widely utilized where the transmitted signal would be spread over a wider spectral bandwidth. The spread spectrum techniques include the direct-sequence spread spectrum (DSSS), frequency-hopping spread spectrum (FHSS), and time-hopping spread spectrum (THSS) [17].

2.3.2 MAC layer attacks

This is the second layer after the physical layer that allows the intelligent allocation of the shared medium using intelligent control mechanisms which include carrier sense multiple access/congestion detection (CSMA/CD), carrier sense multiple access/congestion avoidance (CSMA/CA), orthogonal FDMA (OFDMA), CDMA, and so on. In the wireless-MAC layer, there are four main types of attacks that can occur. They include MAC spoofing, man-in-the-middle (MITM), identity theft, and network injection [18]. Every node in the network is typically equipped with a network interface card (NIC) and a distinct MAC address, which is used for user

identification. A MAC spoofing attack happens when an attacker alters its assigned MAC address to conceal its identity or impersonates another node on the network to eavesdrop traffic and carry out illegal activities such as stealing private information; this is referred to as identity theft. The MITM attack involves the attackers first sniffing the network to capture the MAC addresses of the authorized communicating nodes, after which the attacker impersonates the two nodes and establishes a connection with them to act as a relay between the victims, giving them the impression that they are communicating directly with one another over a private connection. Network injection, on the other hand, attempts to prevent networking equipment such as routers, switches, and access points from functioning by the injection of fraudulent re-configurable network commands. This is done to shut down the entire network, necessitating resetting or reprogramming of all networking equipment.

2.3.3 Network layer attacks

The Internet protocol (IP) is the major protocol utilized in this layer for the delivery of packets from the sender to the receiver through a relay router based on IP address. In this layer, the attacks are focused on exploiting the IP weaknesses and can be classified into three types namely: IP spoofing, IP hijacking, and Smurf attacks [13,19]. Similar to MAC address spoofing, IP spoofing is when an attacker generates a fabricated IP address to conceal their identity or impersonates another node on the network to conduct illicit activities. This can also waste network capacity and potentially bring the network down since the network node that receives packets with a faked source IP address will interact with the same faked address. IP hijacking is another attack conducted by hijackers to obtain the IP address of an authorized user to disconnect the authorized user and then impersonate them on the network to access and steal confidential information. Prefix, route, and border gateway protocol hijacking are the three major types of IP hijacking attack [20]. A Smurf attack is a type of DoS attack where a significant number of Internet Control Message Protocol (ICMP) packets are sent to a target or group of targets from a faked source IP broadcast address with the intention of bringing down the target's network upon the receipt of the ICMP packets. The target would be required to respond which would lead to a substantial amount of traffic in the network. Firewalls are widely utilized to prevent this attack. It can be utilized to reject any malicious packets from a fabricated IP address. Another solution, although not scalable, is to configure each node in the network to not respond to ICMP requests.

2.3.4 Transport layer attacks

This is the fourth layer and the heart of the OSI model. As mentioned earlier, TCP and UDP are the two major protocols in this layer. The TCP is a connection-based protocol that supports the seamless and reliable delivery of segments from one node to another, such as email delivery and file transfer. UDP is the opposite of the TCP as it is not a connection-based protocol and does not guarantee the reliable delivery

of segments from one node to the other, but it has lower overhead and latency. It is typically used for time-dependent applications which do not demand reliable delivery of segments, such as IP television, Voice and Video over IP (VoIP). Attacks such as TCP flooding, UDP flooding, and TCP sequence number predictions are the major attacks faced in this layer [19]. TCP flooding or Ping flooding is another type of DoS attack where the attacker sends a significant number of ping requests to a target or group of targets such as Address Resolution Protocol (ARP) echo requests, and the target responds by sending ping replies. This will eventually cause flooding for the target node's input and output buffers, as well as connection delay, especially if the ping requests are of a substantial amount. To perform a TCP sequence number prediction attack, the attacker tries to estimate the TCP segment sequence index of the source node, fabricates the segment, and then sends it to the target receiver. This has thus infringed on the integrity of the packet. UDP flooding is similar to TCP flooding; however, instead of sending ping queries, malicious UDP packets are delivered to the target node, forcing it to respond to these multiple packets, rendering the node unreachable to other authorized nodes in the network. A firewall can be used to defend against this attack as well as to limit the response rate of UDP segments.

2.3.5 Application layer attacks

This is the last layer of the OSI model, but the first layer that the users interact with. It comprises various protocols such as HTTP, FTP, and SMTP. However, these protocols expose this layer to several security vulnerabilities. There are five major application-layer attacks which include malware attacks, SQL injection, SMTP attack, FTP bounce, Cross-site scripting that can be categorized under HTTP attacks, FTP attacks, and SMTP attacks [17]. The malware attack is an example of attacks categorized under the HTTP attacks that include key loggers, backdoors, worms, viruses, and Trojan horse. A malware refers to any damaging software in the form of code or script developed by an attacker to interrupt the authorized transmission or steal confidential data. SQL injection is another type of HTTP attack commonly used to exploit data-driven systems by inserting malicious SQL statements to gain unauthorized access to a website. Cross-site scripting is also another type of HTTP attack where the attacker inserts client-side script into a web page causing the browser to automatically download malicious scripts when the user loads the web page, thus allowing the attacker to easily bypass security restrictions and steal sensitive information such as cookies information and perform other series of malicious activity [21]. An FTP bounce attack is when an attacker exploits the vulnerabilities of the FTP protocol using the PORT command to request port access using a victim's IP address, acting as a middleman. The SMTP is the protocol utilized to send emails over the Internet, but lacks encryption for sensitive information such as user credentials or the original message contained in the email, which has raised severe privacy issues. The SMTP attack includes password sniffers, SMTP viruses, worms, and email spoofing [18].

Table 2.2 presents the summary and taxonomy of the major attacks in each layer of the OSI reference model.

Table 2.2 Attacks in the OSI layers

OSI layers	Major attacks
Physical layer	Eavesdropping and Jamming attacks
MAC layer	MAC spoofing, MITM, identity theft, and network injection
Network layer	IP spoofing, IP hijacking, and Smurf attacks
Transport layer	TCP flooding, UDP flooding, and TCP sequence number
Application layer	Malware attacks, SQL injection, SMTP attack, FTP bounce, cross-site scripting

2.4 Security and privacy in wireless communication

This section presents the various security and privacy issues and vulnerabilities of the different cellular generations from 1G to 5G.

2.4.1 1G

There are several limitations in the 1G network as mentioned earlier, one of which is in terms of security. Both the AMPS and TACS did not have authentication and data encryption because 1G was analog, making it relatively simple for the interception of calls and the retrieval of the two unique identities, which include the mobile identity number (MIN) and the electronic serial number (ESN), which can be utilized to impersonate a device on the network. This can thus lead to an impersonation attack [22]. However, the first security measure implemented in 1G to defend against eavesdropping is known as voice scrambling which was used in Nordic Mobile Telephone (NMT) for both the mobile station (MS) and the base station (BS). Although, it was not a particularly strong encryption technique, it did prevent call interception by attackers [23].

