Chapter 3
5G Network Implementation: A Survey on Security Issues, Challenges, and Future Directions

Sharma Ji
https://orcid.org/0009-0005-4283-5756
Ajay Kumar Garg Engineering College, India

Abhishek Kumar Mishra
School of Computer Science and Applications IFTM University, India

ABSTRACT

Fifth generation (5G) wireless network is a wireless communication standard technology, with substantially faster speeds, extremely low latency, and all-pervasive connectivity. The 5G wireless technology includes strong encryption and authentication systems, the possibility of supply chain threats, and network vulnerability. In this chapter, a brief review of complex environment for 5G networks and the security flaws in the novel technology ideas that 5G will incorporate is presented. Various security issues in Future Generations (XG), post-5G, cellular technology, and potential solutions to the security challenges are also discussed.

1. INTRODUCTION

Every generation of wireless transmission (WT) moves the technology closer to its goal of providing high-quality, dependable data communication, much like cable data communication. 5G represents a significant advancement in this regard, offering dense base station (BS) deployment with improved quality, incredibly low latency, and higher capacity, together with high coverage and very high 5G public-private

DOI: 10.4018/979-8-3693-5643-2.ch003

collaboration estimates that around 7 trillion objects or devices would be connected and that with advanced privacy, the average service delivery time will drop from 90 hours to 90 minutes (A. Almusaylim & Jhanjhi, 2019). .

A technological growth in the field of network is presented in Table 1.

Using a variety of technologies, 5G seeks to create a smart, digital society with high-quality service availability, as illustrated in Figure 1 (Ahmad et al., 2017).

5G technologies will benefit nearly all businesses and industries. One of the main industries that will be transformed by taking advantage of 5G's advantages is healthcare. This includes data analytics, wearable technology-enabled real-time patient monitoring, and expansion of telehealth via smart devices in underserved areas (Aqeel et al., 2022).

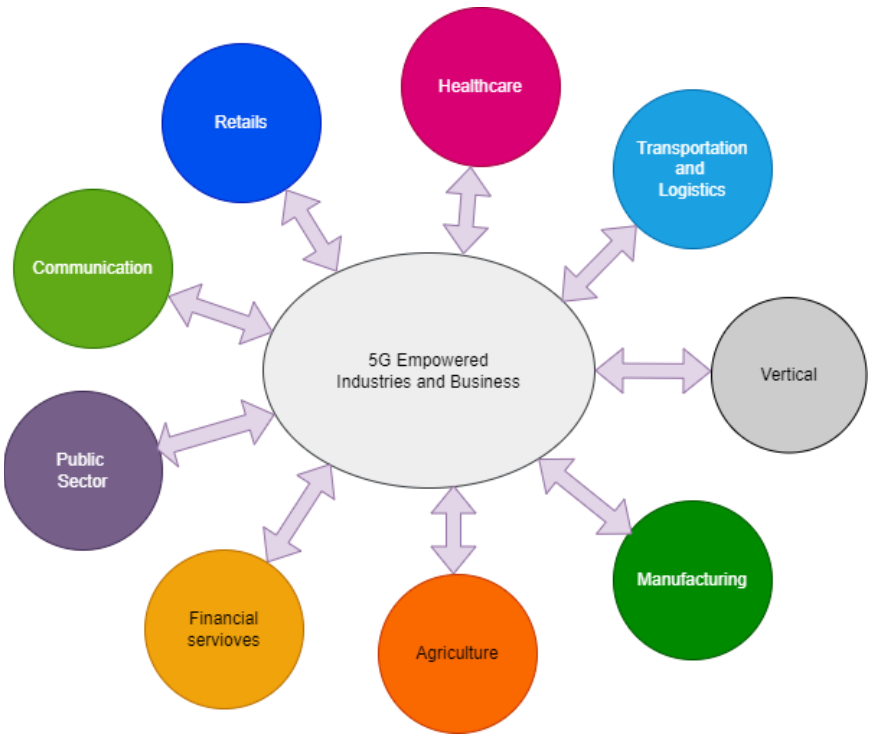
Figure 2 illustrates some important sectors that will gain from 5G are transportation logistics, vertical, manufacturing, agriculture, financial services, public sector, communication, and retail (Norp, 2018).

Table 1. Recent technological growth in network sector

Technology	1G	2G	3G	4G	5G
Installation	1979-1991	1991-2001	2001-2009	2009-2020	2020 to Till Now
Bandwidth of Data	2Kbps	64Kbps	2Mbps	1Gbps	More than1Gbps
Technologies	AMPS, NMT, TACS	GSM/GPRS, D-AMPS, CDMA One	WCDMA/HSPA+, CDMA200 DO, TD-SCDMA	LTE, Advanced LTE	Not standardized till now
Key differentiator	Mobility	Secure, Mass Adoption	Better internet experience, applications	Faster broadband internet, lower latency	Faster internet, IoT, wide Range of applications
Services	Voice	SMS, Higher capacity Packetized data, Digital Voice	Cohesive high-class audio, Video and data	Wearable devices, Dynamic information access	Dynamic information access, wearable devices with AI capabilities
Core network	PSTN	PSTN	Packet Network	Internet	Internet
Weakness	Poor spectral efficiency, Major security concerns	Challenging to support request for email, Narrow data rates	Failure of WAP for internet access, Tied to legacy, Real performance failed to match hype	Mobile explicit Architecture and protocols	Infrastructure, security, privacy etc.

Figure 1. Diverse devices interconnectivity using 5G
[Source: https://www.etsi.org/technologies/5g?tmpl=component]

Figure 2. 5G Empowered industries/business



Vehicle-to-vehicle connections, real-time data collection, analysis, and communication, quicker shipping and transit times, and more ecologically friendly and fuel-efficient vehicles are just a few of the ways that 5G will revolutionize logistics and transportation. Manufacturing is anticipated to be the sector most benefiting from 5G. Manufacturers will be able to interact with remote workers, increase production standards, and perform real-time machine analysis with reduced latency and increased bandwidth (Omar et al., 2017).

The agriculture sector will benefit from 5G's smart farming, yield-boosting technologies, and resistance to climate change. 5G is expected to have a significant positive impact on the financial services sector by enhancing back-end operations, expediting service delivery, enabling mobile payment apps, and gaining deeper customer insight (Ganesh Babu et al., 2020).

The public sector is predicted to undergo transformation thanks to 5G, which will make everything smart, enable 24/7 communication with residents, and equip government employees with the newest technology (Humayun et al., 2021).

5G's lower latency and faster transmission rates are predicted to significantly improve communications (Duan et al., 2020). The 5G network's rapid speed will facilitate communication. Low latency, on the other hand, will speed up response times. Last but not least, 5G will have a favourable effect on retail. By sending a lot of data to customers, it will allow shops to enhance their offerings (Apruzzese et al., 2023).

The conversation above demonstrates that 5G is an urgent necessity and will have a good effect on nearly every area of life by linking all facets of it; yet, in order to ensure its security, it requires strong architecture and solutions. To fully realize the potential benefits of 5G networks, academics and practitioners must solve the security and privacy concerns (Fong et al., 2019). Next-generation mobile networks (NGMN) state that flash network traffic, user plane integrity, radio interface security, roaming security, signalling storms, and denial-of-service (DoS) attacks on end-user devices and the infrastructure are some of the major issues that 5G networks will have to deal with, as illustrated in Figure 3.

Furthermore, a brief summary of the evolution of security in 1G networks to 5G networks is presented in Table 2 (Mangla et al., 2023).

Prior to offering any solutions for 5G network security and privacy, it is necessary to compile the most important security problems, obstacles, and opportunities in order to give 5G researchers and practitioners a thorough understanding. This chapter provides a thorough survey of 5G in order to do this (Hasnat et al., 2019).

