World Journal of Advanced Engineering Technology and Sciences

eISSN: 2582-8266

Cross Ref DOI: 10.30574/wjaets

Journal homepage: https://wjaets.com/

(Review Article)

Check for updates

Cyber-security and performance Issues in 4G LTE network

Lydiah Moraa Machora *

Jaramogi Oginga Odinga University of Science and Technology, 40601, Bondo.

World Journal of Advanced Engineering Technology and Sciences, 2024, 12(02), 622–662

Publication history: Received on 01 June 2024; revised on 03 August 2024; accepted on 06 August 2024

Article DOI: https://doi.org/10.30574/wjaets.2024.12.2.0328

Abstract

The 4G LTE (Long Term Evolution) network represents a substantial challenge in wireless communication technology, providing slightly improved data transfer rates, decreased response time, and heightened connectedness from the 3G network. Nevertheless, there are significant worries surrounding the cybersecurity of these sophisticated network. The convergence of people, procedures, and technology to defend business, persons, or networks against digital attacks is known as cybersecurity. Cybersecurity is essential to protect organizational assets from risks such as but not limited to personal data breaches, unauthorized access leading to reputational and financial impact (Sandhu 2021). Previously isolated systems are now interconnected and sharing data. (Möller 2023) states that this connectedness also poses some inconveniences as well, whenever a device joins the Internet, it becomes publicly discovered. Once these devices are discovered, they become open to cyberattacks (Singh & Kumar, 2020 and Aphane, 2023). Cybersecurity has become an essential part of our daily lives due to the increasing frequency and severity of cyberattacks. Cybersecurity consultants face a significant challenge in measuring the effectiveness of cybersecurity measures in organizations in terms of performance in the 4G LTE networks. Another challenge could be finding a cybersecurity architecture that is effective and can fit different situations (Mbelli and Dwolatzky, 2016; Carcary, Doherty & Conway, 2019). The main aim of this study was to look on cybersecurity and performance issues on the 4G LTE networks, develop a comprehensive cybersecurity architecture that can be used by cybersecurity consultants when measuring cybersecurity effectiveness, performances and the solutions in security, privacy and performance. The following section will provide a brief overview of cybersecurity architectures, then followed by the research methodology utilised in this study. The proposed cybersecurity architecture presented and followed by the research methodology, summary of the results and implications of the study.

Keywords: 4G Network; Cybersecurity; Performance

1. Introduction

Cybersecurity, a critical feature in today's always-connected digital world, is scrutinized more than ever as we migrate from 4G Long-Term Evolution (LTE) networks to the future 5G networks [1]. The current article is prompted by an urgent necessity to study on cybersecurity performance of 4G LTE network. While the benefits of previous networks before 4G in terms of speed and efficiency are widely known, there still needs to be a more thorough understanding of how these technologies compare regarding the performance. 4G LTE networks have been around for a while and are well-known for their weaknesses and defenses. The security procedures of 4G LTE have been thoroughly examined, resulting in fixes, upgrades, and newer versions of security protocols [2]. Its evolution called 5G, conversely, is based on a more complicated design that incorporates new technologies such as network slicing, edge computing, and a rise in connected devices due to the IoT. While these features provide several advantages, they create new layers of possible vulnerabilities, further complicating the 4G cybersecurity picture. The convergence of various technologies inside the 4G ecosystem necessitates a full review of current security models and the development of new paradigms to handle these specific issues [3]. Understanding how well 4G networks can survive cyberattacks compared to 3G LTE networks

* Corresponding author: Lydiah Moraa Machora

is becoming more important as cyber threats become more complex. Will 4G's sophisticated features make it more resistant to the cybersecurity, or will they provide new entry points for hackers in its performances? Answering these concerns is crucial for individual users, corporations, and governments banking heavily on cybersecurity and performance issues in 4G technology to power anything [4]. The 4G wireless technology has recently coined for improving broadband performance and allowing multimedia programs. Therefore, its architectures and standards have considerably enhanced to transfer higher data rates than 2G and 3G. Meanwhile, Long-Term Evolution (LTE) has evolved to become one of the effective technologies that accomplish the 4G wireless performance goals. The authors in [5] has investigated a new threat known as paging storm attacks, this attack affects the cell's limitation of LTE adds a delay in requesting. Paging storm attacks can be launched from a regional botnet to exhaust the limited paging capacity of cells in a 4G/LTE (Long-Term Evolution) network. As paging storm attacks can delay paging requests and affect the productivity in video calls and the voice in the calling applications. 4G/LTE is mentioned in [6] as consisting of two main components which are the E-UTRAN and the EPC, each of these is prone to various types of attacks. Recent studies shows that 4G/LTE is exposed to many threats or attacks that menace its integrity [7], performance and security issues. LTE architecture is an open access system that means it can connect to any network at any time. The authors in [8] have made a survey on threats that put LTE security at risk. Even with the security improvements that have been implemented onto LTE, there is still vulnerability in integrity, performance and security issues which needs to be protected.

1.1. Problem Statement

The global transition from 4G LTE to other network technologies like the 5G technology is set to transform various industries, including healthcare, transportation, industrial automation, and others. While the benefits of data speed, latency, and device connection are widely recognized, there needs to be a significant gap in the understanding and appraisal of the cybersecurity consequences of this technological transition. As wireless networks expand, so do the complications associated with safeguarding these networks and their performances. The cybersecurity world is teeming with ever changing and more sophisticated threats, and each generation of wireless technology introduces its own set of difficulties and risks. Because 4G LTE networks have been operational for a long time, their security and performance have gone through several revisions, assessments, and enhancements. Thus, the problem addressed by this article is to comprehensively evaluate cybersecurity and performance of 4G LTE network.

2. 4G LTE architecture

An LTE architecture includes the modules needed to install network protocols between base stations and mobile systems [9]. As presented in Figure 1 above, the 4G LTE system architecture involves three modules: User Equipment (UE), Evolved Universal Terrestrial Radio Access Network (E-UTRAN), and Evolved Packet Core (EPC). The UE, for example, laptops or smartphones, can link to the wireless network across the evolved NodeB (eNodeB) using the EUTRAN base stations [10]. The eNodeB utilizes some access network protocols for exchanging messages with the UE. The E-UTRAN links to the EPC which is an IP-based infrastructure, while the EPC links to the provider of the wireline IP network [11]. The 4G LTE network architecture has some enhancements compared to 3G wireless network.

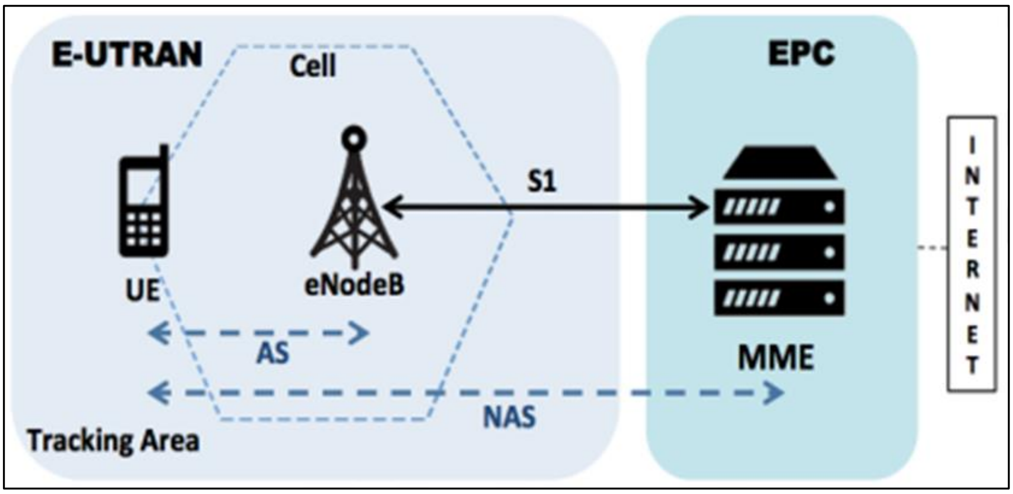

Figure 1 4G LTE System Architecture

Firstly, it has two types of network elements (NEs): the eNodeB that is an improved base station and the Access Gateway (AGW) that integrates all the functions, specifically Mobility Management Entity (MME), needed for the EPC. The MME can control the UE identification, as well as processing security authentication and mobility. LTE can support a meshed structure that improves wireless network performance, for example, an eNodeB can connect with several AGWs. On the hand, as the architecture is compatible with the TCP/IP model, traffic packets at any UE can be handled using the AGW and eNodeB with different IP-based devices, such as routers. Table 1 presents a summary of the features of the 4G Technologies.

Table 1 Characteristics of 4G Technologies

Features	**4G**
Standards	Single unified standard, ITU, IMT-Advanced
Data Rates	100Mps
Services	Dynamic information access with higher multimedia quality, wearable devices
Technology	Unified IP, seamless combination of broad-band, LAN/WAN/PAN, WLAN
Core network	Internet
Multiplexing	CDMA

3. Security Issues In 4G LTE Network

In 4G LTE Network, security issues identified on the layers that are inserted in the 4G LTE network architecture on the unique identifiers (IDs) for smartphones (i.e., UEs). A temporary unique ID is used on the SIM card which had security issues until it had to be temporarily placed to prevent attackers from stealing identifiers. Another security issues which were seen was 4G singling between UE and ME until the technique for improving 4G security was added to protect singling between the UE and MME [12]. Security mechanisms are utilized to secure the connections between 4G networks and secure non-4G networks using key management authentication protocols. Although several security controls are used for 4G/LTE wireless technology, its design, which is based on an open-IP architecture.

As explained in [13], 4G LTE (Long-Term Evolution) is a standard for wireless broadband communication, designed to provide high-speed data and voice communication. While it offers significant advancements over previous generations, such as faster speeds and lower latency [14], it also introduces a range of security challenges. The increased complexity and openness of LTE networks make them susceptible to various threats, necessitating robust security measures to protect user data and ensure network integrity. Some of the security threats in these networks are described in the sub-sections below.

3.1. Eavesdropping and Data Interception

One of the primary security concerns in 4G LTE networks is eavesdropping, where attackers intercept communication between users and the network [15], [16]. Despite encryption mechanisms like IPSec and SSL/TLS being implemented, vulnerabilities in these protocols or weak configurations can be exploited [17], [18]. Attackers can capture and decrypt sensitive data, leading to privacy breaches and information theft. Therefore, it is crucial to continually update and strengthen encryption protocols to counteract evolving eavesdropping techniques [19], [20].

3.2. Man-in-the-Middle Attacks

Man-in-the-Middle (MitM) attacks are another significant threat in LTE networks. In such attacks, an adversary intercepts and potentially alters communication between two parties without their knowledge [21]. This can be done by exploiting weaknesses in the network's authentication processes or by using rogue base stations. These attacks exploit vulnerabilities in the network's authentication and encryption protocols to eavesdrop on sensitive data, such as personal information and login credentials [22], [23]. Figure 2 shows a typical MitM in a 4G network.