2.4.2 2G – GSM

The digital nature of the 2G wireless network enabled the security limitations of the 1G network to be adequately addressed, particularly with the introduction of cryptography for authentication and the subscriber identity module (SIM) for verifying user's identity. However, the 2G network also has security and privacy issues. For example, spamming is one of the major security issues where attackers send unwanted messages to victims. Furthermore, the Abis interface, which is the interface between the BS and BS controller (BSC), is not encrypted. As a result, audio and signaling signals can be easily intercepted by attackers who can intercept E1-based communication. Another vulnerability is that the only method operators can authenticate the MS is through a unilateral process, which leaves the MS with no way to verify the operator, allowing an attacker to pose as the actual operator and launch an MITM attack [24]. A fabricated BS can be erected with a higher transmitting power than the other, making it the most preferred BS for several MSs to interact with. This can result in session hijacking, which is an attack on network

authentication in 2G, where an attacker may be able to obtain the international mobile subscriber identity (IMSI) information from the MS [22]. Furthermore, some of the security solutions deployed in the 2G network were shown to have serious weaknesses, such as the COMP128 and A5 cryptographic algorithms, which were used to provide radio-path encryption and user authentication, respectively [25].

2.4.3 3G – UMTS

The 3G mobile system was developed to overcome the limitations in the 2G mobile systems including the security issues identified. In the 3G network, security measure implemented can be classified into five as follows: Network Access Security, User Domain Security, Application Security, Network Domain Security, and, finally, Visibility and Configurability Security. This thus provided flexibility and possible scalability to accommodate new threats. However, with the significant number of users, the network vulnerabilities were exposed and easily exploited. They include eavesdropping, access to confidential information, MITM, DoS, location update spoofing, as well as identity theft attacks [23].

2.4.4 4G – LTE

The 4G network provided security solutions to the security flaws identified in the previous generation as well as new cryptographic algorithms. The evolved packet system (EPS) encryption and EPS integrity algorithms as well as the use of 256 bits were the major security measure that was introduced and implemented in 4G network. Further significant improvement seen in the 4G network as regard to security includes the utilization of different algorithms and key sizes for the user and control plane traffic. However, the 4G network is IP-based and utilizes diameter signaling which made it less secure and very vulnerable against various attacks which include eavesdropping attacks, TCP flooding attacks, user identity theft, DoS attack, intrusion attack, address spoofing, GPRS tunneling protocol (GTP)-based attacks, particularly the backhaul traffic in 4G network. It also has many entry points including compromised smart mobile devices and access networks [26]. Furthermore, authentication in the 4G network was provided by the EPS-Authentication and Key Agreement (EPS-AKA). However, it was still susceptible to various vulnerabilities such as user identity theft and impersonation, computational overhead, MITM attack, malware spreading, and authentication delay [27].

2.4.5 5G

The 5G network addresses most of the crucial limitations of the earlier generations while facilitating requirements such as increased data rate and capacity, enhanced device connectivity, reduced cost and latency, and guaranteed quality of service (QoS) [28]. However, the 5G network is also faced with security issues due to the numerous applications and technologies it supports. To evaluate these security issues, it is imperative to analyze the threats and vulnerabilities of the enabling technologies.

2.4.5.1 Device-to-device (D2D) communication

D2D communication allows users to connect directly without the usage of BSs or access points (APs) [29]. It offers various benefits in terms of spectrum efficiency, expansion of coverage, increase in capacity, radio resource reusing, management of power, etc. It is regarded to be the fundamental technology for developing point-to-point communications to obtain improved coverage and higher data speeds for 5G user devices [30]. D2D communication is similar to vehicle to everything (V2X) communication and M2M communication which are also enabling technologies in 5G wireless network. Some of the characteristics of D2D communication include the following: the utilization of the open-air transmission which is freely accessible, the network comprising mobile phones, exposure of the network architecture, and the limited resources (bands and channels). These characteristics make the 5G technology vulnerable to several attacks including eavesdropping, jamming, DoS attacks, and injection attacks. Although different solutions have been utilized to combat these attacks. For instance, movement from the eavesdropper was a proposed solution for an eavesdropping attack [29].

2.4.5.2 Network function virtualization (NFV)

NFV is another essential enabling technology in 5G wireless networks, allowing for customized network slicing across distributed clouds to build programmable networks for 5G applications. In other words, it is one of the solutions for 5G automation in the service provider production environment because it enables service providers to design network functions such as firewall, Intrusion Detection, Network Address Translation (NAT), Domain Name Service (DNS), dynamic that meets Service Level Agreements (SLAs) and service models by implementation in software running on clouds accessible from a centralized repository [31,32]. Although the NFV technology has numerous benefits, it has security issues which makes it vulnerable to attacks such as configuration attack, DoS attack, hijacking attack, penetration attacks, and resource (network slice) theft attacks [33].

2.4.5.3 Software-defined network (SDN)

The SDN, similar to the NFV, allows for a centralized and programmable network management function in a software-oriented network management platform while the infrastructure of the network deals with the applications and network service [34]. This simplifies network control, management, and operation while also accelerating the development and deployment of network features. However, due to the fact that the network control is centralized, it makes the controller a bottleneck for the entire network which can be vulnerable to several attacks including eavesdropping, DoS, hijacking, configuration, MITM, and saturation attacks. Saturation attack also known as malware spreading attack, where if a malicious application is to be granted access, it can easily spread throughout the network [33].

2.4.5.4 Massive MIMO

Massive MIMO (mMIMO) is also known as an extensive antenna system where a base station is equipped with more than 100 antennas' elements that would be

utilized to service a significant number of users simultaneously with a frequency band. It is one of the core enabling technologies of the 5G wireless network, improving its data speed and bandwidth efficiency while servicing a significant number of users [35]. Some advantages of this technology include lower latency and energy usage, simplified MAC layer, and increased capacity because of spatial multiplexing. mMIMO is vulnerable to majorly eavesdropping attack which can be either passive or active [24].

2.4.5.5 HetNet

HetNet is one of the solutions proposed to enhance the 5G network and it encompasses key elements such as small cells, mMIMO, mmWaves, and D2D communication [36]. The deployment of low-power base stations or small cells was proposed as a method to densify the network due to the increasing need for high data rates to operate applications. This would result in higher spectral efficiency as well as reduce the power consumption of mobile phones due to its communication with nearby small cells. Modern methods of data transmission used by small cells in 5G wireless network include beamforming, millimeter wave, and MIMO. HetNet is vulnerable to several attacks including eavesdropping, DoS, jamming, MITM, and hacking attacks [37].

From this brief review of the key enabling technologies in 5G wireless network, it can be seen that they are all vulnerable to different attacks, particularly eavesdropping attacks, based on their features, thus making the 5G network itself to be vulnerable. The taxonomy of these various attacks in cellular communication across the generations are presented in Table 2.3.

Table 2.3 Taxonomy of attacks in cellular communication

Attacks	1G	2G	3G	4G	5G
Eavesdropping	✓	✓	✓	✓	✓
Jamming	×	×	×	✓	✓
Identity theft & impersonation	✓	×	✓	✓	×
Spamming	×	✓	×	×	×
Fabricated BS	×	✓	✓	×	×
MITM	✓	×	✓	×	✓
DoS/DDoS	×	×	✓	✓	✓
Spoofing	×	×	✓	×	✓
TCP or UDP flooding	×	×	×	✓	✓
Malware	×	×	×	✓	✓
Injection	×	×	×	×	✓
Sniffing	×	×	×	×	✓
Hijacking	×	×	×	×	✓
Configuration	×	×	×	×	✓
Network slice theft	×	×	×	×	✓
Penetration	×	×	×	×	✓

2.5 Emerging wireless communication systems

This section presents and discusses the different emerging wireless communication system as well as provides a brief review of different research works that have considered these technologies and systems.