Figure 3. 5G common security issues

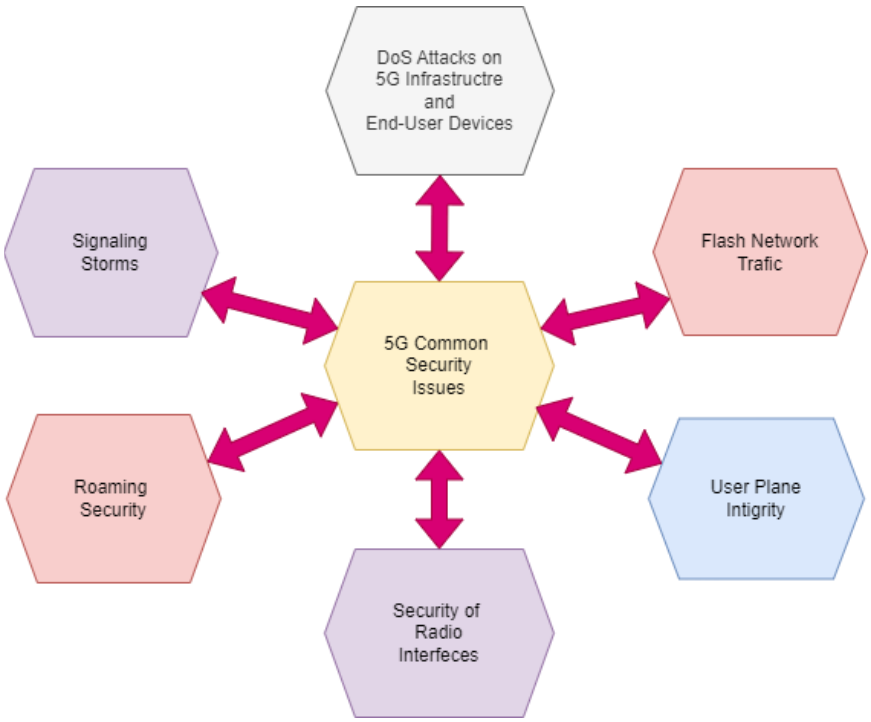


Table 2. Summary of evolution of security from 1G to 5G network technology

Network	Security System	Security Issues
1G	Absence of clear security or privacy ensures	Call interception, eavesdropping, and a lack of privacy protection.
2G	Protection based on encryption and anonymity during authentication	Fake base station, radio link security, one-way authentication, and spamming
3G	Adopted the 2G security, secure access to the network, introduced Authentication and Key Agreement (AKA) and two-way authentication	IP traffic security vulnerabilities, encryption keys security, roaming security.
4G	New integrity protection, non-3G Partnership Project (3GPP) access security, encryption key security, and trust method have been developed	DoS attacks, data integrity, Base Transceiver Station (BTS)security, and Listening in on long-term keys are security issues brought on by an increase in IP traffic. Not suitable for the security of new services and equipment, such as the massive IoT that 5G is expected to enable.
5G	Encompass enhanced authentication, robust encryption, network slicing isolation, and IoT-specific safeguards to ensure confidentiality, integrity, and availability of data in the evolving wireless landscape.	Safe guarding network slicing, managing IoT security at scale, addressing Increased attack surfaces due to denser deployments, ensuring robust authentication and encryption, and protecting against emerging threats in a rapidly evolving technology landscape.

2. 5G NETWORKS AND SECURITY ISSUES

This section of the article will go over the potential presented by 5G networks, common security threats that target 5G and their mitigation strategies, security services provided by 5G network operators, and related difficulties (Hussain et al., 2020).

2.1 The Complex Environment for 5G Networks and the Security Flaws

In addition to providing fast data speeds, minimal latency, and a wide range of applications, 5G networks may have security issues that need to be resolved. Small cells and edge devices are just a few of the many network components that make up 5G networks' distributed architecture, which opens up new attack vectors and increases attack surfaces. The network slicing feature of 5G allows for the creation of numerous virtual networks on the same infrastructure, providing customisation and service differentiation (Javaid et al., 2018). If not set appropriately, however, this function may lead to concerns with isolation and security.

SDN and NFV technologies play a major role in 5G networks, which presents new security problems because virtualized network functions are susceptible to attacks if not sufficiently secured. Due to its weak security measures, 5G's support for a large number of IoT devices may result in security flaws that could give hackers access to them. There may be a rise in man-in-the-middle attacks as tiny cells and edge devices become more widely used. In these attacks, hackers intercept and alter data traveling between devices and networks (Khan et al., 2020). Because 5G networks include more connected devices and endpoints, they are more susceptible to denial-of-service (DoS) attacks, which facilitate an attacker's ability to overwhelm the network (Li et al., 2019).

Industry stakeholders must work together to create a strong framework that includes intrusion detection, network segmentation, encryption, access control, and frequent evaluations to sustain 5G network security (Humayun et al., 2020).

2.2. Common Security Attacks on 5G Network and Mitigation Techniques

Although 5G is a quickly expanding phenomenon with many benefits, security is a concern that must be taken into consideration. Even though 5G network providers work hard to give their target users quick and safe data transmission, security breaches are still possible. To assist 5G practitioners, some frequent security threats in this area along with mitigation methods are discussed here (Natarajan et al., 2021).

2.2.1 Eavesdropping and Traffic Analysis

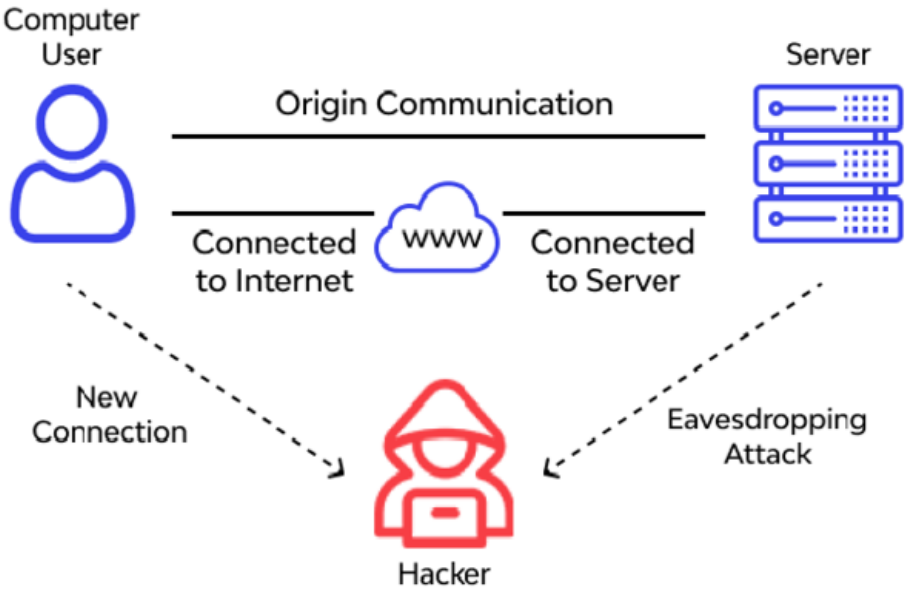
An intrusive party attempts to intercept a message from its intended recipients in this type of passive attack without interfering with regular communication. Since the attack is passive, it is challenging to identify; but, there are steps you can take to lessen the chance of being overheard, including raising awareness and implementing robust encryption, network access control, network segmentation, and physical security. Another passive approach is traffic analysis, in which hackers attempt to intercept location and identity by examining traffic patterns but are unable to access the data due to encryption (Nataraj et al., 2022). PLS analysis has been the focus of research lately to combat eavesdropping (Wang, N., et al., 2019), (Qiao, X., et al., 2019), (Ahmad, I., et al., 2017), (Varga, P., et al., 2020).