Although LTE networks use strong encryption and mutual authentication to mitigate such risks, MitM attacks can still occur if attackers manage to deploy rogue base stations or exploit weaknesses in the key exchange processes. Ensuring robust encryption standards, continuous monitoring for rogue elements, and implementing advanced authentication mechanisms are crucial to defending against these sophisticated threats [24], [25]. MitM attacks can lead to unauthorized access, data manipulation, and severe breaches in confidentiality and integrity [26]. Implementing mutual authentication and rigorous validation of network elements can mitigate these risks.

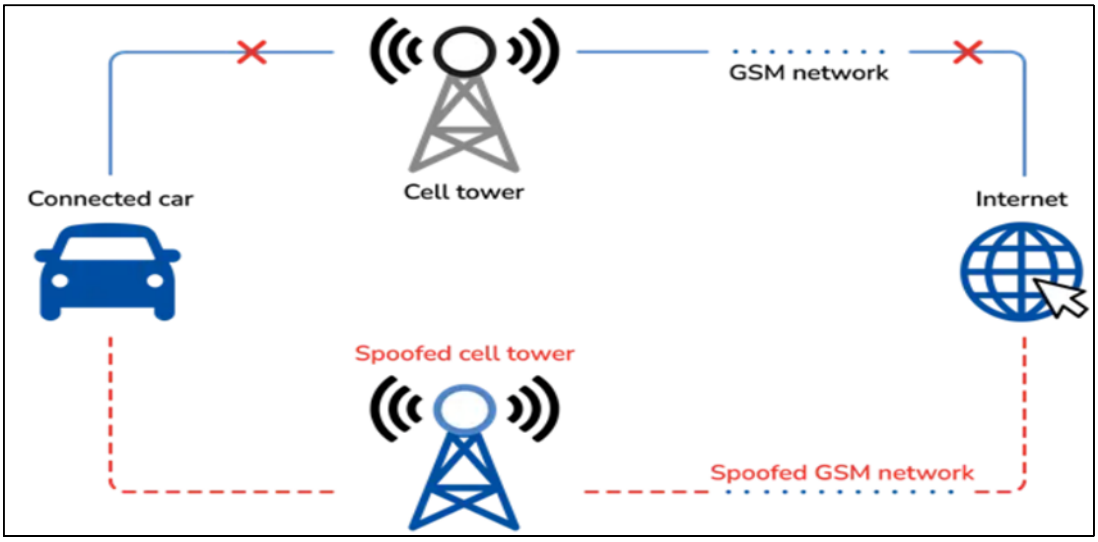

Figure 2 MitM in 4G network

3.3. Jamming and Denial of Service Attacks

Jamming attacks disrupt network services by overwhelming the communication channels with noise or false signals, rendering the network unusable for legitimate users [27]. Denial of Service (DoS) attacks flood the network with excessive traffic, causing service degradation or complete shutdown [28], [29]. Both types of attacks can severely impact the availability and reliability of LTE networks. As explained in [30], these attacks aim to disrupt communication services by overwhelming the network with excessive traffic or blocking legitimate signals. Jamming involves transmitting interference signals that disrupt the communication between user devices and base stations, leading to degraded service or complete service outages [31]. Figure 3 illustrates a typical jamming attack in 4G networks.

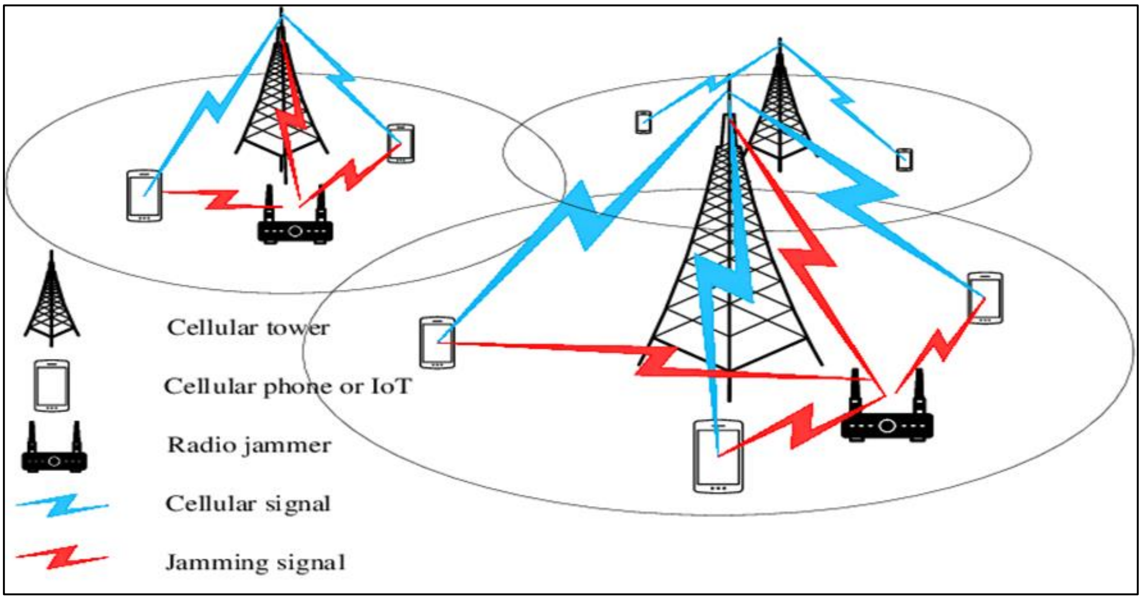

Figure 3 Jamming attacks in 4G network

DoS attacks target network resources by flooding them with malicious requests, causing congestion and preventing legitimate users from accessing network services. To combat these threats, strategies such as deploying advanced signal processing techniques, implementing traffic monitoring and filtering, and ensuring redundancy and load balancing are essential. Additionally, real-time detection systems that can identify and mitigate jamming and DoS activities are crucial for maintaining network reliability and availability [32]. Figure 5 below gives a depiction of a DoS attack in cellular network.

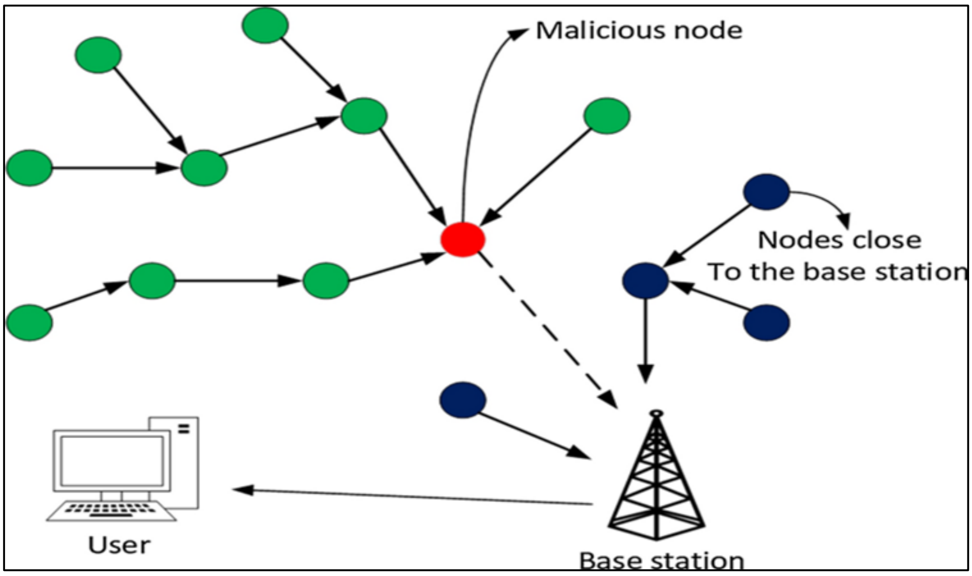

Figure 4 DoS attacks

Techniques such as spread spectrum technology and robust intrusion detection systems are essential to detect and mitigate these threats.

3.4. Rogue Base Stations (IMSI Catchers)

Rogue base stations, such as IMSI catchers or Stingrays, mimic legitimate cell towers to intercept communications, capture IMSI numbers, and track user locations [33], [34]. These can force devices to downgrade to less secure networks, increasing vulnerability to attacks. As discussed in [35], rogue base station attacks in 4G LTE networks involve malicious actors deploying unauthorized base stations that mimic legitimate ones, tricking user devices into connecting to them [36], [37]. An illustration of IMSI Catchers attack is depicted in Figure 5 below.

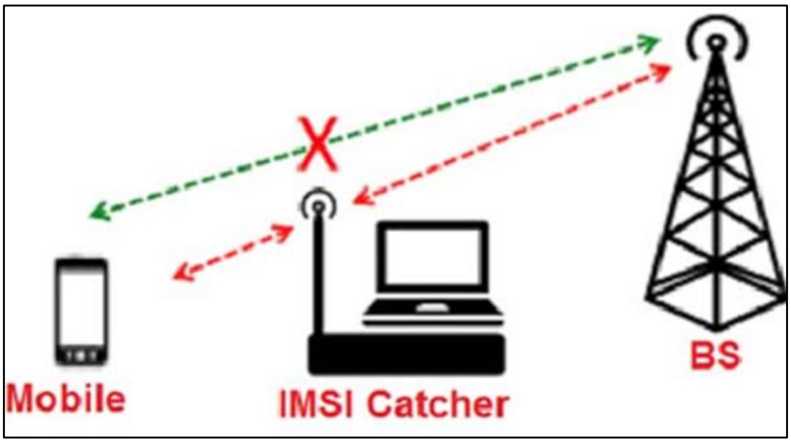

Figure 5 IMSI Catchers attack

Once connected, these rogue base stations can intercept or manipulate communications, potentially capturing sensitive information [38], injecting malicious content, or redirecting traffic to fraudulent services. These attacks exploit weaknesses in network authentication and the absence of stringent checks for base station legitimacy. To counteract this threat, network operators need to implement robust base station authentication protocols, utilize encryption to protect data transmission, and employ advanced monitoring systems to detect and neutralize unauthorized base stations quickly.

3.5. Signaling Storms

Signaling storms in 4G LTE networks refer to scenarios where an excessive number of signaling messages overwhelm the network's signaling infrastructure, leading to performance degradation and service disruptions [39], [40]. These attacks flood the network with unnecessary or malicious signaling requests, such as authentication or registration requests, which can exhaust network resources, cause delays, and even result in system outages. To mitigate the risk of signaling storms, it is crucial to implement robust traffic management and filtering mechanisms, deploy rate limiting to control signaling message volumes, and continuously monitor network traffic for unusual patterns that may indicate an ongoing attack [41]. Additionally, enhancing the network's capacity to handle high signaling loads and ensuring effective response strategies can help maintain service stability during such attacks [42]. Signaling storms occur when an overwhelming number of signaling messages are sent to the network, causing congestion and potential service disruption. These can be triggered intentionally by attackers or accidentally by malfunctioning devices.