2.5.1 Low-cost IoT devices

Internet of Things (IoT) simply refers to a connection of physical objects, such as microwaves, doors, fans, and lighting integrated with electronic sensors and software to allow collection and sharing of data using a communication protocol. The collected data are sent to the server or microcontroller for further analysis which then processes the information to derive knowledge and translate them into a particular action [38]. One of the requirements of an IoT system is low cost which can be met using boards based on Alf and Vegard's RISC (AVR) processors including the Arduino as well as the ESP8266 board. These boards widely utilized several applications and systems including GPS trackers, home assistants, inventory management system, and can be configured with the Arduino Integrated Design Environment (IDE) [39]. The Arduino microcontroller, however, was seen to be the least expensive when compared with other latest existing microcontrollers [40]. The different types of Arduino boards as well as the working principle have been reviewed in [41]. To fully comprehend the potential of IoT, it is imperative to examine its convergence with the 5G wireless network which among other things, offers to manage the complexities of IoT such as scalability, wider coverage, backhaul connectivity, cost, and installation, accomplished using the 5G enabling technologies [42]. It is estimated that there would be a significant number of connected IoT devices that would produce enormous amounts of data and this has led to the development of an architecture known as the 5G I-IoT model, that is, the convergence of 5G, AI, and IoT [43]. This has found application in critical services such as remote healthcare, VAR, drones, security surveillance, and autonomous cars as shown in Figure 2.3. However, security is the major challenge faced by the 5G I-IoT environment due to the openness of the network and the lack of robust security schemes [43]. As a result, the 5G I-IoT environment is vulnerable to several attacks including eavesdropping, replay, MITM, impersonating, and malware attacks [43].

2.5.2 Ultra-reliable and low latency communications (URLLC)

The URLLC is one of the key application scenarios in the 5G New Radio (NR) defined by the International Telecommunication Union (ITU-R) along with eMBB and massive machine-type communication (mMTC) to satisfy the requirements of several mission-critical applications, such as remote healthcare, drone-based logistics, factory automation, smart grid, autonomous cars, VAR, and AI-based personal assistants, among others, that require low latency, better reliability, high connection density, higher throughput, and scalability [44,45]. Figure 2.4 shows the various applications as well as the key requirements of URLLC.

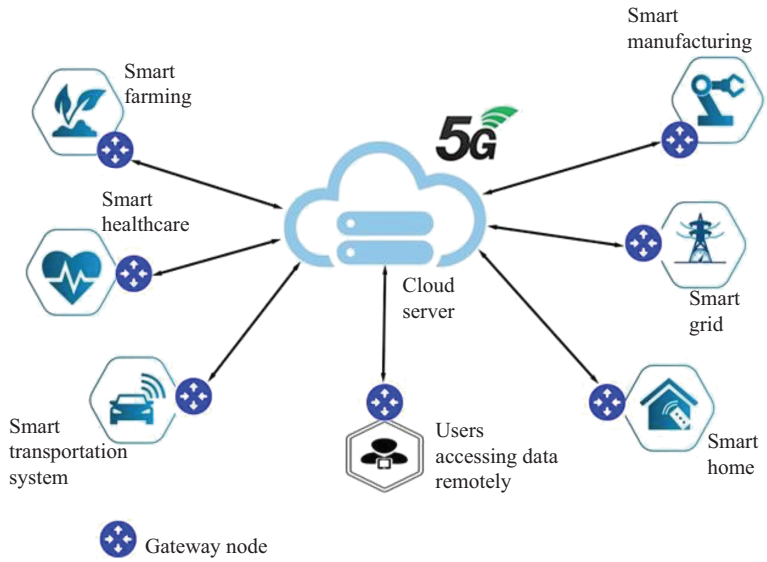


Figure 2.3 5G I-IoT environment [43]

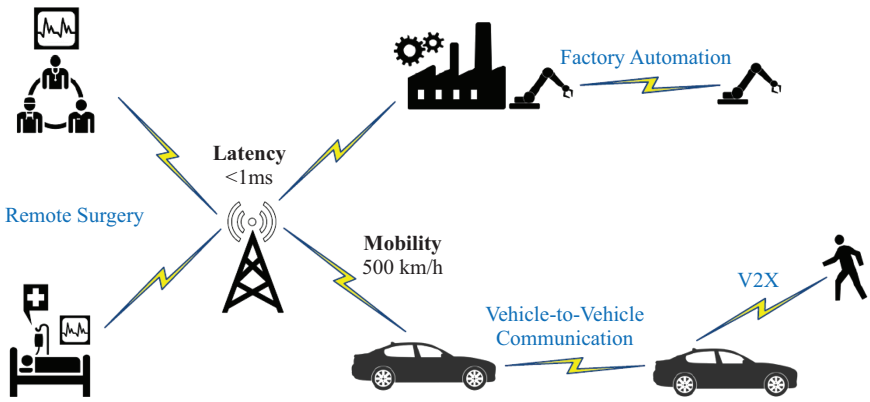


Figure 2.4 Applications and key requirements of URLLC [46]

Ultra-reliability and reduced latency are the two key requirements of the URLLC. Where reliability is the capability to transmit a specific volume of packet with high success rate within a particular period, latency refers to the delay in an accurate transmission from the source to the destination [47]. In other words, latency is the time required for a packet to make a round-trip across the network. It is classified into User Plane Latency (UPL) and Control Plane latency (CPL). The

UPL is the required time taken between when the sender transmits the packet to when the receiver receives it and according to the ITU-R, the minimum requirement of UPL in URLLC is 1 ms, assuming unloaded conditions with small packets for both uplink and downlink [47]. The CPL, on the other hand, is the time taken between when the user equipment (UE) changes status from idle state to active state. According to the ITU-R, the minimum requirement of the CPL is 20 ms, but less than 10 ms is most preferred [47].

Security challenges associated with most URLLC applications are also critical, as an attack can have disastrous consequences. For example, if a remote surgeon's communication is hijacked by an attacker, the entire communication will not only slow down but the patient's life is also endangered. The major attack in the URLLC application scenario is the eavesdropping attack which is an attack on confidentiality and privacy. To ensure confidentiality and protection against eavesdropping attacks, cryptography algorithms have been widely used in traditional networks. For URLLC, however, these cryptography algorithms are not efficient and may affect the two key requirements of URLLC due to the high-intricacy signal processing used for encrypting and decrypting. Key distribution may cause an additional delay in some application scenarios [5]. The physical layer security (PLS) has been proposed and demonstrated to be a potential solution for protecting against attacks in 5G URLLC network such as eavesdropping attacks because unlike cryptography, PLS does not require a key exchange for encryption and decryption [5].

2.5.3 eMBB

The eMBB is another key application scenario in 5G NR and an extension of the 4G broadband service. eMBB is concerned with the provision of increased data rate, enhanced connectivity and mobility. High throughput is the key requirement of eMBB which is to increase data rate while ensuring reasonable accuracy with a packet error rate (PER) of around 10^{-3} [48,49]. Throughput is generally referred to as the rate at which information is successfully delivered over a channel. It is affected by various factors such as channel type, network protocol, user density, packet loss, power, latency, and bandwidth [48]. Different techniques have been utilized to improve mobile broadband [50]; however, three strategies – broadband expansion, cell density expansion, and spectral efficiency increase – were utilized to increase the throughput of the 5G network [48]. To increase the bandwidth, the 5G network utilized the millimeter wave band and adopted flexible TDD as well as full duplex schemes. To increase the cell density, increased cell density was adopted as well as a heterogeneous network which include small cells. To enhance the efficiency of the spectrum, low-density parity-check (LDPC) codes as well as mMIMO were adopted. Figure 2.5 shows the various applications as well as the key requirement of eMBB.