Virtual Private Network usage and encryption are examples of mitigation. Monitoring network traffic patterns to obtain insights without having to view the content is known as traffic analysis (Qiao et al., 2019). Traffic padding, information protection, and secure protocols are all part of mitigation. It can happen in a variety of settings, such as network interactions, emails, text messages, and phone conversations. There are several justifications for eavesdropping, including as privacy violations, cybercrime, and espionage. Eavesdropping can be done through a variety of methods, including man-in-the-middle attacks, passive listening, and taking advantage of communication protocol flaws. Since eavesdropping frequently violates people's privacy and might result in the theft of sensitive information, it can be both unlawful and immoral (Hussain et al., 2019).

Instead of concentrating on the actual substance of the data, traffic analysis is a type of network surveillance that examines the patterns, metadata, and features of data transfer. It entails keeping an eye on and evaluating network traffic's quantity, timing, source, destination, and other details. Traffic analysis can offer important insights into communication patterns and behaviour, even though it might not disclose the precise content of messages or data Information such as that is communicating, when they are communicating, and how frequently they communicate can be inferred from traffic analysis (Sharma et al., 2020). This information can be used for various purposes, including network optimization, intrusion detection, and even to derive sensitive information, such as user habits or organizational structures (Javaid et al., 2023).

If utilized maliciously, both traffic analysis and eavesdropping can present serious security risks. Organizations and individuals can use a variety of security measures, including intrusion detection systems, virtual private networks (VPNs), and encryption, to reduce these dangers. Maintaining up-to-date knowledge of the most recent cyber security dangers and best practices is also crucial for defending against traffic analysis and eavesdropping assaults (Varga et al., 2020).

Figure 4. Eavesdropping attack

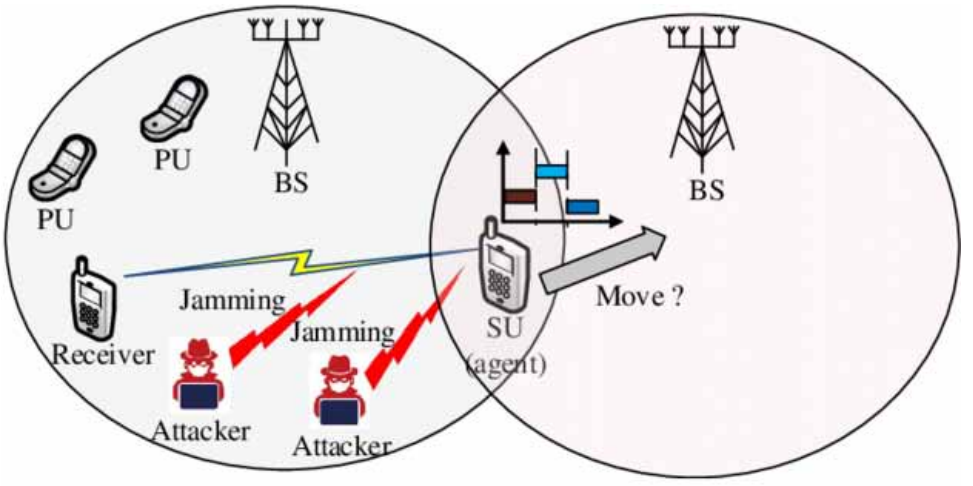


The operation of the eavesdropping assault is depicted in Figure 4. Figure 4 shows how an eavesdropper uses traffic sensing to try and intercept a message intended for someone else.

2.2.2. Jamming

In contrast to eavesdropping and traffic analysis, jamming stops all valid user communication. Through deliberate interference with malicious malware, it stops authorized users from using radio resources. Anti-jamming methods, such as the spread spectrum technique (SST) and the random key distribution approach can stop the jamming attack (Verma & Lalwani, 2019). Figure 5 illustrates how the jamming assault operates. Jamming has a variety of uses, both authorized and unauthorized. Military and law enforcement operations, such as interfering with adversaries' communication networks, are examples of legal applications. Jamming, however, is frequently connected to illicit actions, such as interfering with GPS signals, wireless networks, or mobile phone connections. In these situations, it may be utilized for illegal activity, malevolent intent, or invasion of privacy (Wang et al., 2019).

Figure 5. Jamming attack



Jamming is legal or illegal depending on the intended purpose and the jurisdiction. Jamming is prohibited in many nations, particularly when used for private or business purposes since it might interfere with essential services like emergency communications. In certain situations, authorized organizations like the military and law police may employ jamming. Several countermeasures can be used to prevent jamming frequency (Duan, W., et al, 2020).These consist of signal diversity, encryption, physical security measures, and frequency hopping techniques. In certain situations, jamming sources can be found and identified with the aid of directional antennas and signal analysis software. Jamming can have detrimental effects, especially if it disrupts emergency services or vital infrastructure. For example, disruption of GPS signals can affect aviation, logistics, and navigation. Disrupting mobile phone signals might cause communication problems in emergencies (Zhang et al, 2019). Laws and restrictions are in place in several nations to restrict the use and sale of jamming devices. In many places, it may be illegal or restricted to import, own, or use jammers.

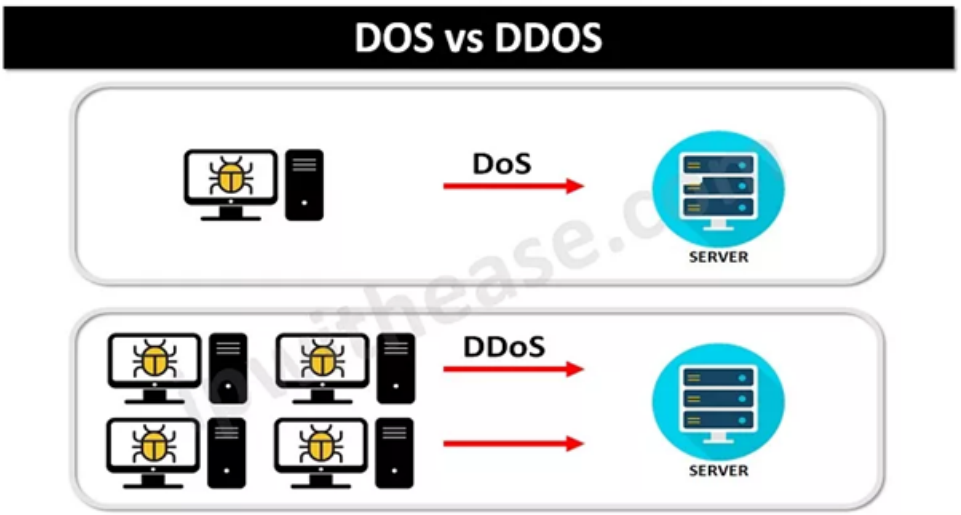
It's essential to use jamming technology responsibly and within the bounds of the law. Unauthorized jamming is not only illegal but also has the potential to cause harm, disrupt critical services, and infringe upon the rights of others.

2.2.3 DoS and DDoS

Due to the vast number of interconnected devices, DoS and DDoS assaults are the main security concerns for 5G operators. The goal of this attack is to deplete all

of the network's resources in order to prevent access by authorized users. While in a DDoS assault, several systems target a single system with a DoS attack, in a DoS attack, attackers overwhelm the server with TCP and UDP packets. Figure 6 illustrates DoS and DDoS attacks. Increased bandwidth, anti-DDoS hardware, DNS server security, redundant infrastructure, and appropriate network monitoring can all help stop DoS and DDoS attacks (Wang et al., 2019). A denial-of-service (DoS) attack occurs when an attacker sends more network packets or requests than the target system is capable of handling. The system may become sluggish, unresponsive, or completely unavailable as a result of this heavy usage.