3.6. Replay Attacks

Replay attacks in 4G LTE networks involve an attacker capturing valid signaling or data messages and retransmitting them to the network or another user to impersonate a legitimate entity or disrupt communications [43], [44]. By replaying previously intercepted messages, attackers can bypass authentication mechanisms, initiate unauthorized transactions, or inject malicious commands [45]. Although LTE networks use encryption and authentication protocols to mitigate such risks, vulnerabilities in these processes can still be exploited. To defend against replay attacks, implementing techniques like timestamping and sequence numbering to ensure the uniqueness of each message, along with strong encryption and secure key management practices, is essential for maintaining the integrity and security of network communications [46]. In replay attacks, an attacker captures a legitimate data transmission and retransmits it to the network. This can be used to gain unauthorized access or disrupt network services by repeating valid communication sessions.

3.7. LTE Redirection Attacks

Redirection attacks involve redirecting user traffic to malicious networks or websites. By exploiting vulnerabilities in the redirection mechanisms, attackers can intercept data, inject malicious content, or launch phishing attacks. As explained in [47], these attacks involve manipulating a user's connection to redirect them from a legitimate service to a malicious one, often without the user's knowledge. This can be achieved through tactics such as intercepting and altering signaling messages or exploiting vulnerabilities in the network's routing and authentication processes [48]. Once redirected, users may be exposed to phishing sites, malicious content, or unauthorized data collection. To counteract redirection attacks, it is crucial to implement robust security measures including secure signaling protocols, encryption of user data, and rigorous verification processes for network elements and services [49]-[50]. Additionally, continuous monitoring and anomaly detection can help identify and mitigate suspicious redirection attempts.

3.8. Downgrade Attacks

Downgrade attacks in 4G LTE networks involve forcing a network or device to revert to less secure protocols or weaker encryption standards, thereby exposing communications to increased risk [51], [52]. As shown in Figure 6, attackers exploit vulnerabilities in the network's ability to negotiate security settings, manipulating the system to use outdated or less robust encryption algorithms and protocols that are easier to break [53], [54]. This can lead to compromised data integrity and confidentiality.

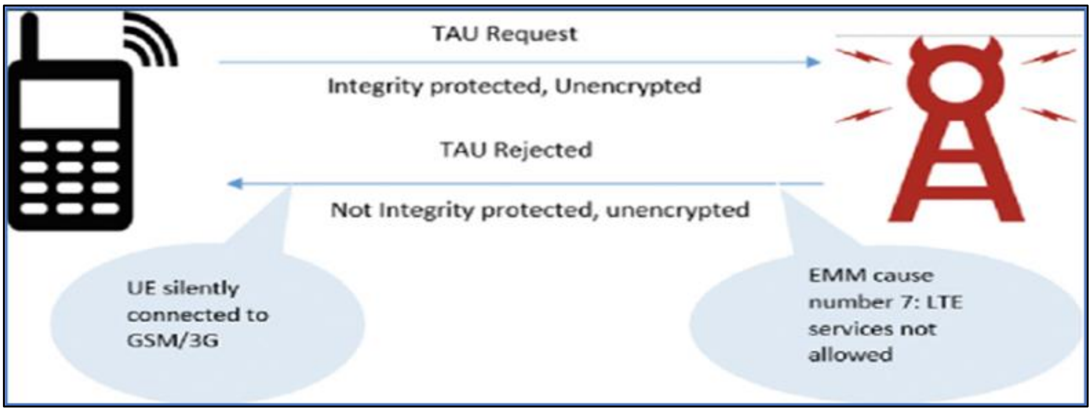

Figure 6 Downgrade attack

To mitigate downgrade attacks, it is essential to enforce strict protocol version control and ensure that only the most secure and up-to-date encryption standards are used. Implementing robust mechanisms for validating and negotiating security parameters can help prevent attackers from successfully downgrading network security [55]. Downgrade attacks force devices to switch to older, less secure network protocols (e.g., from 4G to 3G or 2G). These older protocols may have known vulnerabilities [56] that can be exploited to compromise security and intercept data.

3.9. Spoofing Attacks

Spoofing attacks involve masquerading as a legitimate network entity to deceive users or network components [57]. Attackers can impersonate base stations, user devices, or network elements to intercept communications or manipulate data. These attacks involve an attacker impersonating a legitimate entity, such as a base station, user device, or network element, to deceive and exploit other network participants [58], [59]. By mimicking trusted components, attackers can intercept or manipulate communications, gain unauthorized access to sensitive data, or disrupt network operations [60], [61]. Spoofing can target various elements, including User Equipment (UE) or evolved Node Bs (eNBs), and often exploits weaknesses in authentication and verification processes. To defend against spoofing attacks, it is crucial to implement strong authentication mechanisms [62], such as mutual authentication between devices and network elements, and to utilize encryption and secure signaling protocols to ensure the integrity and authenticity of communications.

3.10. IMSI Paging Attacks

IMSI paging attacks exploit the paging mechanism used to locate devices. Attackers can repeatedly trigger paging requests, causing excessive signaling and potential network congestion, leading to denial of service. As discussed in [63], IMSI paging attacks in 4G LTE networks involve an attacker exploiting the paging process, where the network attempts to locate a specific user device using its International Mobile Subscriber Identity (IMSI). An illustration of a typical IMSI paging procedure is depicted below.

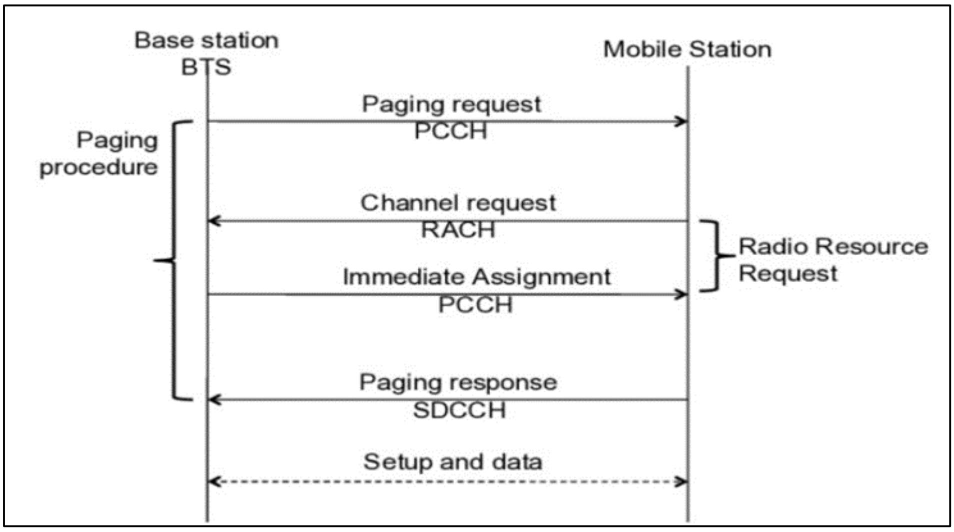

Figure 7 Paging procedure

In such attacks, the attacker may use a fake IMSI to flood the network with paging requests or use IMSI catchers to intercept and monitor the paging signals intended for legitimate users [64]- [67]. This can lead to unauthorized tracking of user locations, interception of communications, or disruption of the paging process. To mitigate IMSI paging attacks, implementing techniques like IMSI anonymization, paging encryption, and enhanced monitoring of paging traffic for unusual patterns can help protect user privacy [68] and network integrity.

3.11. RRC (Radio Resource Control) Attacks

Radio Resource Control (RRC) attacks in 4G LTE networks involve exploiting vulnerabilities in the RRC protocol, which manages the allocation and control of radio resources between user devices and base stations [69]. Attackers may initiate unauthorized RRC connections, manipulate signaling messages to disrupt resource allocation, or overload the network with fraudulent requests. Such attacks can degrade network performance, cause service interruptions, or lead to unauthorized access [70]-[72]. A simplified radio resource management is depicted in Figure 8.

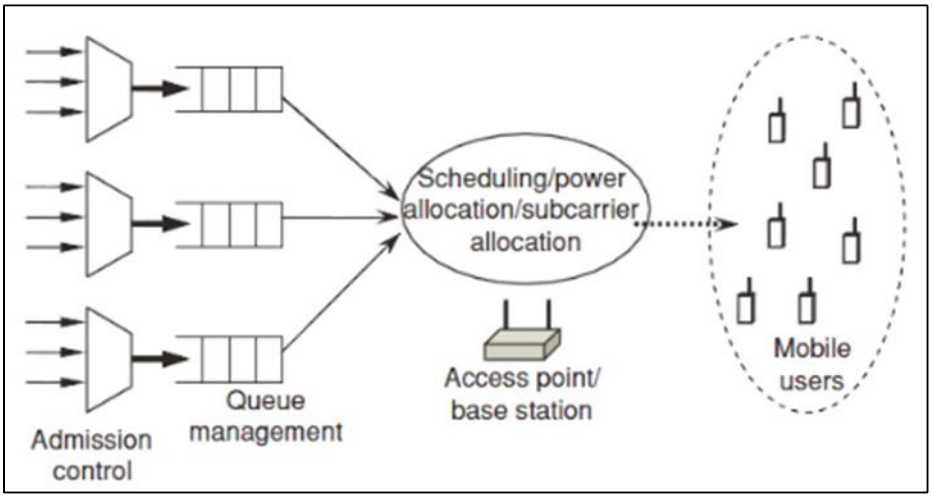

Figure 8 Radio resource management in 4G networks

To counteract RRC attacks, it is essential to implement robust security measures including authentication and integrity protection [73] for RRC messages, monitoring for abnormal signaling patterns, and deploying mechanisms to detect and prevent unauthorized RRC connection attempts. According to [74], RRC attacks target the control plane of the LTE network, manipulating the RRC signaling messages to disrupt network operations, cause service degradation, or execute unauthorized actions on user devices.

3.12. Resource Exhaustion Attacks

Resource exhaustion attacks deplete network resources such as bandwidth, processing power, or memory [75]. By overwhelming the network with requests, attackers can cause service interruptions and degrade performance. According to [76], resource exhaustion attacks in 4G LTE networks involve deliberately overwhelming network resources, such as signaling channels, processing capacity, or bandwidth, to degrade service quality or disrupt normal operations [77], [78]. Attackers achieve this by generating excessive or malformed signaling messages, initiating numerous connections, or consuming substantial amounts of network bandwidth. This can lead to service degradation, increased latency [79], and even network outages for legitimate users. To defend against resource exhaustion attacks, network operators should deploy traffic filtering and rate-limiting mechanisms, implement anomaly detection systems to identify unusual patterns, and ensure robust capacity planning and resource allocation strategies to maintain network resilience and service availability.