For eMBB, two major security issues are associated with it. They lack adequate monitoring system and user privacy leakage [51]. The eMBB applications such as 4K/8K high-definition video streaming, and VAR-based mobile roaming

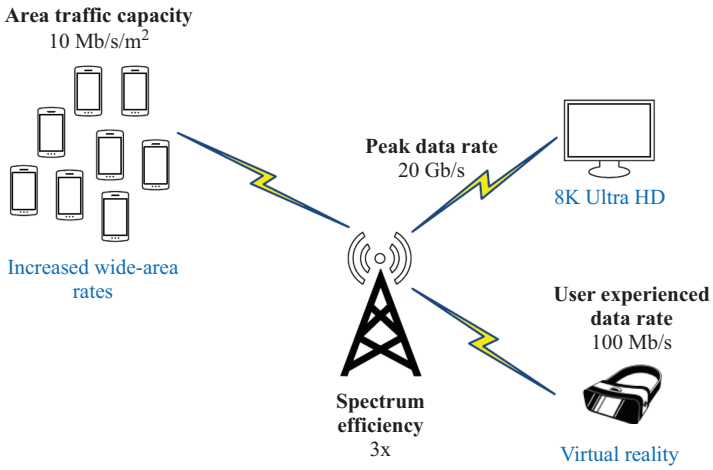


Figure 2.5 Applications and key requirements of eMBB [46]

immersive services produce an enormous amount of traffic which makes it difficult to monitor using security nodes including Firewalls and Intrusion Detection systems [51]. Furthermore, user privacy leakage can occur due to the openness of the network as these services and applications supported contain users-sensitive information including device identification and address identification.

2.5.4 Massive machine-type communication (mMTC)

mMTC, another key application scenario defined by the ITU-R, is also known as massive M2M (mM2M) communication that supports a significant number of devices to directly communicate with one another or to access the Internet with or without any human inputs [48]. Connection density and network energy efficiency are the two key requirements of the mMTC with the aim of connecting a significant number of low-rate energy-saving devices, also known as machine-type devices, to cellular network [46,52]. Figure 2.6 shows the various applications as well as the key requirements of mMTC.

Connection density, in this context, is concerned with the capability of the 5G network to support a very large number of device connections to the Internet, particularly IoT devices while network energy efficiency is the capability of the radio access technology (RAT) to reduce the consumption of energy of the radio access network (RAN) in respect to the generated amount of traffic. Various techniques have been proposed and developed to satisfy these requirements. However, similar to the other scenarios, the mMTC is also vulnerable to various threats and attacks which include fake terminals, modification attacks, eavesdropping attacks, and remote control due to the simplicity of the IoT devices and weak security protection capabilities [51].

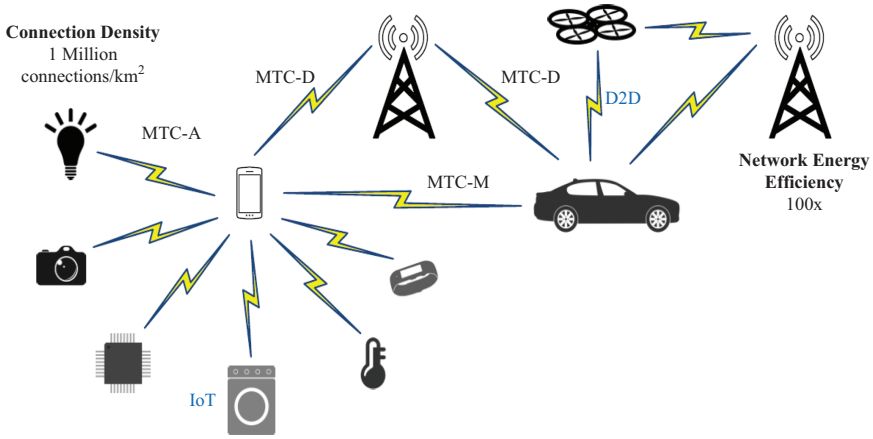


Figure 2.6 Applications and key requirements of mMTC [46]

2.6 Application of AI and ML to wireless security system design

In this section, AI and ML are introduced and a brief review of the application of AI and ML to the security aspect of wireless communication is carried out. As illustrated in Figure 2.7, AI is a vast field that covers both ML and deep learning (DL). AI is a general phrase that refers to computer intelligence that may replicate human intelligence and abilities including learning, reasoning, decision-making, perception, and problem-solving [48].

ML, on the other hand, is a subset of AI with a focus on extracting knowledge from a significant amount of data. It refers to the capability of machines to learn without being explicitly programmed. AI and ML have proven their effectiveness in various fields including medicine, education, engineering, transportation, industrial robotics, agriculture, etc., for their high accuracy in terms of classification, identification, and automation. Similarly, AI and ML have been utilized to develop, simulate, and implement several efficient and effective security algorithms to defend against various threats and attacks [53].

ML was applied for detecting jamming attack in [54] for wireless IoT networks using the received signal strength indication (RSSI) data from both simulation and real networks where the results obtained after analysis showed that the proposed model achieved high accuracy with no communication cost or overhead for nodes in the network. Similarly, the work [55] used ML for the detection of distributed DoS (DDoS) for consumer IoT devices where results showed that routers or other intermediary nodes can detect sources of the DDoS attack automatically using the proposed low-cost ML algorithm.

Furthermore, the work [56] proposed an ML-based antenna design scheme to enhance the security of IoT network where the simulation results obtained showed

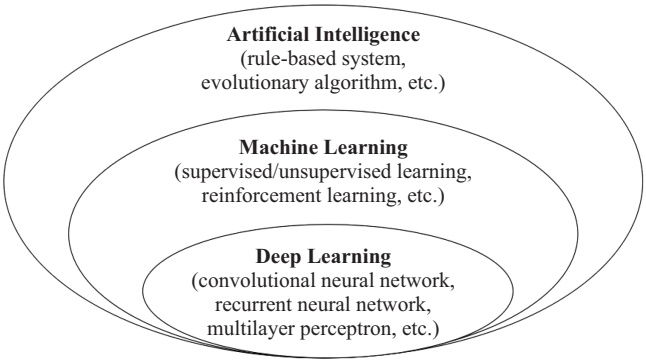


Figure 2.7 Relationship between AI, ML, and DL [48]

that the proposed scheme is suitable to be applied in PLS communication in which signal-to-noise ratio (SNR) of wiretap channels is decreased while ensuring reliable communication on the major channel thus preventing the leakage of information. The work [57] proposed a model that can detect abnormalities in an IoT network using deep neural network (DNN) with chicken swarm optimization (CSO) where results showed that the proposed model is highly accurate with better detection rate compared to other models. An ML-based security approach was proposed in [58] for autonomous IoT systems to achieve optimal energy efficiency and better reliable transmission. Results showed that the proposed model optimized the network performance, achieved fault–tolerant data transmission, and accomplished network confidentiality against adversaries using a cryptography-based deterministic algorithm. Further reviews of AI- and ML-based techniques for the security of IoT systems were presented in [59,60] against various threats and attacks including the future challenges when employing these techniques.