Figure 6. DoS and DDoS attack



DoS attacks frequently seek to deplete vital resources, including memory, CPU power, network bandwidth, and connection capacity. It's possible that authorized users won't be able to access the system if these resources run out. Certain DoS attacks use software or network infrastructure flaws in the target machine. These flaws could be used by attackers to bring down the system or make it unusable. DoS assaults can be carried out by attackers for a number of reasons, such as monetary gain, retaliation, political objectives, or just the sheer joy of wreaking havoc. Organizations employ a variety of security tools, including firewalls, intrusion detection systems, load balancers, and content delivery networks (CDNs), to ward off DoS attacks. By identifying and removing malicious traffic, these solutions can assist keep legitimate users from accessing the system (Verma & Lalwani, 2019).

Most jurisdictions prohibit denial-of-service attacks. Penalties and criminal charges may follow participation in or assistance with a denial of service attack. DoS assaults can impair an organization's reputation, interrupt corporate operations, and result in financial losses, thus it's critical that they are guarded against with a proactive security plan. Having an incident response strategy in case of an attack, implementing strong security solutions, and keeping an eye on network traffic are all examples of mitigation techniques.

A Distributed Denial of Service (DDoS) attack is a malicious attempt to disrupt the regular functioning of a network, service, or website by overwhelming it with a flood of internet traffic originating from multiple sources. Unlike a simple Denial of Service (DoS) attack, where a single system is used to flood the target, a DDoS attack involves multiple compromised systems, often forming a botnet, to launch the attack. The distributed nature of the attack makes it more powerful and challenging to mitigate (Aqeel et al., 2022).

Key characteristics of DDoS attacks

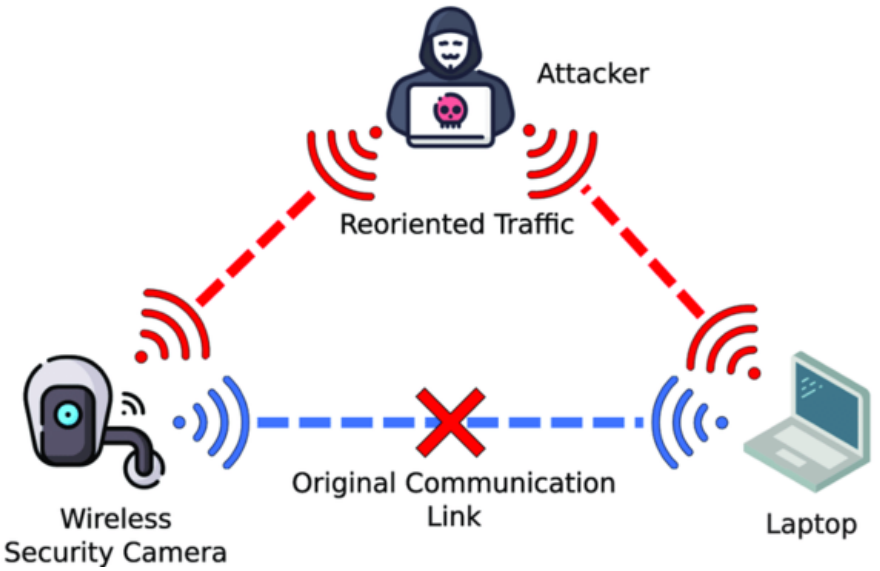
DDoS assaults use several sources, frequently thousands or more, dispersed around the internet. These sources are typically compromised, attacker-controlled equipment like PCs, servers, or Internet of Things gadgets. A DDoS assault aims to overwhelm the target with an enormous amount of traffic, frequently more than it can manage. Overuse of the service by genuine users may result in server resource exhaustion, network bandwidth saturation, and service inaccessibility. To conduct a denial-of-service assault, attackers usually take control of a botnet, which is a network of compromised devices. These devices can be remotely controlled by the attacker and are frequently infected with malware. DDoS assaults can be driven by a number of things, such as activism, financial extortion, competitive sabotage, or just a desire to cause havoc and disruption. Organizations frequently employ specialized DDoS mitigation services and appliances as a line of defence against DDoS attacks. With the help of these technologies, harmful traffic should be recognized and filtered out to make room for legal traffic. Most jurisdictions forbid DDoS attacks, and individuals who initiate or take part in them may be prosecuted and punished criminally.

DDoS assaults pose a serious risk to internet businesses and services since they can cause disruptions, monetary losses, and reputational harm. Strong security measures, such as load balancing, rate limitation, and traffic analysis, are essential for defending against DDoS assaults. Internet service providers (ISPs) and DDoS mitigation providers must work together to help absorb and lessen attack traffic.

2.2.4 Man-in-the-Middle Attack (MITM)

A 5G vulnerability known as MITM is a 4G vulnerability that allows an attacker to take over a legitimate user's communication channel and intercept messages as they see fit. This type of active attack jeopardizes the confidentiality, availability, and integrity of data. Mutual authentication, data encryption, the use of IDS solutions, Security Services in 5G networks, employee awareness through training, and base station can all be used to thwart this. A detailed description of the MITM architecture is presented in Figure 7.

Figure 7. MITM attack in 5G network



3. 5G NETWORK SECURITY SERVICES

Safeguarding data confidentiality, integrity, and availability, as well as resolving security problems and threats in the 5G environment, are essential security services in a 5G network. To protect user data confidentiality and make sure that it cannot be read by unauthorized parties even if intercepted, data encryption is an essential component of 5G technology. Verifying network user, device, and service identities and preventing illegal access require secure user and device authentication protocols. Only those who are permitted can use the services and resources on the network thanks to access control systems that manage access to these resources. Data

integrity depends on encryption keys, and key management services make sure they are created, shared, and updated appropriately. Security measures must be put in place to safeguard and isolate various slices of the 5G network from interference and unwanted access.

Together, the security services provide a strong foundation for 5G networks, protecting them against a range of risks such as service interruption, illegal access, and data breaches.

3.1 Authentication

Entity and message authentication make up 4G cellular networks' authentication. In 5G networks, symmetric-key-based authentication is impractical because of differing trust models, novel service delivery models, and privacy issues. It is necessary to have flexible and hybrid mutual authentication, which can be done in three different ways: network-only, service provider-only, and network and service provider-only. In order to handle mutual authentication and rapid handover, 5G networks define three authentication methods: 5G-AKA, EAP-TLS, and EAP-AKA. By enabling network and mobile device authentication, EAP-AKA makes sure that both sides can rely on one another. To create this trust, a mutual authentication procedure is used. EAP-AKA aids in safeguarding user identity data. It accomplishes this by maintaining the confidentiality of the user's long-term identity—such as their International Mobile Subscriber Identity, or IMSI—during the authentication procedure. For security and privacy purposes, this is crucial.

In addition, EAP-AKA makes it easier to generate session keys, which are necessary for safe connection between the network and mobile device. To preserve the confidentiality and integrity of the transmission, these keys are utilized for data encryption and decryption. Through the use of a challenge-response mechanism, the network asks the mobile device to submit particular data that should only be known by authorized devices. The mobile device proves its legitimacy by responding with the required data. EAP-AKA is widely used in 4G (LTE) and 3G (UMTS) mobile networks, where it is essential for maintaining communication security and guarding against different types of network threats. Although EAP-AKA was widely used in previous generations of mobile networks, 5G networks have included additional security and authentication features. Although newer authentication techniques, such EAP-AKA', have been proposed to improve security in the rapidly changing 5G landscape, EAP-AKA is still employed in 5G.