3.13. Stealth Attacks

Stealth attacks in 4G LTE networks involve malicious activities that are designed to evade detection and remain hidden while compromising network security [80]. Attackers employing stealth tactics might use sophisticated techniques to hide their presence, such as blending malicious traffic with legitimate network activity or exploiting subtle vulnerabilities that go unnoticed by conventional security systems [81], [82]. This can include stealthy data exfiltration, covert command and control channels, or subtle tampering with signaling messages. To counteract stealth attacks, it is crucial to implement advanced monitoring and anomaly detection systems that use machine learning and behavioral analysis to identify subtle deviations from normal network patterns [83], [84]. Additionally, regularly updating security protocols [85] and performing thorough security audits can help uncover and mitigate these hidden threats. Stealth attacks aim to avoid detection while compromising network security. These attacks use sophisticated techniques to hide malicious activities, making it difficult for security systems to identify and respond to threats.

3.14. Rogue Relay Attacks

Rogue relay attacks involve placing a malicious relay device between the user and the network. This device intercepts and manipulates communication, potentially altering data or injecting malicious content [86]. These attacks involve an attacker deploying a malicious relay node that intercepts and forwards communications between user devices and legitimate network components [87], [88]. By positioning themselves between the user and the network, attackers can eavesdrop on sensitive information, inject malicious data, or disrupt communication flows [89], [90]. This attack exploits vulnerabilities in the network's trust and authentication mechanisms, potentially compromising data integrity and user privacy [91]. Figure 9 shows a typical rogue relay attack.

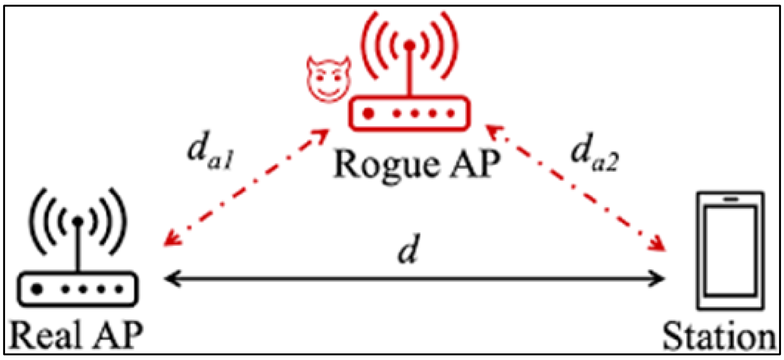

Figure 9 Rogue relay attacks

To defend against rogue relay attacks, it is essential to enforce strict authentication and encryption for all network nodes, implement robust anomaly detection systems to identify unauthorized relays, and regularly audit network elements to ensure they are operating within defined security parameters.

3.15. Timing Attacks

Timing attacks exploit the timing relationships between network events to infer sensitive information. By analyzing delays and response times, attackers can deduce details about network operations or user activities [92]. According to [93], timing attacks in 4G LTE networks exploit the predictable timing patterns in network operations to infer sensitive information or disrupt communication. By analyzing the timing of signaling messages or data transmissions, attackers can potentially deduce user behavior, network activities, or encryption keys [94], [95]. For instance, variations in response times or delays can reveal information about the network's internal processes or the presence of specific users [96]. To mitigate timing attacks, it is crucial to implement countermeasures such as randomizing timing intervals, introducing artificial delays to obfuscate timing patterns, and employing robust encryption techniques [97] to ensure that timing information alone cannot compromise data security or user privacy.

3.16. Baseband Attacks

Baseband attacks target the firmware and software that control the radio functions of mobile devices [98]. By exploiting vulnerabilities in the baseband, attackers can gain control over the device’s communication capabilities and intercept data. As explained in [99], baseband attacks in 4G LTE networks target the baseband processor, which handles low-level communication functions between the user device and the network. These attacks exploit vulnerabilities in the baseband firmware or hardware to gain unauthorized access to sensitive data, intercept communications, or inject malicious commands [100]-[102]. Baseband attacks can bypass higher-level security mechanisms because they operate at a lower level in the device’s architecture, making them particularly dangerous and difficult to detect. To mitigate baseband attacks, it is essential to regularly update baseband firmware with security patches, employ robust security mechanisms [103] at the hardware level, and implement stringent access controls and monitoring to detect and respond to unusual baseband activity.

3.17. Authentication Bypass Attacks

Authentication bypass attacks in 4G LTE networks involve exploiting weaknesses in the authentication process to gain unauthorized access to network resources or services [104]. Attackers may bypass the usual authentication mechanisms by exploiting vulnerabilities in the authentication protocols or by using techniques like fake base stations or compromised credentials [105]-[107]. This type of attack can lead to unauthorized access to sensitive user data, disruption of network services, or further exploitation of the network. Authentication bypass attacks exploit weaknesses in the authentication mechanisms of LTE networks. Attackers can bypass authentication procedures to gain unauthorized access to network services and user data [108]. To defend against authentication bypass attacks, it is critical to implement robust authentication protocols [109], ensure encryption of authentication exchanges, and continuously monitor for unusual authentication patterns that may indicate attempted bypasses. Additionally, regular updates and security patches for authentication systems help close potential vulnerabilities that could be exploited.

3.18. Network Slicing Attacks

As shown in Figure 10, network slicing attacks in 4G LTE networks involve exploiting the concept of network slicing, which allows multiple virtual networks to operate on a single physical infrastructure, each optimized for different applications or services [110]. Attackers may target the isolation mechanisms between slices to breach one slice and gain unauthorized access to resources or data in another slice. Such attacks can disrupt service quality, compromise sensitive data, or affect the performance of other slices [111]-[113].

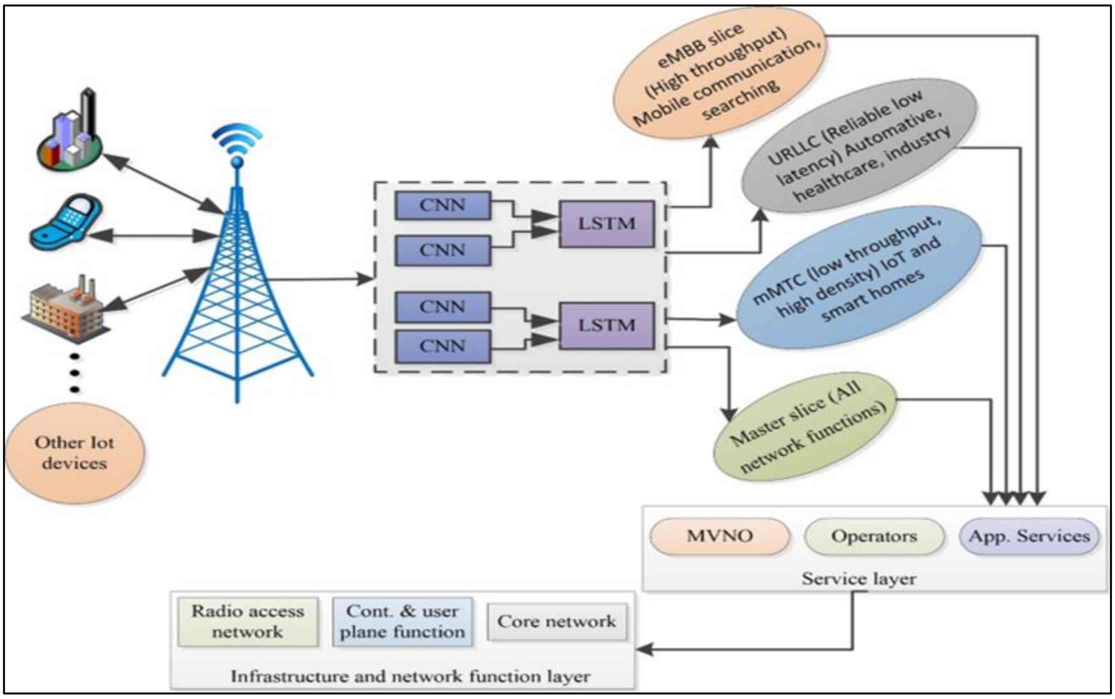

Figure 10 Network slicing

To mitigate network slicing attacks, it is essential to implement stringent isolation and segmentation policies, enforce robust access controls, and continuously monitor inter-slice communications for anomalies [114]. Additionally, applying security measures specific to each network slice and ensuring comprehensive end-to-end encryption [115] can help protect against potential breaches and maintain the integrity of isolated network environments. Network slicing in LTE allows multiple virtual networks to share the same physical infrastructure. Attacks on network slicing can compromise isolation between slices, leading to data leakage, resource misallocation, and security breaches.

3.19. Location Tracking

Location tracking in 4G LTE networks involves monitoring and determining the geographical position of user devices based on network signals, such as those exchanged between user equipment and base stations [116], [117], as shown in Figure 11. While location tracking can be used for legitimate purposes like providing location-based services, it can also pose significant privacy risks if misused or if unauthorized parties gain access to this information [118]-[120]. Attackers might exploit vulnerabilities in the location tracking system to track users without their consent or to gather sensitive location data for malicious purposes. To address these concerns, it is crucial to implement strong privacy protections [121], such as anonymizing location data and obtaining user consent for location-based services. Additionally, enhancing security measures around the transmission and storage of location data can help prevent unauthorized access and ensure that users' location information remains protected. Location tracking attacks exploit vulnerabilities in LTE protocols to track the physical location of users. By analyzing signaling messages and network interactions, attackers can monitor user movements and violate privacy.

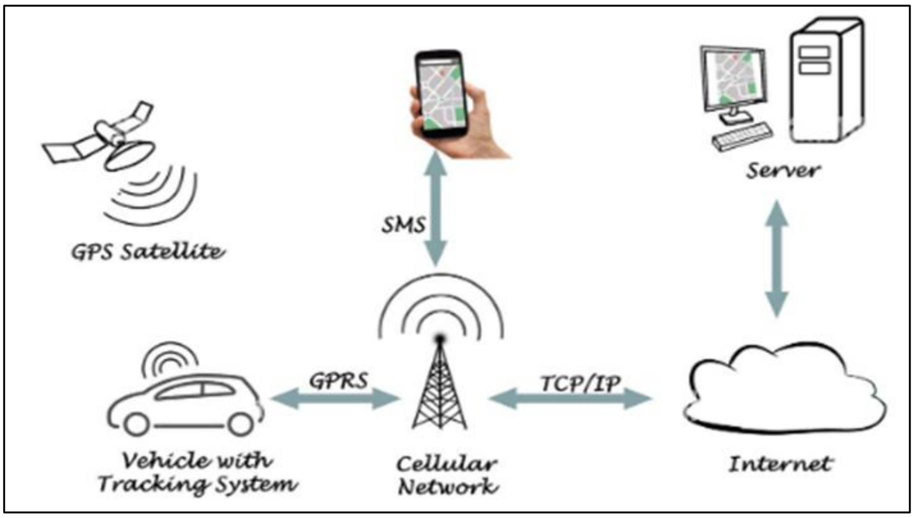

Figure 11 Location Tracking

3.20. Security in IoT Devices

The proliferation of Internet of Things (IoT) devices connected to 4G LTE networks introduces additional security challenges. Many IoT devices have limited computational resources and often lack robust security features, making them easy targets for attackers [122]-[126]. Compromised IoT devices can be used to launch large-scale attacks on the network. Ensuring secure firmware updates, employing device-level encryption [127], and implementing strict access controls are essential for securing IoT devices.