A generative adversarial network (GAN), an unsupervised learning scheme, was utilized in [61] to secure wireless sensor network middleware. Results obtained showed that the algorithm improves the data accuracy and ensures protection from adversaries with less energy, and throughput compared to other conventional schemes. Similarly, the work [62] reviewed the AI applications for intrusions detection in software-defined wireless sensor network (SDWSN) where it was shown that AI techniques are effective techniques that can be used in SDWSNs to defend against malicious attacks. Further reviews of the security of IoT and WSNs against various threats and attacks using ML techniques are presented in [63].

In [64], the constraints of traditional cryptographic and physical layer authentication solutions, such as low dependability, increased latencies, and security overheads, led to the application of ML for intelligent authentication in 5G and beyond wireless networks. Similarly, the work in [46] investigated the ML contributions to satisfying each target requirement of the 5G network, particularly the 5G use cases. The research showed that ML can be utilized as a solution mechanism to solve some of the impending issues in the 5G-and-beyond network.

Furthermore, the work [53] presented the AI- and ML-driven applications for the security of the 5G network, their challenges as well as future research recommendations.

From the brief review, it can be seen that both AI and ML have been proven to be effective solutions to the security issues in wireless communication, particularly in IoT, WSNs, and mobile communication systems, against adversaries such as eavesdropping attacks, DDoS attacks, intrusion attacks, and jamming attacks. It was also seen that these learning-based techniques are energy-efficient while ensuring confidentiality without security overheads and can be applied to the security of future wireless communication systems. However, there are gaps to fill in this research area.

2.7 Security issues and challenges in future wireless communication systems

The future wireless communication system, that is, the 5G-and-beyond network or simply 6G wireless network, is faced with different security threats and attacks. This section presents these issues and challenges as well as proffers further research directions.

The 5G wireless network addressed the limitations of the previous network generations by facilitating increased reliability, ultra-low latency, connection density, increased throughput, network energy efficiency, and low IoT devices using the key application scenarios as discussed in Section 2.2. However, the 5G wireless network is also insecure due to the numerous applications and enabling technologies such as NFV, SDN, HetNet, M2M, and D2D communication, that it supports. They are vulnerable to different attacks including eavesdropping, MITM, impersonation, hijacking, malware, and sniffing attacks to mention a few. This motivated the interest of researchers and other stakeholders who have tried to propose algorithms to defend against these attacks. This include the use of the PLS technique to protect against eavesdropping attacks instead of cryptographic algorithms which are not efficient. However, there are still gaps to fill in this research area.

A glimpse into the future presents the 6G wireless network which promises to have a radio latency as low as 0.1 ms, one-tenth of the 5G network, and supports both underwater and space communication [65]. There is a plethora of advantages that the 6G wireless network has over the existing 5G network. Figure 2.8 shows the emerging use cases for the 6G wireless network.

The 6G network has numerous security issues and challenges as a result of the key-supported technologies and applications that are discussed as follows.

2.7.1 AI

AI, as discussed earlier, is a very broad field that has so many applications in various aspects of our daily lives. Specifically, AI is commonly regarded as one of the important technologies in the future wireless networks [65]. For a complete autonomous network, the 6G network depends on AI. Therefore, threats and attacks

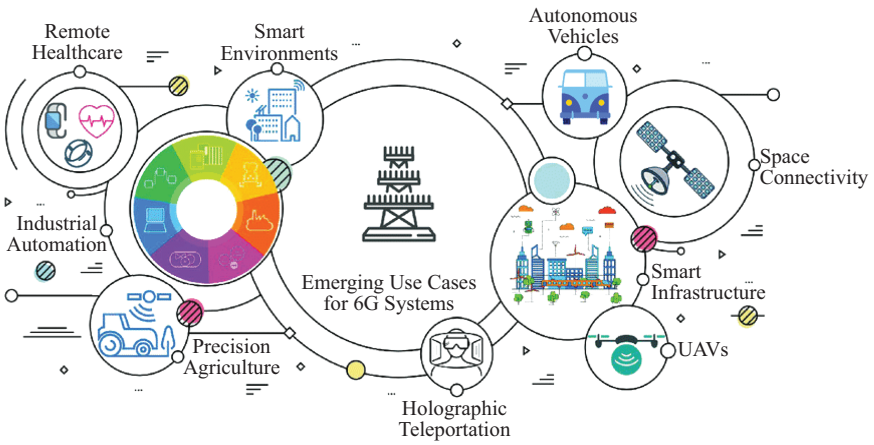


Figure 2.8 6G emerging use cases [3]

against AI systems, especially ML-based systems such as a poisonous attack, model manipulation, data manipulation, data injection, membership inference, and logic corruption attacks, would also affect 6G [66].

2.7.2 Molecular communication (MC)

MC is one of the key technologies in 6G network that enables information transmission using biochemical signals which is a solution to allow introduction of human in-body nano-networks under the scope of Internet of nano-things [67,68]. In MC, information is encoded using the concentration, release time, and type of molecules. Also, the propagation from the source to the destination can be passive, involving only molecular diffusion, or active, involving diffusion–advection and molecular motors [68]. Various threats and attacks have been identified at several levels of MC which include Jamming, flooding, and desynchronization attacks [66].

2.7.3 Quantum communication (QC)

QC is one of the technologies with promising applications in the 6G wireless network. Enhancement of security as well as the accurate delivery of transmitted data is one of most significant advantages of QC where if an attacker tries to interfere, interrupt, or modify the data, the quantum state would be affected; thus the receiver would be aware if interference has occurred [66]. QC offers a lot of solutions and is suitable for long-distance communication. However, it is not a universal remedy to all security threats and attacks as it is vulnerable to quantum cloning attacks and quantum collision attacks [69].

2.7.4 Blockchain

Blockchain technology is another technology that will unveil the potential of 6G network. It has a wide range of possible applications, some of which include

spectrum sharing, distributed ledger technology, and network decentralization [66]. The blockchain technology is regarded as an essential technology for establishing trust in future wireless networks, and it has found applications in smart contracts, national ID systems, censorship resistance systems, bitcoins, healthcare systems, and other areas [70]. However, the blockchain technology also has several security issues, which include 51% attacks, forking issues, eclipse attacks, application bugs, short address, timestamp dependence, scalability issues, regulatory issues, and integration issue related to network access management, communication procedures, and authentication [71].

2.7.5 Terahertz (THz) technology

mmWave bands have been extensively used to satisfy the demands of the 5G network, but they are insufficient for the 6G network due to increased transmission rate demand. Additionally, the radio frequency is nearly exhausted and cannot be used for future wireless networks. As a result, the terahertz communication, which operates in the 0.1–10 THz band, has been proposed to be used for future wireless communication. Due to numerous benefits of the 6G wireless network which include supporting data rate of up to 100 Gbps or higher, minimized attenuation through certain materials and because of its narrow beam and short pulse duration, THz can be utilized to minimize the probability of eavesdropping. However, there are other security challenges in THz wireless communication as the technology is susceptible to access management attacks [69].

2.7.6 Visible light communication (VLC)

The VLC, a technology that utilizes visible spectrum light waves to transmit signals with wavelength range of 380–750 nm, is another emerging technology that can be employed to address the ever-increasing demand for wireless connectivity in future wireless communication systems [72]. The benefits of the technology include the use of unlicensed frequency with free-of-charge optical bandwidth, cost effectiveness, longevity, and energy-saving. VLC is thought to be more secure than other wireless technologies since its coverage is restricted to devices that are open to light, implying that it has fewer security weaknesses than radio frequency [72]. The VLC is also facing some security and privacy challenges which include eavesdropping attacks and jamming or data modification attacks [69]. Further reviews of the security issues and challenges in the 6G wireless network can be seen in [65,69].