EAP-AKA is a crucial part of mobile network security since it offers a solid framework for user-to-network communication security and mobile device authentication. It supports network integrity and user privacy protection.

3.2 Confidentiality

Privacy and data confidentiality are aspects of confidentiality. Managing proper user information, such as data, identity, and location privacy, is part of privacy. Data confidentiality restricts access to intended users and shields data from passive attacks. 5G uses robust data encryption to protect data confidentiality. In response to privacy concerns, location privacy can be protected by k-anonymity, location encryption, and fake location; identity privacy can be protected by anonymous authentication; data privacy requires robust authentication (Apruzzese et al., 2023). Data sensitivity classification is a common practice in maintaining confidentiality. There are various levels of classification for information, including highly classified, internal, public, and confidential, each with its own set of security controls and safeguards.

Only authorized people or organizations should be able to access secret information. Mechanisms for encryption, authorization, and authentication are used to accomplish this. Access should only be granted to those who have a valid need to know. An essential instrument for preserving secrecy is data encryption. It entails converting data into a format that is unintelligible and requires the right decryption key to decode. This is particularly crucial for safeguarding data when it's being transmitted or kept on devices. Data privacy and confidentiality are closely related. To protect people's personal information, organizations are frequently obliged to abide with privacy laws and regulations, such as the General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA).NDAs are frequently used in the legal and business worlds to guarantee that parties to a partnership or transaction agree not to reveal secret information to outside parties. Employers frequently offer training and awareness initiatives to enlighten staff members about the value of confidentiality and appropriate ways to handle sensitive data. Secure physical security measures, like secured filing cabinets, rooms with restricted access, and surveillance, are crucial for safeguarding private documents and data kept in tangible forms.

Firewalls, intrusion detection systems, and antivirus software are examples of cyber security techniques that assist stop illegal access to computer networks and systems. Incident response strategies are necessary for organizations to handle security incidents and data breaches that may jeopardize confidentiality. A prompt reaction can lessen the effects of a breach. Confidentiality maintenance is not only required by law and security, but it is also morally right. Ethics rules require professionals in industries such as healthcare, law, and finance to keep their customers' or patients' confidential information private.

A breach of confidentiality may result in identity theft, data breaches, legal ramifications, harm to one's reputation, and monetary damages. As a result, both

individuals and organizations need to take confidentiality seriously and put the right safeguards in place to secure sensitive data.

3.3 Availability

The degree to which a service or piece of information is accessible to its intended users at the appropriate time and place is referred to as availability. This function assesses a system's resilience and is a crucial performance parameter in 5G networks. Through interception, attacks like denial-of-service (DoS) and jamming render the service unavailable to users. The availability feature is enhanced by 5G networks, which offer higher bandwidth and capacity. Large-scale, networked IoT devices still require further defence against these intrusions.

Appropriate resource allocation and pseudorandom time-hopping spread spectrum (PTHSS) can contribute to increased information and service availability (Hasnat et al., 2019). 5G networks are designed to provide high availability, aiming for uptime levels close to 100%. This means that users should have access to the network and its services for the vast majority of the time. To achieve high availability, 5G networks incorporate redundancy in various components and infrastructure. This redundancy includes backup power supplies, multiple data centres, and redundant network paths to prevent single points of failure. Ensuring reliability are essential for availability. 5G networks employ robust technology and redundancy to reduce the risk of network failures, such as hardware or software issues, which could impact the availability of services. 5G networks use failover mechanisms to automatically switch to backup components or paths in case of a failure, minimizing downtime and service interruptions.

In 5G, network slicing allows operators to create separate virtual networks on a shared physical infrastructure. This enables the allocation of specific resources to guarantee the availability of critical services, such as emergency communications or industrial applications. Security plays a crucial role in ensuring the availability of 5G networks. Protection against cyberattacks and threats helps maintain network integrity and uptime. Service providers and operators often define specific availability levels in SLAs to set expectations for network uptime. These agreements outline the consequences of downtime and the compensation for users in case of service disruptions.

Regular maintenance and monitoring of network components, as well as real-time analysis of network performance, are crucial for identifying and addressing potential issues that could affect availability. Resilience is the ability of the network to recover quickly from disruptions. 5G networks are designed to be resilient, with the capability to recover from faults or failures swiftly.

High availability in 5G is vital for various use cases, including critical communications, the Internet of Things (IoT), autonomous vehicles, and industrial applications. Ensuring that these services have consistent and uninterrupted access to the network is a fundamental requirement for the successful deployment of 5G technology.

3.3 Integrity

One of the most important security criteria is integrity, which guards against unauthorized parties actively attacking and changing data. Via insider harmful attacks like code injection and data manipulation, hostile insiders jeopardize the integrity of data. Moreover, insiders' legitimate identities make them challenging to identify. Massive device interconnection is the goal of 5G, and it is anticipated to assist applications like healthcare and transportation that are directly tied to people. Data integrity is a major issue in these situations that requires attention (Apruzzese et al., 2023). Integrity guarantees that during transmission, data doesn't change or become altered. This implies that when a packet or message is sent across a 5G network, it reaches its destination exactly as intended, free from any tampering or illegal modifications.

5G networks employ cryptographic techniques to authenticate data and confirm its origins in order to preserve integrity. This procedure verifies that the data is authentic and hasn't been tampered with while in transit. Data integrity is typically checked using hash functions and message digests, which are algorithms that generate a fixed-size "digest" or "hash" of the data and attach it to the message. The recipient can compute the hash once the data is received and compare it to the transmitted hash; if the two matches, the data integrity are confirmed. Integrity mechanisms guard against replay attacks, insertion of malicious data, and unauthorized modifications to a message's content, among other forms of tampering. These safeguards are essential for making sure that sensitive data, like software upgrades or financial transactions, is protected. Secure communication channels with integrity checks and encryption are established in 5G. This guarantees that data is integral (protected from modification) and confidential (protected from eavesdropping).

In order to preserve the integrity of user data and signals, 5G networks employ security standards and protocols such the employment of integrity algorithms within the AKA (Authentication and Key Agreement) procedure. The integrity of user data and signals is preserved by 5G networks through the use of security standards and protocols, such as integrity algorithms in the AKA procedure.5G networks use security measures against potential threats and vulnerabilities that could jeopardize the integrity of the system as a whole to guarantee the integrity of the network itself. Integrity is an essential part of 5G security since it guarantees that the data

and communications in the network are reliable and unchangeable. It also helps to protect private data and keeps the network's dependability intact.

3.4 New Trust Models

5G will replace current Wi-Fi connections and is predicted to deliver speeds ten times faster than 4G. However, there is a significant obstacle that needs to be overcome to foster trust between network organizations and stakeholders. The capacity to trust is crucial for adaptation; 5G operators must ensure that no computer device has been corrupted. To accomplish this, 5G service providers must create new trust models, which call for an innovative architectural strategy. The validity of the operating system, hardware, network management, and access control must be guaranteed by new trust models (Zhang, et al., 2019) (Ahmad et al., 2017). End-to-end encryption, which protects data as it moves from the user's device to the intended destination, is emphasized by 5G networks. This aids in preventing unwanted access and eavesdropping. With 5G, network slicing makes it possible to establish several virtual networks on a single physical infrastructure. Trust and security can be improved by isolating distinct environments for various use cases by allocating resources and security policies to each network slice.

A Zero Trust security model, in which trust is never presumed based on network location, can be implemented by 5G networks. Rather, access is provided based on need-to-know, with on-going authentication and authorization of each user and device. For 5G trust models to work, robust authorization and authentication procedures are essential. To guarantee that only authorized entities can access the network and its resources, multi-factor authentication and identity and access management (IAM) solutions are employed. For 5G trust models to work, robust authorization and authentication procedures are essential. To guarantee that only authorized entities can access the network and its resources, multi-factor authentication and identity and access management (IAM) solutions are employed. Trust is established through secure boot processes, where devices validate the integrity of their firmware and software components. This ensures that only trusted software runs on devices (Aqeel et al., 2022).