3.21. Threats to Core Network Elements

Core network elements such as the Serving Gateway (SGW) and the Packet Data Network Gateway (PGW) are critical components of the LTE architecture [128]-[132]. Attacks targeting these elements can disrupt the entire network, leading to service outages and data breaches. Protecting these core elements requires implementing strong authentication mechanisms [133], securing communication channels, and conducting regular security assessments to identify and address vulnerabilities.

3.22. Future Directions and Enhancements

As 5G networks are being rolled out, the security of 4G LTE networks remains crucial due to their coexistence and backward compatibility [134], [135]. Enhancing LTE security involves continuous monitoring, adopting advanced encryption algorithms, and integrating artificial intelligence for threat detection and response [136]-[138]. Collaboration among industry stakeholders, government agencies, and researchers is essential to develop and implement comprehensive security frameworks that address both current and emerging threats [139] in 4G LTE networks.

It is evident that while 4G LTE networks have revolutionized mobile communication, they also present numerous security challenges that must be addressed to protect users and ensure network reliability. From eavesdropping and MitM attacks to jamming and signaling storms, the threats are diverse and complex. Implementing robust security measures, ongoing monitoring, and proactive threat mitigation strategies are essential to safeguarding 4G LTE networks against these evolving threats. As technology advances, continuous efforts to enhance security protocols and practices will be critical in maintaining the integrity and trustworthiness of mobile communication networks.

4. Privacy Issues In 4G LTE Network

In this type of network, it has privacy issues on its attacks against the privacy of mobile users' data attempt to expose sensitive data/multimedia of users. A man-in-the-middle (MITM) attack is the most serious privacy issues in wireless networks that depend on a false base station attack when anomalous third-party masquerades its base transceiver station. For instance, we consider the privacy issue attack in the exploitation of vulnerabilities it creates threats and thus represents a risk from the point of view of the owner. Conversely, in the security methodology the perception of risks to assets by the owner leads to the implementation of a set of counter-measures within the telecommunication network. The owner wants to minimize risks in privacy and imposes countermeasures that he considers necessary to protect the asset, as shown in Figure 12. He therefore describes the security and privacy objective.

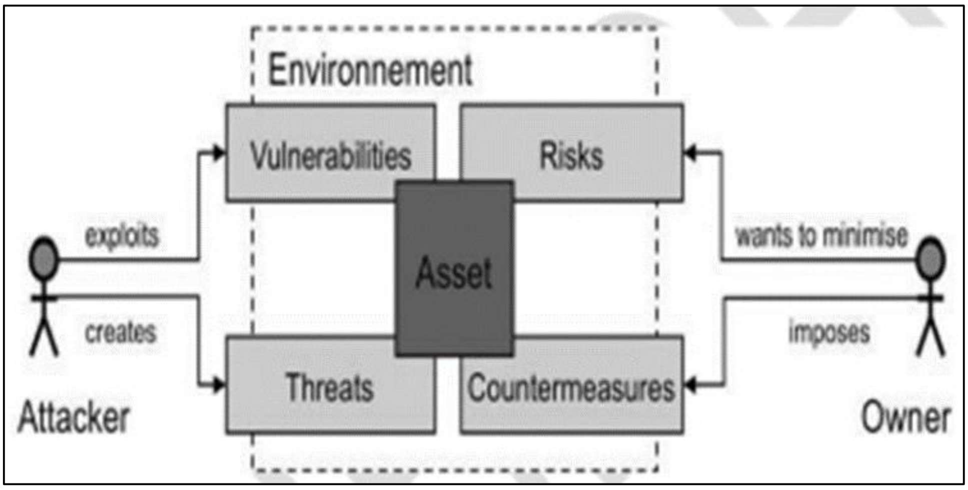

Figure 12 Relationship between asset, attacker and owner in privacy issue

Privacy issues in 4G networks arise from various vulnerabilities that can expose users' personal information and communications to unauthorized access. These issues include the risk of interception of data transmissions, location tracking, and exploitation of weak encryption protocols. Attackers can exploit flaws in the network architecture or use sophisticated techniques like IMSI catchers (Stingrays) to eavesdrop on calls and messages, capture sensitive data, and track users' movements. Additionally, the storage and processing of user data by network providers and third parties pose further risks of data breaches and unauthorized access, raising significant concerns about the protection of user privacy in 4G networks. Table 2 describes some of the privacy issues surrounding 4G LTE networks.

Table 2 Privacy Issues In 4G LTE Network

Privacy issue	**Description**
Location Tracking	4G LTE networks constantly exchange information to maintain connectivity, which can be exploited to track a user's location [140]-[144]. Techniques like analyzing cell tower connections and timing advance values enable adversaries to determine a user's movement patterns, posing significant privacy risks [145].
IMSI Catching	IMSI catchers or Stingrays mimic legitimate cell towers to intercept IMSI numbers, allowing attackers to track user devices [146]-[150]. This compromises the anonymity of users [151] and enables targeted surveillance and monitoring.
Metadata Exposure	Communication metadata, such as call durations, times, and participants, can reveal sensitive information about user behavior and relationships even if the content of the communication is encrypted [152]-[157]. This metadata can be collected and analyzed by malicious actors.
Data Retention Policies	Mobile network operators (MNOs) often retain user data, including communication logs and location history, for extended periods [158], [159]. This data, if accessed by unauthorized parties or misused by the operators themselves, can lead to significant privacy violations.
Unauthorized Data Access	Weak access controls and insufficient encryption of stored data in LTE networks can lead to unauthorized access by insiders or external attackers [160]-[162]. This compromises user privacy [163] and exposes sensitive information.
Subscriber Identity Module (SIM) Exploits	SIM cards store crucial information used for authentication and communication [163]-[168]. Exploiting vulnerabilities in SIM cards, such as the SIMjacker exploit, allows attackers to access sensitive data [169] and monitor user activities.

Rogue Base Stations	Rogue base stations can force devices to downgrade to less secure networks, capturing communication data and tracking users [170]. These attacks compromise the confidentiality and integrity of user communications.
User Profiling	Data collected from 4G LTE networks can be used to create detailed profiles of users, including their habits, preferences, and movements [171], [172]. Such profiling can be used for targeted advertising, social engineering, or even more malicious purposes.
Surveillance and Interception	Law enforcement and intelligence agencies may intercept communications for surveillance purposes [173]. While legal frameworks exist, unauthorized or excessive surveillance can infringe on user privacy rights.
Privacy Risks in IoT Devices	The proliferation of IoT devices connected to LTE networks introduces additional privacy risks [174]. Many IoT devices collect and transmit personal data, which can be intercepted [175] or misused if the devices are not adequately secured.
Network Slicing	Network slicing allows for the creation of multiple virtual networks on a single physical infrastructure [176]. If isolation between slices is not maintained, it can lead to data leakage and privacy breaches across different slices [177]-[179].
Third-Party Services	Mobile applications and services often rely on third-party providers, which may collect and process user data [180]. Weak privacy policies or inadequate security measures [181] in third-party services can result in data breaches and unauthorized access to user information.
Encryption Weaknesses	While LTE networks use encryption to protect data, weaknesses in encryption protocols or improper implementation can leave data vulnerable to interception and decryption by attackers [182]-[187].
Social Engineering Attacks	Attackers can use social engineering techniques to trick users into revealing sensitive information, such as login credentials or personal details [188], [189]. This information can be used to compromise user accounts and privacy.
Cross-Network Attacks	Interconnected networks, such as those between LTE and older generation networks (3G/2G), can be exploited to launch cross-network attacks [190]-[192]. Vulnerabilities in the older networks can be used to compromise the security and privacy [193] of LTE communications.
Insecure API Access	Application Programming Interfaces (APIs) used by LTE networks and services may have security weaknesses [194]. Exploiting these APIs can allow attackers to access sensitive data and perform unauthorized actions, compromising user privacy.
Denial of Service (DoS) Attacks	DoS attacks can disrupt network services, leading to the exposure of user data in transit or stored in the network [195]-[199]. Service disruptions can also force users to connect to less secure networks, increasing privacy risks.
Data Aggregation	Data collected from various sources within LTE networks can be aggregated to form a comprehensive profile of users [200], [201]. Unauthorized aggregation and analysis of such data can result in privacy violations and misuse of personal information.
Over-the-Air (OTA) Updates	OTA updates to mobile devices and network infrastructure can be intercepted or manipulated if not properly secured [202]. Compromised updates can introduce malware or alter device configurations, leading to privacy breaches.
Edge Computing Privacy Risks	The deployment of edge computing in LTE networks aims to reduce latency by processing data closer to the source [203], [204]. However, it also introduces privacy risks as sensitive data is processed and stored at the network edge, potentially exposing it to local threats [204], [205.

Evidently, the extensive use of 4G LTE networks for communication and data transfer introduces numerous privacy issues that need to be addressed. From location tracking and IMSI catching to unauthorized data access and profiling, users face a variety of threats to their personal information. Ensuring robust encryption, secure access controls, and privacy-conscious data handling practices are essential to protect user privacy in the evolving landscape of mobile networks. Continuous vigilance, coupled with advancements in security protocols and user awareness, will be crucial in mitigating these privacy risks.

5. Performance Issues In 4G Network

This section focuses on performances metrics in a 4G LTE Networks. Therefore, we will focus in the following metrics in relation to this study: - Throughput, Goodput, Latency, packet delivery ratio and bandwidth utilization.

5.1. Throughput

Throughput in 4G networks refers to the rate at which data is successfully transmitted from one point to another within the network. It is a critical performance metric that determines the efficiency and speed of data transfer, directly impacting the user experience in terms of browsing, streaming, and downloading content. High throughput is achieved through advanced technologies like Orthogonal Frequency Division Multiplexing (OFDM) and Multiple Input Multiple Output (MIMO), which enhance the capacity and reliability of the network. However, throughput can be affected by factors such as network congestion, signal interference, and the distance between the user and the cell tower. Ensuring optimal throughput is essential for meeting the high data demands of modern applications and maintaining the quality of service in 4G networks. Throughput in the 4G LTE network it drives a test in the data rate (Kbit/s) from the UE to the eNodeB [206].