2.8 Conclusions and recommendations

Wireless communication is one of the most successful technologies that has impacted our daily lives. This chapter has presented the historical description of wireless communication focusing on the mobile generations from 1G to 5G as well as the various security and privacy issues and vulnerabilities. The emerging wireless communication systems in the 5G wireless network have also been discussed and the application of AI and ML to wireless security design has been reviewed.

The various security issues and challenges in the 6G wireless network based on the key technologies have been briefly reviewed. The review on the security issues and challenges has shown that both 5G and 6G are vulnerable to threats and attacks. Although some key highlighted technologies such as AI, THz, and QC have been utilized to defend against some security threats and attacks such as eavesdropping attacks, however, these technologies are also vulnerable to several attacks.

In the future work, further research issues which can assist the global communities to achieve improved security for the 5G wireless network and beyond have been identified and elaborated. Some efforts on potential solutions to these several attacks are yet to meet the requirements of future wireless communication networks as the current security protocols are limited in terms of efficiency, overhead information, robustness, and would be unable to handle massive connections and large amount of data as the authentication mechanisms requires a longer period to complete preliminary authentication. Further research especially in the following areas is therefore recommended:

1. The development of novel delay-sensitive and robust protocols for security and privacy against different attacks across all the OSI layers of the 5G-and-beyond network.
2. The modification and optimization of existing security protocols to meet the fast pace requirement of the 5G-and-beyond wireless network as well as dynamic nature of the attacks across all the OSI layers.

References

[1] C. Azad, S. Agrawal, T. Medininagar, and V. K. Jha, "Security, privacy and accountability in wireless network: a review," *Int. J. Eng. Res. Technol.*, vol. 2, no. 7, pp. 399–408, 2013.

[2] S. B. Sadkhan and N. A. Abbas, "Privacy and security of wireless communication networks," in *Mobile Networks and Cloud Computing Convergence for Progressive Services and Applications*, IGI Global, Pennsylvania, PA, 2013, pp. 58–78. doi: 10.4018/978-1-4666-4781-7.ch004.

[3] I. F. Akyildiz, A. Kak, and S. Nie, "6G and beyond: the future of wireless communications systems," *IEEE Access*, vol. 8, pp. 133995–134030, 2020, doi: 10.1109/ACCESS.2020.3010896.

[4] K. R. Rao, S. N. T. Rao, and P. C. Reddy, "Wireless communication security and privacy issues and challenges," *Int. J. Comput. Sci. Inf. Secur.*, vol. 15, no. 7, pp. 202–209, 2017.

[5] R. Chen, C. Li, S. Yan, R. Malaney, and J. Yuan, "Physical layer security for ultra-reliable and low-latency communications," *IEEE Wirel. Commun.*, vol. 26, no. 5, pp. 6–11, 2019, doi: 10.1109/MWC.001.1900051.

[6] A. Maitra, "Early history of wireless communications," in *Souvenir of 33rd Annual Convention of Radio Physics and Electronics Association, University of Calcutta*, 2003.

[7] M. H. Mahmud, "Cellular mobile technologies (1G to 5G) and massive MIMO," *Int. J. Sci. Res.*, vol. 8, no. 7, pp. 929–937, 2019. Available: https://www.researchgate.net/profile/Md-Mahmud-22/publication/349493734_Cellular_Mobile_Technologies_1G_to_5G_and_Massive_MIMO/links/608c112192851c490fa9c763/Cellular-Mobile-Technologies-1G-to-5G-and-Massive-MIMO.pdf

[8] S. Patel, V. Shah, and M. Kansara, "Comparative study of 2G, 3G and 4G," *Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol.*, vol. 3, no. 3, pp. 1962–1964, 2018.

[9] M. Arshad, A. Farooq, and A. Shah, "Evolution and development towards 4th generation (4G) mobile communication systems," *J. Am. Sci.*, vol. 6, no. 12, pp. 6, 2010.

[10] N. Rawat, "Future and challenges of 4G wireless technology," *Int. J. Sci. Eng. Res.*, vol. 3, no. 12, pp. 1–7, 2012. Available: http://www.ijser.org/researchpaper%5CFuture-and-Challenges-of-4G-Wireless-Technology.pdf

[11] B. S. Usmonov, R. O. Sattorivich, and U. A. Rustamov, "5g Technology evolution," in *International Conference on Information Science and Communications Technologies: Applications, Trends and Opportunities, ICISCT 2019*, 2019, pp. 1–5. doi: 10.1109/ICISCT47635.2019.9011957.

[12] M. Attaran, "The impact of 5G on the evolution of intelligent automation and industry digitization," *J. Ambient Intell. Humaniz. Comput.*, vol. 2021, pp. 1-17, 2021, doi: 10.1007/s12652-020-02521-x.

[13] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A survey on wireless security: technical challenges, recent advances, and future trends," *Proc. IEEE*, vol. 104, no. 9, pp. 1727–1765, 2016, doi: 10.1109/JPROC.2016.2558521.

[14] H. N. Dai, H. Wang, H. Xiao, X. Li, and Q. Wang, "On eavesdropping attacks in wireless networks," in *Proceedings – 19th IEEE International Conference on Computational Science and Engineering, 14th IEEE International Conference on Embedded and Ubiquitous Computing and 15th International Symposium on Distributed Computing and Applications to Business*, Engi, 2017, pp. 138–141, doi: 10.1109/CSE-EUC-DCABES.2016.173.

[15] A. Mpitziopoulos, D. Gavalas, C. Konstantopoulos, and G. Pantziou, "A survey on jamming attacks and countermeasures in WSNs," *IEEE Commun. Surv. Tutorials*, vol. 11, no. 4, pp. 42–56, 2009, doi: 10.1109/SURV.2009.090404.

[16] Y. Arjoune, F. Salahdine, M. S. Islam, E. Ghribi, and N. Kaabouch, "A novel jamming attacks detection approach based on machine learning for wireless communication," in *International Conference on Information Networking*, January 2020, vol. 2020, pp. 459–464, doi: 10.1109/ICOIN48656.2020.9016462.

[17] P. Sinha, V. K. Jha, A. K. Rai, and B. Bhushan, "Security vulnerabilities, attacks and countermeasures in wireless sensor networks at various layers of OSI reference model: a survey," in *Proceedings of IEEE International Conference on Signal Processing and Communication, ICSPC 2017*, January 2018, vol. 2018, pp. 288–293, doi: 10.1109/CSPC.2017.8305855.

[18] G. K. Ijemaru, I. A. Adeyanju, K. O. Olusuyi, T. J. Ofusori, E. T. Ngharamike, and A. A. Sobowale, "Security challenges of wireless

communications networks: a survey," *Int. J. Appl. Eng. Res.*, vol. 13, no. 8, pp. 5680–5692, 2018, [Online]. Available: http://www.ripublication.com

[19] E. Sula, "A review of network layer and transport layer attacks on wireless networks.," *Int. J. Mod. Eng. Res.*, vol. 8, no. 12, pp. 23–27, 2018.

[20] X. Hu and Z. M. Mao, "Accurate real-time identification of IP prefix hijacking," *Proceedings – IEEE Symposium on Security and Privacy*, 2007, pp. 3–17, doi: 10.1109/SP.2007.7.