5G network elements, such as base stations and core network components, implement security measures to protect against attacks and vulnerabilities. Security mechanisms like intrusion detection and prevention systems are used. Trust models in 5G consider the unique requirements of the Internet of Things (IoT) devices (Omar et al., 2017). Strong security for IoT devices, including secure on boarding and device attestation helps build trust in the IoT ecosystem. Techniques like differential privacy and data anonymization are employed to protect user privacy in 5G networks while still allowing for data collection and analysis. Various organizations and standard

bodies are actively working on defining security and trust standards for 5G, such as the 3rd Generation Partnership Project (3GPP) and the Internet Engineering Task Force (IETF).

These trust models and security mechanisms in 5G are crucial for building a secure and trusted network environment. They help address the increasing complexity of modern communication systems, protect against new threats, and foster trust between users, devices, and network operators in the 5G ecosystem.

3.5 More Privacy Concerns

The issue of privacy is brought about by the 5G network's high data transfer volume. Sensitive personal information that needs to be protected from cyber breaches will be transferred via large-scale networked devices, such as wearable IoT sensors. It is necessary to protect each of the three aspects of privacy: location, identity, and data. In order to do this, 5G service providers must establish new guidelines for data granularity, robust encryption, awareness, and appropriate identity management (Sharma et al., 2020), (Zhang et al, 2019), (Wang et al., 2019).

4. SECURITY ATTACK MODELS

Attackers are developing new techniques to compromise security as a result of technological advancements. End-to-end security is unavoidable in these situations. Monitoring and controlling network devices requires the development of automated and complex security mechanisms. Radio interface security, user plane integrity, flash network traffic, roaming security, DoS attack, signal storms, etc. are a few of the major security issues that 5G network providers should be prepared to handle (Ahmad et al., 2017). Higher frequency bands, such as the terahertz spectrum and millimetre waves, are used by 5G networks. Attackers may find it simpler to intercept signals at higher frequencies over shorter distances, which could jeopardize the anonymity of data transmission.

The attack surface is expanded by the widespread deployment of Internet of Things (IoT) devices in 5G networks. IoT device vulnerabilities, such unpatched firmware or inadequate security configurations, can be used to compromise the network as a whole. A feature of 5G called "network slicing" makes several virtual networks on a shared infrastructure. Vulnerabilities in the network slicing system could allow an attacker to access different slices without authorization; potentially impacting different services. Attacks against 5G core networks have the potential to be quite significant. Service delivery can be affected, for example, by attacks on the Software-Defined Networking (SDN) and Network Function Virtualization (NFV)

components. Attackers may set up rogue base stations or small cells to impersonate legitimate network access points. This can lead to device connections being redirected to the rogue infrastructure, enabling various attacks (Varga et al., 2020).

Adopting strong security measures, patching and updating network components on a regular basis, and enforcing configuration management best practices are essential to fending off these new dangers. Furthermore, in order to mitigate these new security attack models in 5G, stakeholder collaboration, sharing of threat intelligence and adherence to security standards are crucial.

5. SERVICE DELIVERY MODEL AND NETWORK OPPORTUNITIES

5G is an improvement over previous network generations, offering high speed, low latency, greater bandwidth, and flexible new layers. In these situations, it is anticipated that new service delivery models will appear that will take advantage of edge computing, cloud computing, and SDN to provide the best possible network services (Sharma et al., 2020), (Qiao et al., 2019). In comparison to earlier generations, the 5G service delivery paradigm known as eMBB offers far higher data speeds and more network capacity. Applications such as virtual reality (VR), augmented reality (AR), and streaming ultra-high quality video are made possible by it. Low latency and high dependability are requirements for services that URLLC is built to meet. Applications such as remote robotic control, autonomous cars, and critical infrastructure monitoring require it. URLLC guarantees excellent accuracy and low latency in data delivery.

The goal of mMTC is to link a vast number of IoT devices in an effective and dependable manner. Applications like industrial IoT, smart cities, and environmental monitoring are appropriate for it. Many low-power devices can be connected simultaneously thanks to mMTC. The deployment of edge computing resources nearer to the end-user or device is made possible by 5G. This makes it appropriate for applications like real-time video analytics, Internet of Things data processing, and AR/VR experiences since it enables low-latency processing and real-time data analysis. With 5G (Sharma et al., 2020), content providers can cache and distribute material closer to the network's edge thanks to CDNs. Users will get a faster, more seamless access to internet services and multimedia content as a result of the reduced latency.

Due to its large bandwidth and low latency, 5G is perfect for providing realistic AR and VR experiences. Applications for these technologies include virtual tours, gaming, and remote instruction, among others. Real-time telemedicine and remote healthcare services such as online consultations, remote monitoring of medical records

and remote assistance for surgeries are made possible by 5G. 5G's dependability and reduced latency are essential for these kinds of applications (Mangla et al., 2023).

The utilization of IoT devices and sensors to improve municipal services, increase energy efficiency, and simplify city administration is made possible by 5G.5G enables the development of private networks customized to meet certain industrial and business requirements. 5G can be used by businesses to provide specialized services and safe, dedicated connectivity. Innovative apps, services, and industries have a plethora of opportunities thanks to these new 5G service delivery models. They rely on the primary features of 5G networks lower latency, faster data rates, and network slicing to offer better user experiences and accommodate a range of use cases.

The 5G Network Opportunities: It is anticipated that 5G networks will revolutionize mobile broadband by offering customers more opportunities. Here are some significant opportunities that 5G service providers are offering to their customers (Zhang et al., 2019), (Liet al., 2019), (Wang et al., 2019), (Qiao et al., 2019). The number of cellular phone users and data-intensive applications is exponentially growing, and existing cellular networks cannot support this demand. This problem should be resolved by 5G, which will offer fast speed, increased bandwidth, and minimal latency. The economy's main sectors—healthcare, manufacturing, education, energy, transportation, and logistics, for example—will all function as planned and without any problems. Because 5G will connect everything, everywhere, a global digital economy will be created.

By making social services, job searching, and other activities more accessible, it will expand economic chances. It will benefit different communities by giving people anywhere in the world access to high-speed internet at a reasonable price.

6. THREAT LANDSCAPE AND SECURITY CHALLENGES

A 5G network's extensive interconnectedness and rapid data transfer improve the threat environment. In these situations, to gain clients' trust in 5G services, 5G service providers must develop a thorough architecture, threat assessment, asset identification, exposure identification, and appropriate network management and control. It is necessary to identify the main security vulnerabilities that affect every tier of the 5G network and to take proactive steps to defend it from both internal and external cyber-attacks (Zhang et al., 2019), (Li et al., 2019), (Ahmad et al., 2017).

The attack surface is increased by the advent of edge computing, IoT, and device proliferation in 5G networks, giving potential attackers more places to enter the network. Device connections may be routed to the rogue infrastructure as a result of attackers impersonating genuine network access points using rogue base stations or

small cells. Because many IoT devices lack strong security safeguards, they are open to hacking. IoT devices that have been compromised can be utilized in botnets for a variety of assaults. Because 5G uses higher frequency channels, it might be simpler for adversaries to collect signals over shorter distances, which could jeopardize the secrecy of data. Because computer resources are dispersed closer to the edge of the network, edge computing raises security risks. Accessing edge devices or data without authorization might result in security lapses. Attacks on the infrastructure and equipment supply chain for 5G may present vulnerabilities at the hardware or software level, jeopardizing the network's integrity and security. Attacks on 5G networks have the potential to seriously jeopardize vital infrastructure, such as emergency services, energy, healthcare, and transportation.