5.2. Latency

Latency in 4G networks refers to the time delay between when a data packet is sent and when it is received at its destination. It is a crucial factor influencing the responsiveness of network-dependent applications, such as online gaming, video conferencing, and real-time communication services. Lower latency results in faster, more immediate interactions, enhancing the overall user experience. 4G networks typically aim to achieve latencies in the range of 30 to 50 milliseconds, which is significantly lower than previous generations. However, factors such as network congestion, signal quality, and the distance between the user and the server can impact latency. Managing and minimizing latency is essential for ensuring smooth and efficient network performance, particularly for applications requiring real-time data exchange. Latency is another important performance issue characteristic that is assess. We say latency, is the amount of time it takes for data to travel from source to destination [207]. Therefore, we can use Milliseconds (ms) to quantify latency as shown in the figure 2 below. The 4G Mean Latency is 50 Ms.

5.3. Packet delivery Ratio

Packet Delivery Ratio (PDR) in 4G networks is a key performance metric that measures the percentage of data packets successfully delivered from the source to the destination over the network. A high PDR indicates a reliable and efficient network, where most packets reach their intended destinations without loss, ensuring high-quality service for applications like voice calls, video streaming, and online gaming. Conversely, a low PDR can result in poor user experiences due to packet loss, which can cause interruptions, delays, and degraded quality of service. Factors influencing PDR include network congestion, signal interference, and the robustness of error correction protocols. Maintaining a high PDR is essential for the smooth operation of network services and for meeting user expectations in 4G networks. In wireless networks, the packet delivery ratio (PDR) is a metric that indicates the successful delivery of data packets from the sender to the receiver [208]. It refers to the percentage of packets reaching their intended destination without errors or loss.

5.4. Bandwidth Utilization

In this section, each generation of wireless cellular technology has introduced increased bandwidth speeds and network capacity. 4G has speeds of up to 150 Mbit/s download and 50 Mbit/s upload [209]. Figure 13 shows the 4G LTE network bandwidth utilization. Bandwidth in a computer network sense is, its transmission capacity, which (as it is a function of the speed of transmission) is usually expressed in bps (bits per second).

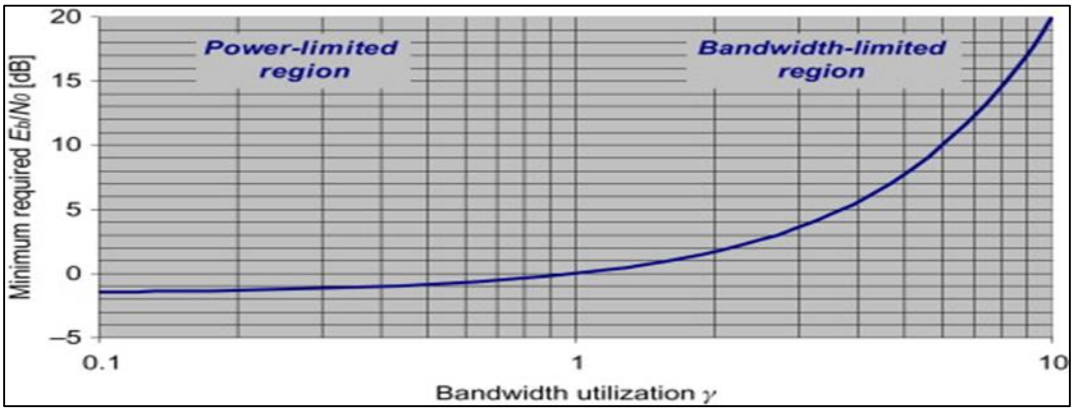

Figure 13 4G LTE Network Bandwidth Utilization

The most common wired bandwidths are 1 Gbps (often called gigabit Ethernet), 10 Mbps (standard Ethernet), and 100 Mbps (fast Ethernet). Wireless is generally slower; 802.11 g supports up to 54 Mbps, for example. Note that these are maximums and a wired network stands a better chance of providing the full bandwidth due to less interference.

5.5. Goodput

In this section we define goodput, that focuses on solely the useful application layer payload actually delivered across the network without including protocol overhead, retransmissions and error data. This is a measure of data throughput from the end-user viewpoint and represents the actual usable data delivered, as shown in Figure 14. Goodput is generally less than throughput because extra overhead and retransmitted data are not useful for the end user [210]. In practice, goodput is crucial to evaluate the real network performance. For instance, in high-latency [211] or congested networks, a considerable amount of the transmitted data is made up of control information, error correction information. or retransmissions due to loss of packets. These factors may exaggerate the reported throughput, distorting the network performance picture to a positive light. While the goodput provides a more realistic perspective by showing how much useful information is being transmitted, through rate.

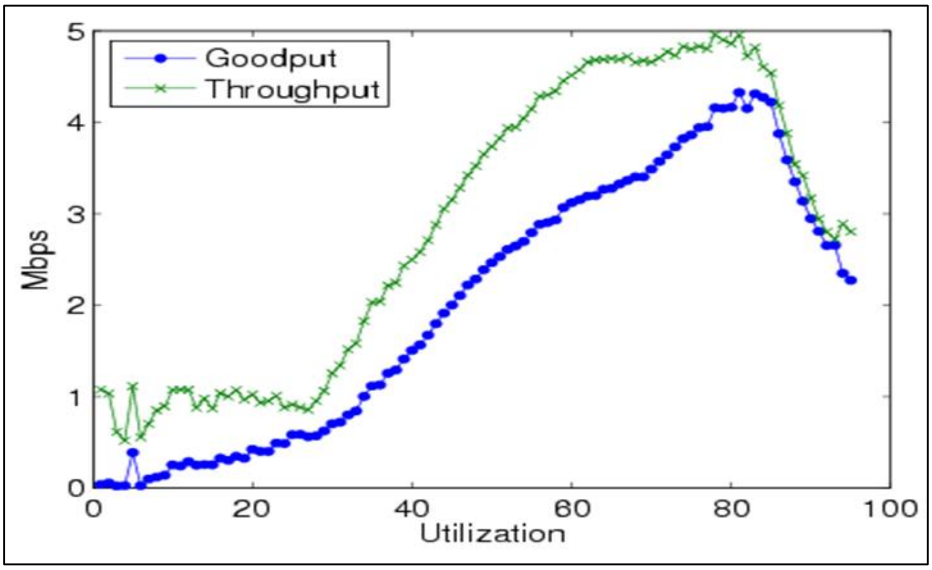

Figure 14 Network goodput

Performance issues in 4G networks can arise from various factors, impacting the quality of service and user experience. These issues include network congestion, which occurs when too many users access the network simultaneously, leading to slower data speeds and higher latency. Signal interference from physical obstacles, weather conditions, or electronic devices can degrade signal quality and reduce throughput. Additionally, the distance between users and cell towers affects signal strength and can cause connectivity problems. Table 3 presents some of the performance challenges in 4G networks. Other performance challenges include inadequate infrastructure, limited bandwidth, and the impact of mobility on handover efficiency between cell towers. Addressing these issues requires continuous optimization of network resources, deployment of advanced technologies, and investment in infrastructure upgrades to ensure consistent and reliable performance in 4G networks.

Table 3 Summary of performance issues in LTE networks

Performance issue	Description
Spectrum Scarcity	The radio frequency spectrum available for 4G LTE networks is limited, and as demand for mobile data grows, managing this limited resource becomes increasingly challenging [212]-[216]. Efficient spectrum allocation and usage are crucial to maintaining network performance [217] and avoiding congestion.
Interference Management	Interference from other devices, networks, and environmental factors can degrade LTE network performance [218]. [219]. Effective interference management techniques, such as advanced signal processing and interference coordination, are essential to maintain high-quality communication.
Latency Reduction	While 4G LTE has significantly reduced latency compared to previous generations, achieving ultra-low latency for real-time applications like gaming and video conferencing remains a challenge [220]. Continuous optimization of network protocols and infrastructure is needed to further reduce latency.
Backhaul Capacity	The backhaul network, which connects cell towers to the core network, must handle increasing data traffic. Insufficient backhaul capacity can create bottlenecks, leading to reduced data rates and higher latency [221]. Upgrading backhaul infrastructure to fiber or high-capacity wireless links is necessary.
Load Balancing	As user demand fluctuates across different cell towers and regions, load balancing is critical to ensure that network resources are utilized efficiently [222]. Ineffective load balancing can lead to some cells being overloaded while others are underutilized, degrading overall performance.
Handover Optimization	In mobile networks, users frequently move between cell coverage areas, requiring handovers from one cell tower to another [223]. Poorly managed handovers can result in dropped calls, interrupted data sessions, and degraded service quality [224]. Optimizing handover algorithms is essential to maintain seamless connectivity.
Network Congestion	High traffic volumes, especially during peak times or large events, can lead to network congestion [225]. Congestion management techniques, such as traffic prioritization and dynamic resource allocation, are needed to maintain service quality under heavy load conditions.
Quality of Service (QoS) Management	Ensuring consistent QoS for different types of applications (e.g., voice, video, and data) is a complex challenge [226]. Implementing effective QoS management strategies, including traffic shaping and prioritization, is crucial to meet diverse application requirements.
Coverage Gaps	Despite widespread LTE deployment, coverage gaps still exist in rural and remote areas, as well as inside buildings and underground locations [227]. Expanding coverage and improving indoor penetration through small cells and distributed antenna systems (DAS) can address these gaps.
Energy Efficiency	LTE networks consume significant power, particularly in densely populated areas with high data demand [228]. Improving energy efficiency [229] through techniques like sleep modes for base stations and optimizing power usage is important for reducing operational costs and environmental impact.
User Mobility	High-speed user mobility, such as users in cars or trains, poses challenges for maintaining stable and high-quality connections [230]. Developing advanced mobility management techniques to handle rapid cell transitions and varying signal conditions is essential for performance.

Carrier Aggregation	Carrier aggregation combines multiple frequency bands to increase data rates and capacity. However, managing multiple carriers introduces complexity in signal processing and resource allocation, which can impact performance if not handled effectively [231].
Device Diversity	The wide range of devices (smartphones, tablets, IoT devices) with varying capabilities and performance characteristics can strain the network. Ensuring compatibility and optimal performance for all device types requires extensive testing and network optimization [232].
Software Upgrades	Frequent software upgrades are needed to address security vulnerabilities, introduce new features, and improve performance. Managing these upgrades without disrupting service and ensuring backward compatibility is a continuous challenge [233].
Network Slicing	Implementing network slicing to create virtualized networks for different applications (e.g., IoT, emergency services) requires sophisticated orchestration and resource management. Ineffective slicing can lead to resource contention and degraded performance for critical services [234].
Security Overheads	Implementing robust security measures [235], such as encryption and authentication, introduces computational overhead that can impact performance. Balancing security and performance is crucial to ensure both secure and efficient network operations [236].
Inter-Cell Interference Coordination (ICIC)	In dense network deployments, interference between adjacent cells can degrade performance [237]. Advanced ICIC techniques are needed to mitigate this interference and optimize spectral efficiency, ensuring high data rates and reduced interference.
Real-Time Analytics	Real-time analytics are essential for monitoring network performance, identifying issues, and optimizing operations [238]. Implementing and maintaining these analytics systems requires substantial computational resources and can introduce latency if not optimized.
Scalability	As the number of connected devices and data traffic grows, the network must scale accordingly. Ensuring that the LTE infrastructure can handle increasing load without compromising performance requires continuous investment and optimization [239].
Network Virtualization	Virtualizing network functions to improve flexibility and efficiency introduces complexity in managing virtual resources. Ensuring that virtualized functions perform at par with traditional hardware-based solutions is critical to maintaining overall network performance [240].