[21] X. Wang and W. Zhang, "Cross-site scripting attacks procedure and prevention strategies," in *MATEC Web Conference*, 2016, vol. 61, p. 3001, doi: 10.1051/matecconf/20166103001.

[22] F. Njoroge and L. Kamau, "A survey of cryptographic methods in mobile network technologies from 1G to 4G," *Jomo Kenyatta Univ. Agric. Technol.*, vol. 10, no. 4, pp. 1–6, 2018.

[23] S. Sullivan, A. Brighente, S. A. P. Kumar, and M. Conti, "5G security challenges and solutions: a review by OSI layers," *IEEE Access*, vol. 9, pp. 116294–116314, 2021, doi: 10.1109/ACCESS.2021.3105396.

[24] I. Ahmad, S. Shahabuddin, T. Kumar, J. Okwuibe, A. Gurtov, and M. Ylianttila, Security for 5G and beyond, *IEEE Commun. Surv. Tut.*, vol. 21, no. 4, pp. 3682–3722, 2019, doi:10.1109/COMST.2019.2916180.

[25] S. Gindraux, "From 2 G to 3G: a guide to mobile security," in *Third International Conference on 3G Mobile Communication Technologies*, no. 489. 2002, doi:10.1049/cp:20020410.

[26] S. Mavoungou, G. Kaddoum, M. Taha, and G. Matar, "Survey on threats and attacks on mobile networks," *IEEE Access*, vol. 4, pp. 4543–4572, 2016, doi: 10.1109/ACCESS.2016.2601009.

[27] K. A. Alezabi, F. Hashim, S. J. Hashim, and B. M. Ali, "An efficient authentication and key agreement protocol for 4G (LTE) networks," in *IEEE TENSYMP 2014 – 2014 IEEE Region 10 Symposium*, 2014, pp. 502–507, doi: 10.1109/tenconspring.2014.6863085.

[28] A. K. Jain, R. Acharya, S. Jakhar, and T. Mishra, "Fifth generation (5G) wireless technology 'Revolution in Telecommunication,'" in *Proceedings of the International Conference on Inventive Communication and Computational Technologies, ICICCT 2018*, 2018, pp. 1867–1872, doi: 10.1109/ICICCT.2018.8473011.

[29] A. Celik, J. Tetzner, K. Sinha, and J. Matta, "5G device-to-device communication security and multipath routing solutions," *Appl. Netw. Sci.*, vol. 4, no. 1, pp. 102, 2019, doi: 10.1007/s41109-019-0220-6.

[30] N. T. Le, M. A. Hossain, A. Islam, D. Y. Kim, Y. J. Choi, and Y. M. Jang, "Survey of promising technologies for 5g networks," *Mob. Inf. Syst.*, vol. 2016, p. 25, 2016, doi: 10.1155/2016/2676589.

[31] B. Han, V. Gopalakrishnan, L. Ji, and S. Lee, "Network function virtualization: challenges and opportunities for innovations," *IEEE Commun. Mag.*, vol. 53, no. 2, pp. 90–97, 2015, doi: 10.1109/MCOM.2015.7045396.

[32] A. A. Barakabitze, A. Ahmad, R. Mijumbi, and A. Hines, "5G network slicing using SDN and NFV: a survey of taxonomy, architectures and future

challenges," *Comput. Netw.*, vol. 167, p. 106984, 2020, doi: 10.1016/j.comnet.2019.106984.

[33] I. Ahmad, T. Kumar, M. Liyanage, J. Okwuibe, M. Ylianttila, and A. Gurtov, "5G security: analysis of threats and solutions," in *2017 IEEE Conference on Standards for Communications and Networking, CSCN 2017*, pp. 193–199, 2017, doi: 10.1109/CSCN.2017.8088621.

[34] N. Panwar, S. Sharma, and A. K. Singh, "A survey on 5G: the next generation of mobile communication," *Phys. Commun*., vol. 18, pp. 64–84, 2016, doi: 10.1016/j.phycom.2015.10.006.

[35] S. A. Khwandah, J. P. Cosmas, P. I. Lazaridis, Z. D. Zaharis, and I. P. Chochliouros, "Massive MIMO systems for 5G communications," *Wirel. Pers. Commun.*, vol. 120, no. 3, pp. 2101–2115, 2021, doi: 10.1007/s11277-021-08550-9.

[36] S. I. Al-Qasrawi, "Proposed technologies for solving future 5G heterogeneous networks challenges," *Netw. Comput. Syst*., vol. 7, no. 1, pp. 11–19, 2017.

[37] A. Sharma, V. Balasubramanian, and A. Jolfaei, "Security challenges and solutions for 5G HetNet," in *2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, 2020, doi:10.1109/TrustCom50675.2020.00177.

[38] M. M. Alsulami and N. Akkari, "The role of 5G wireless networks in the internet-of- things (IoT)," in *2018 1st International Conference on Computer Applications & Information Security (ICCAIS)*, 2018, pp. 1–8, doi: 10.1109/cais.2018.8471687.

[39] A. Ciuffoletti, "Low-cost IoT: a holistic approach," *J. Sens. Actuator Netw.*, vol. 7, no. 2, 2018, doi: 10.3390/jsan7020019.

[40] Vidhyotma and J. Singh, *Comparative Analysis of Existing Latest Microcontroller Development Boards*, vol. 545. Springer, Singapore, 2019, doi:10.1007/978-981-13-5802-9_88.

[41] A. S. Ismailov and Z. B. Jo'rayev, "Study of arduino microcontroller board," *Sci. J*., vol. 3, no. 3, pp. 172–179, 2022.

[42] M. Agiwal, N. Saxena, and A. Roy, "Towards connected living: 5G enabled Internet of Things (IoT)," *IETE Tech. Rev. (Institution Electron. Telecommun. Eng. India)*, vol. 36, no. 2, pp. 190–202, 2019, doi: 10.1080/02564602.2018.1444516.

[43] M. Wazid, A. K. Das, S. Shetty, P. Gope, and J. J. P. C. Rodrigues, "Security in 5G-enabled Internet of Things communication: issues, challenges and future research roadmap," *IEEE Access*, vol. 9, pp. 4466–4489, 2021, doi: 10.1109/ACCESS.2020.3047895.

[44] H. Ji, S. Park, J. Yeo, Y. Kim, J. Lee, and B. Shim, "Ultra-reliable and low-latency communications in 5G downlink: physical layer aspects," *IEEE Wirel. Commun.*, vol. 25, no. 3, pp. 124–130, 2018, doi: 10.1109/MWC.2018.1700294.

[45] D. Feng, L. Lai, J. Luo, Y. Zhong, C. Zheng, and K. Ying, "Ultra-reliable and low-latency communications: applications, opportunities and

challenges," *Sci. China Inf. Sci.*, vol. 64, no. 2, p. 120301, 2021, doi: 10.1007/s11432-020-2852-1.

[46] M. E. Morocho-Cayamcela, H. Lee, and W. Lim, "Machine learning for 5G/B5G mobile and wireless communications: potential, limitations, and future directions," *IEEE Access*, vol. 7, pp. 137184–137206, 2019, doi: 10.1109/ACCESS.2019.2942390.

[47] A. Slalmi, H. Chaibi, A. Chehri, R. Saadane, G. Jeon, and N. Hakem, "On the ultra-reliable and low-latency communications for tactile internet in 5G era," *Procedia Comput. Sci.*, vol. 176, pp. 3853–3862, 2020, doi: https://doi.org/10.1016/j.procs.2020.09.003.