Vulnerabilities in software-defined networking and network function virtualization components are among the new security issues brought about by the virtualization of network services and the usage of cloud-based infrastructure. Strong security mechanisms, such as encryption, authentication, access control, intrusion detection systems, and frequent software updates, are needed to counter these dangers in the context of 5G. To lessen the dangers connected with 5G technology, stakeholders must work together, adhere to security standards, and continuously monitor and respond to emerging threats.

Security Challenges: To guarantee the confidentiality, integrity, and availability of network services and data, the introduction of 5G networks poses security problems, including important issues. Malicious actors find it more enticing to target the growing attack surface created by the proliferation of connected devices and the development of 5G network infrastructure. IoT gadgets will proliferate thanks to 5G networks, but many of them lack strong security safeguards, making them vulnerable to hackers. With so many small cells and edge devices, 5G's distributed architecture greatly increases the complexity of network security and raises the possibility of vulnerabilities. Network slicing offers isolation and customization, but if not configured properly, an attacker might compromise one slice and impact others, creating security risks. Inconsistencies and vulnerabilities may arise in the 5G ecosystem due to the lack of consistent security standards and practices.

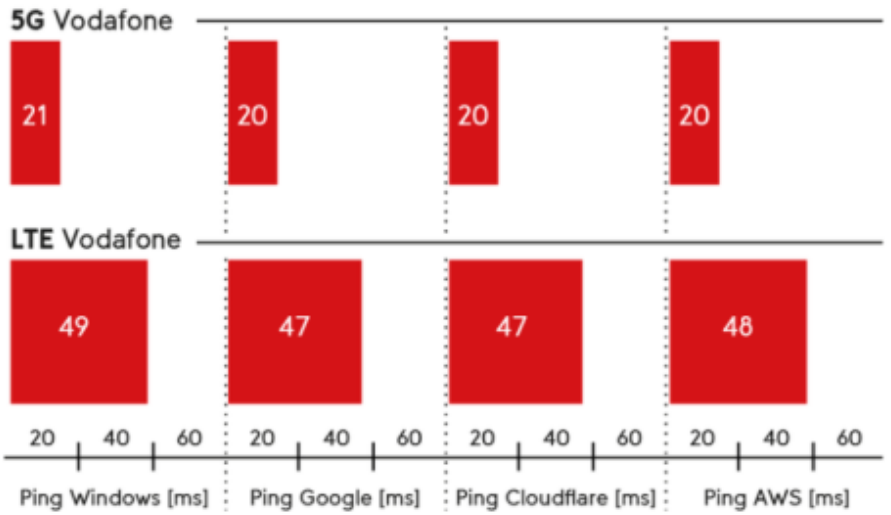
7. RELATED WORK IN 5G NETWORKS AND CASE STUDY

Global operators are building 5G mobile networks or adding first 5G cells to already-existing infrastructures. As a case study, Umlaut and Connect measured data connectivity using 5G technology in a few chosen nations. In Madrid, Spain, they used Samsung Galaxy S10 5G smartphones for driving testing. With peak download data rates of 511.5 Mbps in 5G mode and upload data rates of 69.6 Mbps, the

findings demonstrated remarkable performance. Low latency was further enhanced by 5G; in 5G mode, ping times to many web services dropped from 47 to 50 ms over LTE to around 20 ms. These outstanding outcomes point to a promising and highly effective future for mobile services that are linked. 5G latency comparison with different networks can be shown in Figure 8.

Some of the recent work done by researchers in the filed of 5G networks are summarized in Table 3.

Figure 8. 5G latency comparison with different networks



8. CONCLUSION

Globally, network operators are attempting to transition to 5G. 5G represents a significant advancement over 4G technologies, with significant improvements in data throughput, latency, capacity, bandwidth, and other areas. However, it is necessary to synthesize 5G prospects and problems in order to raise awareness among the general public as well as 5G researchers and practitioners. In order to do this, a through survey which offers information on 5G prospects, difficulties, security services, typical attacks that target 5G, and mitigation strategies is presented here.

Additionally, a case study of a cellular corporation with headquarters in Spain is presented, so that readers may compare 5G to current networks. The case study's findings demonstrate that, in terms of latency and data rate, 5G outperforms 4G

and other current networks. However, because 5G-capable devices are expensive and scarce, 5G is still not widely used. The majority of cell phones are anticipated to support 5G in the coming years, which will have a favourable effect on all the main spheres of life.

Table 3. Recent work towards 5G network

References	Work	Limitations
(Yan et al., 2021)	The authors provide an analytical analysis of the security threats associated with private 5G networks used in industrial settings.	The authors disregard other compelling mitigation techniques in favour of emphasizing authentication procedures as the main line of defence.
(Corici et al., 2021)	With this study, a safe roaming solution between private 5G networks and other nearby and far-off networks is introduced. Encouraging flexibility and mobility inside the network is the goal.	This research offers a secure roaming solution between other adjacent and distant networks and private 5G networks. The objective is to promote adaptability and mobility within the network.
(Mahmood et al., 2022)	Give a thorough analysis of potential uses and applications for industrial private networks by examining the security features of various deployment choices.	The physical layer security and intrusion detection systems need more investigation.
(Banda et al., 2022)	The article offers instructions for the use of this technology in various nations and situations and examines the economic models of 5G networks generally and private 5G networks specifically.	A more thorough investigation on security is absent, despite a few succinct definitions being provided.
(Tang et al., 2021)	The study makes advantage of 5G characteristics to provide a new architecture for smart healthcare that adds new components to meet hospital needs and make long-term operation easier.	The authors stressed the importance of security in sensitive data management and in the hospital setting, but they omitted a discussion of the security features of the newly suggested design.

REFERENCES

Ahmad, I., Kumar, T., Liyanage, M., Okwuibe, J., Ylianttila, M., & Gurtov, A. (2017, September). 5G security: Analysis of threats and solutions. *2017 IEEE Conference on Standards for Communications and Networking (CSCN)*. IEEE. 10.1109/CSCN.2017.8088621

Almusaylim, A., Z., & Jhanjhi, N. (2019, October 17). Comprehensive Review: Privacy Protection of User in Location-Aware Services of Mobile Cloud Computing. *Wireless Personal Communications*, *111*(1), 541–564. doi:10.1007/s11277-019-06872-3

Apruzzese, M., Bruni, M. E., Musso, S., & Perboli, G. (2023, August 1). 5G and Companion Technologies as a Boost in New Business Models for Logistics and Supply Chain. *Sustainability (Basel)*, *15*(15), 11846. doi:10.3390/su151511846

Aqeel, M., Ali, F., Iqbal, M. W., Rana, T. A., Arif, M., & Auwul, M. R. (2022, September 29). A Review of Security and Privacy Concerns in the Internet of Things (IoT). *Journal of Sensors*, *2022*, 1–20. doi:10.1155/2022/5724168

Banda, L., Mzyece, M., & Mekuria, F. (2022). 5G Business Models for Mobile Network Operators—A Survey. *IEEE Access : Practical Innovations, Open Solutions*, *10*, 94851–94886. doi:10.1109/ACCESS.2022.3205011

Corici, M., Chakraborty, P., Magedanz, T., Gomes, A. S., Cordeiro, L., & Mahmood, K. (2021, October 6). 5G Non-Public-Networks (NPN) Roaming Architecture. *2021 12th International Conference on Network of the Future (NoF)*. IEEE. 10.1109/NoF52522.2021.9609936