In a nutshell, 4G LTE networks face a multitude of performance challenges that require ongoing innovation and optimization. From managing spectrum scarcity and interference to ensuring seamless handovers and improving energy efficiency, addressing these issues is essential for delivering high-quality mobile communication services. As technology evolves and user demand continues to grow, continuous efforts to enhance network performance will remain a top priority for mobile network operators and industry stakeholders.

6. Discussion

This section discusses solutions for Security issues, performance issues and privacy issues in 4G LTE Networks technologies.

6.1. Solutions for Security Issues In 4G LTE Networks

The solution to the security issues in this type of network, is that, in order to secure mobile devices that use 4G/LTE wireless technologies, there should be protection for the connections between the UEs and MMEs and between elements in the wireline networks and mobile stations. For satisfying these requirements, the 4G/LTE security is significantly improved by adding the following, advanced key hierarchy, the protracted authentication and key agreement [241], and the additional interworking security for the NEs. These requirements are classified into key building blocks and LTE end-to-end security [242], as explained, on the following elements, a unique and temporary UE identity when a UE is connected with a cell, LTE end-to-end security involves the following elements, Authentication and Key Agreement (AKA) The foundation of LTE security is authenticating the UEs and wireless networks. This can be accomplished using the AKA process which asserts that the serving network authenticates the identity of a user and the UE certifies the network signature. The AKA creates encryption and integrity keys applied for originating various session keys for ensuring the 4G/LTE security and privacy. Confidentiality and integrity of signaling Security of network access control planes is achieved when the RCC and NAS layer signaling is encrypted and integrity protected. Ciphering and integrity protection of LTE RRC signaling is executed at the packet data convergence protocol (PDCP) layer, whereas the NAS layer attains the protection by encrypting the NAS-level signaling. This protection cannot be uniquely performed for each UE connection, but it runs across trusted connections between AGW and eNodeB. User plane confidentiality LTE has a security feature for user plane via encrypting data/voice between the UE and eNodeB. Encryption is executed at the IP layer by utilizing IPsec-based tunnels between AGW and eNodeB, but no integrity protection is offered for the user plane due to performance and efficiency considerations. The PDCP layer is used for enabling encrypting/decrypting the user plane while transmitting traffic between the eNodeB and UE. Table 4 describes some of techniques for solving 4G network security issues.

Table 4 Solutions for Security Issues In 4G LTE Networks

Security solution	Description
Enhanced Encryption Protocols	Implementing strong and up-to-date encryption protocols is critical for securing data transmission in 4G LTE networks [243]. Advanced Encryption Standard (AES) and IPsec can be used to protect data at various layers of the network [244]. Regular updates and patches are essential to counteract evolving threats and vulnerabilities.
Mutual Authentication Mechanisms	Mutual authentication between devices and the network ensures that both parties verify each other's identities before establishing a connection [245]-[247]. This prevents unauthorized access and mitigates man-in-the-middle (MitM) attacks. Public Key Infrastructure (PKI) and digital certificates can be used to implement robust mutual authentication.
Intrusion Detection and Prevention Systems (IDPS)	Deploying IDPS can help monitor network traffic for suspicious activities and potential security breaches [248]. These systems can detect anomalies, identify known attack patterns, and automatically respond to threats, enhancing the overall security of the LTE network.
Secure Firmware Updates	Ensuring that devices and network elements receive secure firmware updates is crucial to maintaining security [249]. Over-the-air (OTA) updates should be encrypted and signed to prevent tampering and ensure that only authenticated updates are applied.
Enhanced Key Management	Effective key management practices, including the secure generation, distribution, and storage of cryptographic keys, are essential for maintaining the integrity of encryption protocols [250]-[253]. Using hardware security modules (HSMs) can provide an additional layer of security for key management.
Physical Security of Infrastructure	Protecting the physical infrastructure of LTE networks, including base stations, core network elements, and data centers, is vital [254]. Implementing physical security measures such as access controls, surveillance systems, and tamper-evident seals can help prevent physical attacks and unauthorized access.
Regular Security Audits and Penetration Testing	Conducting regular security audits and penetration testing helps identify vulnerabilities and weaknesses in the network [255]. These assessments should be performed by independent security experts and should cover all aspects of the LTE network, from infrastructure to protocols and applications.
Network Segmentation	Segregating the network into smaller, isolated segments can limit the spread of an attack and protect critical network components [256]. Implementing virtual LANs (VLANs) and using firewalls to control traffic between segments can enhance security and containment.
Advanced Threat Detection Techniques	Using advanced threat detection techniques such as machine learning and artificial intelligence can improve the ability to identify and respond to new and sophisticated attacks [257]. These technologies can analyze vast amounts of data in real time to detect anomalies and potential threats.
Strong Subscriber Authentication	Enhancing subscriber authentication methods, such as using two-factor authentication (2FA) and biometrics, can improve security [258], [259]. These methods provide an additional layer of protection against unauthorized access and impersonation attacks.

IMSI Encryption	Encrypting the International Mobile Subscriber Identity (IMSI) helps protect users' privacy and prevent tracking [260]. Temporary Mobile Subscriber Identities (TMSIs) can be used to periodically change the IMSI, making it harder for attackers to track users over time.
Secure Boot and Trusted Execution Environments (TEEs)	Implementing secure boot processes ensures that devices and network elements only run authenticated software [261]. Trusted Execution Environments (TEEs) provide a secure area within a device's processor to execute sensitive operations, protecting against malware and unauthorized access.
Robust Access Control Policies	Defining and enforcing robust access control policies helps ensure that only authorized personnel and devices can access network resources [262]. Role-based access control (RBAC) and multi-factor authentication (MFA) can be used to strengthen access controls.
Network Function Virtualization (NFV) Security	Securing virtualized network functions involves ensuring the integrity and isolation of virtual machines and containers [263]. Using secure hypervisors, applying security patches, and implementing micro-segmentation can help protect virtualized environments.
Base Station Authentication	Authenticating base stations to ensure they are legitimate and not rogue devices can prevent man-in-the-middle attacks and unauthorized access [264]. Public Key Infrastructure (PKI) and digital certificates can be used for base station authentication.
End-to-End Encryption	Implementing end-to-end encryption for sensitive data ensures that it remains secure throughout its journey from the sender to the recipient, even if intercepted [265]. This provides an additional layer of protection beyond network-level encryption.
Monitoring and Logging	Continuous monitoring and logging of network activities help in detecting and investigating security incidents [266]. Implementing centralized logging and monitoring solutions can provide real-time visibility into network operations and potential threats.
Jamming Detection and Mitigation	Detecting and mitigating jamming attacks involves using techniques such as spread spectrum and frequency hopping [267]. These methods can help avoid interference and maintain communication even in the presence of jamming attempts.
Rogue Device Detection	Deploying systems to detect and mitigate rogue devices, such as IMSI catchers and rogue base stations, helps protect user privacy and network integrity [268]. These systems can identify and isolate malicious devices to prevent them from compromising the network.
Education and Awareness Programs	Training network administrators, engineers, and end-users about security best practices and emerging threats is essential for maintaining a secure LTE network [269]. Regular education and awareness programs help ensure that all stakeholders are equipped to recognize and respond to security challenges.

Based on Table 3 above, it is clear that addressing security issues in 4G LTE networks requires a comprehensive approach that combines advanced technologies, robust policies, and continuous vigilance. From enhanced encryption and authentication mechanisms to regular security audits and user education, implementing these solutions can significantly improve the security posture of LTE networks. As threats continue to evolve, ongoing efforts to enhance and adapt security measures will be crucial in protecting these critical communication

6.2. Solutions for Privacy Issues in 4G LTE Network

The privacy issues have the solution, called the privacy-preserving authentication and encryption mechanisms have been widely used to protect wireless networks against the MITM attacks. Integrity attacks against integrity attempt to modify exchanging data between the 4G access points and mobile users. Cloning attacks based on the MITM [270] and message modification scenarios are the major integrity attacks that alter mobile user information. Authentication and privacy preserving mechanisms with hash functions have been broadly used for securing 4G wireless networks against integrity attacks [271]. Authentication attacks against authentication attempt to disturb the client-to-server and/or server-to-client authentication process. The password reuse, brute force, password stealing, and dictionary attacks are popular wireless hacking schemes that interrupt the password-based authentication. In the hacking schemes, an attacker can pretend to be a legal user and try to log in to a server by guessing various words as a password from a dictionary. Encryption and authentication techniques have been utilized for preventing such kind of attacks from 4G LTE Networks. Some of the methods for privacy preservation in 4G networks are described in Table 5.