[48] H. Kim, *Design and Optimization for 5G Wireless Communications*, John Wiley & Sons, New York, NY, 2020, doi: 10.1002/9781119494492.

[49] P. Popovski, K. F. Trillingsgaard, O. Simeone, and G. Durisi, "5G wireless network slicing for eMBB, URLLC, and mMTC: a communication-theoretic view," *IEEE Access*, vol. 6, pp. 55765–55779, 2018, doi: 10.1109/ACCESS.2018.2872781.

[50] D. Abdullah and S. Ameen, "Enhanced mobile broadband (EMBB): a review," *J. Inf. Technol. Informatics*, vol. 1, no. 1, pp. 13–19, 2021, [Online]. Available: https://qabasjournals.com/index.php/jiti/article/download/24/36

[51] Q. Qiu, S. Liu, S. Xu, and S. Yu, "Study on security and privacy in 5G-enabled applications," *Wirel. Commun. Mob. Comput.*, vol. 2020, p. 8856683, 2020, doi: 10.1155/2020/8856683.

[52] C. Bockelmann, N. K. Pratas, G. Wunder, *et al*, "Towards massive connectivity support for scalable mMTC communications in 5G networks," *IEEE Access*, vol. 6, pp. 28969–28992, 2018, doi: 10.1109/ACCESS.2018.2837382.

[53] N. Haider, M. Z. Baig, and M. Imran, "Artificial intelligence and machine learning in 5G network security: opportunities, advantages, and future research trends," *CoRR*, vol. abs/2007.0, 2020. Available: http://arxiv.org/abs/2007.04490

[54] B. Upadhyaya, S. Sun, and B. Sikdar, "Machine learning-based jamming detection in wireless IoT networks," in *Proceedings – 2019 IEEE VTS Asia Pacific Wireless Communications Symposium, APWCS 2019*, 2019, pp. 1–5, doi: 10.1109/VTS-APWCS.2019.8851633.

[55] R. Doshi, N. Apthorpe, and N. Feamster, "Machine learning DDoS detection for consumer internet of things devices," in *Proceedings – 2018 IEEE Symposium on Security and Privacy Workshops, SPW 2018*, 2018, pp. 29–35, doi: 10.1109/SPW.2018.00013.

[56] T. Hong, C. Liu, and M. Kadoch, "Machine learning based antenna design for physical layer security in ambient backscatter communications," *Wirel. Commun. Mob. Comput.*, vol. 2019, p. 4870656, 2019, doi: 10.1155/2019/4870656.

[57] R. Khilar, K. Mariyappan, M. S. Christo, *et al*, "Artificial intelligence-based security protocols to resist attacks in internet of things," *Wirel. Commun. Mob. Comput.*, vol. 2022, pp. 1–10, 2022, doi: 10.1155/2022/1440538.

[58] T. Saba, K. Haseeb, A. A. Shah, A. Rehman, U. Tariq, and Z. Mehmood, "A machine-learning-based approach for autonomous IoT security," *IT Prof.*, vol. 23, no. 3, pp. 69–75, 2021, doi: 10.1109/MITP.2020.3031358.

[59] S. M. Tahsien, H. Karimipour, and P. Spachos, "Machine learning based solutions for security of Internet of Things (IoT): a survey," *J. Netw. Comput. Appl.*, vol. 161, pp. 102630, 2020, doi: 10.1016/j.jnca.2020.102630.

[60] S. Zaman, K. Alhazmi, M. A. Aseeri, *et al.*, "Security threats and artificial intelligence based countermeasures for internet of things networks: a comprehensive survey," *IEEE Access*, vol. 9, pp. 94668–94690, 2021, doi: 10.1109/ACCESS.2021.3089681.

[61] R. A. Alshinina and K. M. Elleithy, "A highly accurate deep learning based approach for developing wireless sensor network middleware," *IEEE Access*, vol. 6, pp. 29885–29898, 2018, doi: 10.1109/ACCESS.2018.2844255.

[62] S. M. Wa Umba, A. M. Abu-Mahfouz, T. D. Ramotsoela, and G. P. Hancke, "A review of artificial intelligence based intrusion detection for software-defined wireless sensor networks," in *IEEE International Symposium on Industrial Electronics*, June 2019, vol. 2019, pp. 1277–1282, doi: 10.1109/ISIE.2019.8781458.

[63] M. Mamdouh, M. A. I. Elrukhsi, and A. Khattab, "Securing the internet of things and wireless sensor networks via machine learning: a survey," in *2018 International Conference on Computer and Applications, ICCA 2018*, 2018, pp. 215–218, doi: 10.1109/COMAPP.2018.8460440.

[64] H. Fang, X. Wang, and S. Tomasin, "Machine learning for intelligent authentication in 5G and beyond wireless networks," *IEEE Wirel. Commun.*, vol. 26, no. 5, pp. 55–61, 2019, doi: 10.1109/MWC.001.1900054.

[65] M. Wang, T. Zhu, T. Zhang, J. Zhang, S. Yu, and W. Zhou, "Security and privacy in 6G networks: new areas and new challenges," *Digit. Commun. Netw.*, vol. 6, no. 3, pp. 281–291, 2020, doi: 10.1016/j.dcan.2020.07.003.

[66] Y. Siriwardhana, P. Porambage, M. Liyanage, and M. Ylianttila, "AI and 6G security: opportunities and challenges," in *2021 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit)*, 2021, doi:10.1109/EuCNC/6GSummit51104.2021.9482503.

[67] W. Guo, W. Guo, M. Abbaszadeh, L. Lin, *et al.*, "Molecular physical layer for 6G in wave-denied environments," *IEEE Commun. Mag.*, vol. 59, no. 5, pp. 33–39, 2021, doi: 10.1109/MCOM.001.2000958.

[68] W. Haselmayr, A. Springer, G. Fischer, *et al.*, "Integration of molecular communications into future generation wireless networks," in *1st 6G Wireless Summit. IEEE, Levi, Finland*, pp. 1–2, 2019, [Online]. Available: https://www.gov.uk/government/news/robots-to-fix-

[69] P. Porambage, G. Gur, D. P. Moya Osorio, M. Livanage, and M. Ylianttila, "6G security challenges and potential solutions," in *2021 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit)*, 2021, doi:10.1109/EuCNC/6GSummit51104.2021.9482609.

[70] G. Bindu, I. T. Joseph S, V. R. Kanakala, G. L. K. Niharika, and B. E. Raj, "Impact of blockchain technology in 6G network: a comprehensive survey,"

in *2022 International Conference on Inventive Computation Technologies (ICICT)*, 2022, doi:10.1109/ICICT54344.2022.9850463.

[71] M. R. Islam, M. M. Rahman, M. Mahmud, M. A. Rahman, M. H. S. Mohamad, and A. H. Embong, "A review on blockchain security issues and challenges," in *2021 IEEE 12th Control and System Graduate Research Colloquium (ICSGRC)*, 2021, doi:10.1109/ICSGRC53186.2021.9515276.

[72] S. Ariyanti and M. Suryanegara, "Visible light communication (VLC) for 6G technology: the potency and research challenges," in *Proceedings of the World Conference on Smart Trends in Systems, Security and Sustainability, WS4 2020*, 2020, pp. 490–493, doi: 10.1109/WorldS450073.2020.9210383.