Duan, W., Gu, J., Wen, M., Zhang, G., Ji, Y., & Mumtaz, S. (2020, September). Emerging Technologies for 5G-IoV Networks: Applications, Trends and Opportunities. *IEEE Network*, *34*(5), 283–289. doi:10.1109/MNET.001.1900659

Fong, T. J., Abdullah, A., Jhanjhi, N., & Supramaniam, M. (2019). The Coin Passcode: A Shoulder-Surfing Proof Graphical Password Authentication Model for Mobile Devices. *International Journal of Advanced Computer Science and Applications*, *10*(1). doi:10.14569/IJACSA.2019.0100140

Ganesh Babu, R., Obaidat, M. S., Amudha, V., Manoharan, R., & Sitharthan, R. (2020, August 18). Comparative analysis of distributive linear and non-linear optimised spectrum sensing clustering techniques in cognitive radio network systems. *IET Networks*. doi:10.1049/iet-net.2020.0122

Hasnat, M. A., Rumee, S. T. A., Razzaque, M. A., & Mamun-Or-Rashid, M. (2019, February). Security Study of 5G Heterogeneous Network: Current Solutions, Limitations & Future Direction. *2019 International Conference on Electrical, Computer and Communication Engineering (ECCE)*. IEEE. 10.1109/ECACE.2019.8679326

Humayun, M., Hamid, B., Jhanjhi, N., Suseendran, G., & Talib, M. N. (2021, August 1). 5G Network Security Issues, Challenges, Opportunities and Future Directions: A Survey. *Journal of Physics: Conference Series*, *1979*(1), 012037. doi:10.1088/1742-6596/1979/1/012037

Humayun, M., Jhanjhi, N., Alruwaili, M., Amalathas, S. S., Balasubramanian, V., & Selvaraj, B. (2020). Privacy Protection and Energy Optimization for 5G-Aided Industrial Internet of Things. *IEEE Access : Practical Innovations, Open Solutions*, *8*, 183665–183677. doi:10.1109/ACCESS.2020.3028764

Hussain, R., Hussain, F., & Zeadally, S. (2019, December). Integration of VANET and 5G Security: A review of design and implementation issues. *Future Generation Computer Systems*, *101*, 843–864. doi:10.1016/j.future.2019.07.006

Hussain, S. J., Irfan, M., Jhanjhi, N. Z., Hussain, K., & Humayun, M. (2020, August 9). Performance Enhancement in Wireless Body Area Networks with Secure Communication. *Wireless Personal Communications*, *116*(1), 1–22. doi:10.1007/s11277-020-07702-7

Javaid, M., Haleem, A., Singh, R. P., & Suman, R. (2023, June). 5G technology for healthcare: Features, serviceable pillars, and applications. *Intelligent Pharmacy*, *1*(1), 2–10. doi:10.1016/j.ipha.2023.04.001

Javaid, N., Sher, A., Nasir, H., & Guizani, N. (2018, October). Intelligence in IoT-Based 5G Networks: Opportunities and Challenges. *IEEE Communications Magazine*, *56*(10), 94–100. doi:10.1109/MCOM.2018.1800036

Khan, R., Kumar, P., Jayakody, D. N. K., & Liyanage, M. (2020). A Survey on Security and Privacy of 5G Technologies: Potential Solutions, Recent Advancements, and Future Directions. *IEEE Communications Surveys and Tutorials*, *22*(1), 196–248. doi:10.1109/COMST.2019.2933899

Li, G., Sun, C., Zhang, J., Jorswieck, E., Xiao, B., & Hu, A. (2019, May 15). Physical Layer Key Generation in 5G and Beyond Wireless Communications: Challenges and Opportunities. *Entropy (Basel, Switzerland)*, *21*(5), 497. doi:10.3390/e21050497 PMID:33267211

Mahmood, A., Abedin, S. F., Sauter, T., Gidlund, M., & Landernas, K. (2022, June). Factory 5G: A Review of Industry-Centric Features and Deployment Options. *IEEE Industrial Electronics Magazine*, *16*(2), 24–34. doi:10.1109/MIE.2022.3149209

Mangla, C., Rani, S., Faseeh Qureshi, N. M., & Singh, A. (2023, June). Mitigating 5G security challenges for next-gen industry using quantum computing. *Journal of King Saud University. Computer and Information Sciences*, *35*(6), 101334. doi:10.1016/j.jksuci.2022.07.009

Nataraj, S. K., Al-Turjman, F., Adom, A. H. B., R, S., M, R., & R, K. (2022, September 15). Intelligent Robotic Chair With Thought Control and Communication Aid Using Higher Order Spectra Band Features. *IEEE Sensors Journal*, *22*(18), 17362–17369. doi:10.1109/JSEN.2020.3020971

Natarajan, B., Obaidat, M. S., Sadoun, B., Manoharan, R., Ramachandran, S., & Velusamy, N. (2021, December). New Clustering-Based Semantic Service Selection and User Preferential Model. *IEEE Systems Journal*, *15*(4), 4980–4988. doi:10.1109/JSYST.2020.3025407

Norp, T. (2018). 5G Requirements and Key Performance Indicators. *Journal of ICT Standardization*, *6*(1), 15–30. doi:10.13052/jicts2245-800X.612

Omar, M. A. A., & Zaman, N. (2017). Internet of Things (IoT): Charity Automation. *International Journal of Advanced Computer Science and Applications*, *8*(2). doi:10.14569/IJACSA.2017.080222

Qiao, X., Ren, P., Nan, G., Liu, L., Dustdar, S., & Chen, J. (2019, September). Mobile web augmented reality in 5G and beyond: Challenges, opportunities, and future directions. *China Communications*, *16*(9), 141–154. doi:10.23919/JCC.2019.09.010

Sharma, P. K., Park, J., Park, J. H., & Cho, K. (2020). Wearable Computing for Defence Automation: Opportunities and Challenges in 5G Network. *IEEE Access : Practical Innovations, Open Solutions*, *8*, 65993–66002. doi:10.1109/ACCESS.2020.2985313

Tang, X., Zhao, L., Chong, J., You, Z., Zhu, L., Ren, H., Shang, Y., Han, Y., & Li, G. (2021, November 19). 5G-based smart healthcare system designing and field trial in hospitals. *IET Communications*, *16*(1), 1–13. doi:10.1049/cmu2.12300

Varga, P., Peto, J., Franko, A., Balla, D., Haja, D., Janky, F., Soos, G., Ficzere, D., Maliosz, M., & Toka, L. (2020, February 4). 5G support for Industrial IoT Applications— Challenges, Solutions, and Research gaps. *Sensors (Basel)*, *20*(3), 828. doi:10.3390/s20030828 PMID:32033076

Verma, L., & Lalwani, M. (2019). Digital Transformation. *Technology Optimization and Change Management for Successful Digital Supply Chains*, 256–274. doi:10.4018/978-1-5225-7700-3.ch013

Wang, N., Wang, P., Alipour-Fanid, A., Jiao, L., & Zeng, K. (2019, October). Physical-Layer Security of 5G Wireless Networks for IoT: Challenges and Opportunities. *IEEE Internet of Things Journal*, *6*(5), 8169–8181. doi:10.1109/JIOT.2019.2927379

Wang, N., Wang, P., Alipour-Fanid, A., Jiao, L., & Zeng, K. (2019, October). Physical-Layer Security of 5G Wireless Networks for IoT: Challenges and Opportunities. *IEEE Internet of Things Journal*, *6*(5), 8169–8181. doi:10.1109/JIOT.2019.2927379

Zhang, P., Yang, X., Chen, J., & Huang, Y. (2019). A survey of testing for 5G: Solutions, opportunities, and challenges. *China Communications*, *16*(1), 69–85. doi:10.12676/j.cc.2019.01.007