Table 5 Solutions for Privacy Issues in 4G LTE Network

Privacy solution	**Description**
Enhanced Encryption for Data and Metadata	To protect both data and metadata from interception and analysis, 4G LTE networks should employ advanced encryption techniques [272]. Using end-to-end encryption ensures that only the intended recipients can access the data. Additionally, encrypting metadata, such as call logs and location information, can prevent unauthorized entities from inferring sensitive user details.
IMSI Privacy Protection	Protecting the IMSI (International Mobile Subscriber Identity) is crucial for preventing tracking and unauthorized surveillance. Implementing IMSI pseudonymization, where temporary identifiers are used instead of permanent IMSIs, can help protect user identities from being exposed to IMSI catchers and other tracking tools [273].
Secure Subscriber Identity Modules (SIMs)	Enhancing the security of SIM cards with robust encryption and tamper-resistant features can help protect the sensitive information they store [274]. Using secure elements and hardware-based security can prevent exploits like SIM swapping and SIMjacker attacks.
Improved Location Privacy	To protect users' location privacy, LTE networks can implement techniques like location obfuscation and the use of privacy zones [275]. By providing only the necessary level of location granularity to applications and services, users' precise locations can be kept private.
Network Slicing Isolation	Ensuring strict isolation between different network slices in a virtualized LTE environment can prevent data leakage and unauthorized access across slices [276]. Each slice can be configured with its own security policies and access controls to protect user data and maintain privacy.
Anonymization and Data Minimization	Applying anonymization techniques to user data before it is stored or processed can help protect privacy [277], [278]. Additionally, implementing data minimization principles—collecting only the data that is necessary for a specific purpose—can reduce the risk of privacy breaches.
Privacy-Respecting Data Retention Policies	Implementing strict data retention policies that limit the amount of time user data is stored can help protect privacy [279]. Ensuring that data is securely deleted after its retention period can prevent unauthorized access and misuse.
User Consent and Transparency	Providing users with clear information about how their data is collected, used, and shared, along with obtaining their explicit consent, can enhance privacy [280]. Transparency reports and privacy dashboards can help users understand and manage their data privacy preferences.
Secure OTA Updates	Ensuring that over-the-air (OTA) updates for mobile devices and network infrastructure are secure can prevent malicious updates and ensure the integrity of the system [281]. Using signed updates and secure distribution channels can protect against unauthorized modifications.
Privacy-Preserving Analytics	Implementing privacy-preserving techniques in analytics, such as differential privacy, can allow organizations to gain insights from data without compromising individual user privacy [282]. These techniques add noise to the data, ensuring that individual user information cannot be easily extracted.
Robust Access Control Mechanisms	Enforcing strict access control policies that limit who can access user data is critical for protecting privacy [283]. Role-based access control (RBAC) and fine-grained permissions can ensure that only authorized personnel can access sensitive information.
Regular Privacy Audits	Conducting regular privacy audits and assessments can help identify potential privacy risks and ensure compliance with privacy regulations [284]. These audits can evaluate the effectiveness of privacy measures and recommend improvements.

Advanced Intrusion Detection and Prevention	Deploying advanced intrusion detection and prevention systems (IDPS) that use machine learning and behavioral analysis can help detect and respond to privacy threats in real time [285]. These systems can identify unusual patterns that may indicate a privacy breach.
Edge Computing Privacy Measures	As edge computing becomes more prevalent in LTE networks, implementing strong privacy measures at the edge is crucial [286]. This includes encrypting data processed at edge nodes and ensuring that edge devices are secure from tampering.
Privacy-Enhanced Identity Management	Using advanced identity management solutions that support anonymous authentication and pseudonymous identities can help protect user privacy [287], [288]. These solutions allow users to authenticate without revealing their real identities.
Privacy by Design	Adopting a privacy-by-design approach ensures that privacy considerations are integrated into the design and development of network infrastructure and applications from the outset [289]. This proactive strategy helps identify and mitigate privacy risks early.
Privacy-Preserving IoT Devices	Ensuring that IoT devices connected to LTE networks have robust privacy protections is crucial [290]. This includes implementing secure communication protocols, encrypting data, and providing users with control over data collection and sharing.

Based on Table 4, it is evident that addressing privacy issues in 4G LTE networks requires a comprehensive approach that includes enhancing encryption, protecting user identities, ensuring data minimization, and implementing robust access controls. By adopting these solutions and continuously monitoring for new privacy threats, mobile network operators can protect user privacy and maintain the integrity of their services. Collaboration, education, and adherence to privacy regulations are key components in creating a privacy-respecting mobile communication environment.

6.3. Solutions for Performance Issues

The solution to the performance issues in 4G LTE wireless communication technologies are all carefully examined in this section based on important factors such data speeds, latency, spectral efficiency, and maximum device connectivity. Analyzing the potential and capabilities of any wireless technology requires a fundamental understanding of how these parameters change through generations. Data rates, which are commonly defined in gigabits per second (Gbps), are the rates at which data may be sent through a network. The maximum possible data rates, which are important determinants of the network's capability to effectively manage data traffic. The amount of time it takes for data to travel from its source to its destination is known as latency and is frequently expressed in milliseconds (ms). Lower latency values suggest quicker data transmission and reaction times, making it a significant aspect, especially for real-time applications. The delay drastically lowers with advancements in technology [292]. A very low latency of, for instance 0.1 ms is predicted for the 6G other technology, allowing for practically instantaneous data transfer. The quantity of spectrum efficiency, expressed in bits per hertz (bits/Hz), indicates how well the available spectrum is used for data transmission [293]. Increased network capacity results from improved spectral efficiency, which suggests that more data may be delivered within the specified frequency range. In comparison to 4G and 5G, the anticipated 6G technology is anticipated to achieve a considerable increase in spectral efficiency, suggesting improved spectrum utilization and data transmission efficiency [294]. Table 6 presents some of the key solutions to performance challenges in LTE networks.

Table 6 Solutions for Performance Issues

Performance solution	**Description**
Spectrum Management and Optimization	Efficiently managing the available spectrum is crucial to enhancing LTE network performance. Techniques such as dynamic spectrum sharing and spectrum refarming can optimize the use of existing frequencies [295]. Deploying new spectrum bands, including those in the millimeter-wave range, can also help accommodate growing data demands.
Carrier Aggregation	Carrier aggregation combines multiple frequency bands to increase data throughput and capacity [296]. By utilizing non-contiguous spectrum and aggregating carriers, networks can offer higher data rates and better service quality [297], especially in areas with high traffic demand.

Advanced Antenna Technologies	Implementing advanced antenna technologies like Multiple Input Multiple Output (MIMO) and beamforming can significantly improve network performance [298]. MIMO uses multiple antennas at both the transmitter and receiver to enhance signal quality and data rates, while beamforming focuses the signal in specific directions to reduce interference and increase coverage.
Small Cells and Heterogeneous Networks (HetNets)	Deploying small cells (e.g., femtocells, picocells) and integrating them into HetNets can enhance coverage and capacity in densely populated areas [299]. Small cells help offload traffic from macro cells, reduce congestion, and improve indoor coverage.
Network Slicing	Network slicing allows for the creation of multiple virtual networks on a single physical infrastructure, each optimized for different use cases and performance requirements [300]. This ensures that resources are allocated efficiently, improving overall network performance and enabling new services like IoT and critical communications.
Edge Computing	Edge computing reduces latency by processing data closer to the source, rather than in centralized data centers [301]. This can significantly improve the performance of latency-sensitive applications like augmented reality, real-time gaming, and autonomous vehicles.
Enhanced Interference Management	Advanced interference management techniques, such as Coordinated Multi-Point (CoMP) transmission and reception, can mitigate interference between cells [302]. These techniques involve coordinating transmissions from multiple base stations to improve signal quality and reduce performance degradation due to interference.
Dynamic Traffic Management	Implementing dynamic traffic management and Quality of Service (QoS) mechanisms ensures that network resources are allocated efficiently based on real-time demand [303]. Traffic prioritization, congestion control, and load balancing help maintain high service quality during peak usage times.
Self-Organizing Networks (SON)	SON technology enables automated configuration, optimization, and management of network resources [304]. This reduces the need for manual intervention, improves network performance, and enhances the user experience by dynamically adapting to changing conditions.
Upgraded Backhaul Infrastructure	Upgrading the backhaul network to support higher capacities is essential for maintaining LTE performance [305]. Utilizing fiber optics, microwave links, and other high-capacity backhaul solutions ensures that the increased traffic from enhanced access networks [306] can be effectively handled.
Software-Defined Networking (SDN) and Network Functions Virtualization (NFV)	SDN and NFV enable flexible and dynamic network management by decoupling network functions from hardware [307]. These technologies allow for on-demand resource allocation, rapid service deployment, and improved scalability, enhancing overall network performance.
Advanced Load Balancing	Implementing advanced load balancing algorithms ensures that traffic is evenly distributed across network resources [308]. This prevents congestion in high-traffic areas and ensures optimal utilization of available capacity, improving user experience.
Handover Optimization	Optimizing handover procedures reduces the likelihood of dropped calls and interrupted data sessions as users move between cells [309]. Techniques such as fast handover and seamless mobility management ensure continuous connectivity and improve user satisfaction.
Energy Efficiency Improvements	Improving energy efficiency in network infrastructure reduces operational costs and environmental impact [310]. Implementing energy-saving techniques, such as dynamic power management and sleep modes for base stations, helps maintain performance while reducing energy consumption.
Deployment of Massive MIMO	Massive MIMO involves using a large number of antennas at the base station to improve spectral efficiency and capacity [311]. By focusing multiple data streams on individual users, massive MIMO can significantly enhance network performance in terms of both coverage and throughput.

Latency Reduction Techniques	Implementing techniques to reduce latency, such as optimized protocol stacks and faster processing times, is crucial for applications requiring real-time communication [312]. Low-latency transmission and reception mechanisms ensure better performance for critical services.
High-Capacity Core Networks	Upgrading core network infrastructure to support higher data rates and increased traffic volumes is essential [313]. Implementing high-capacity switches, routers, and efficient data routing protocols [314] ensures that the core network can handle the demands of modern LTE services.
Distributed Antenna Systems (DAS)	DAS improves indoor coverage and capacity by distributing antenna signals throughout buildings and large venues [315]-[318]. This ensures that users experience consistent service quality even in areas where traditional cell towers struggle to provide coverage.
User-Centric Network Design	Designing networks with the user experience in mind ensures that performance improvements align with user needs [319]. User-centric design focuses on optimizing parameters like signal strength, data rates, and latency based on user behavior and requirements.

It is clear from Table 5 that tacking performance issues in 4G LTE networks requires a multi-faceted approach that includes advanced technologies, efficient resource management [320], and continuous optimization. By implementing these solutions, mobile network operators can enhance network capacity, reduce latency, improve coverage, and ensure a high-quality user experience. As the demand for mobile data continues to grow, ongoing innovation and investment in network infrastructure will be essential to meet future performance requirements.

7. Research gaps

On the research gap section, on this type of network, there is these trusted connections through 4G networks in the existence of eavesdroppers are the issues. Especially, when 4G wireless technology is used in the Internet of Things, it requires new cryptographic mechanisms that provide protection and integrity for smartphones and computer systems. Whereby, instead of individual security techniques, a systematic security and privacy protection strategies are required for 4G/LTE wireless connections while connecting with cloud and edge computing paradigms. This will provide valid security mechanisms, for example, trust models, device security, and data assurance techniques. This will be a good area of the future researchers on this issue. Some of the pertinent research gaps are described in Table 7 below.

Table 7 Research gaps

Gap	**Description**
Security gaps	
Advanced Persistent Threats (APTs)	Current defenses against APTs in 4G LTE networks are not fully developed. These sophisticated, long-term attacks require advanced detection and mitigation strategies. *Research Need:* Develop methods for early detection and response to APTs that can adapt to evolving attack strategies.
IoT Security	The rapid proliferation of IoT devices connected to LTE networks introduces new vulnerabilities and attack vectors. *Research Need:* Design comprehensive security frameworks for IoT devices that include secure boot processes, authentication, and communication protocols tailored for LTE networks.
AI-Driven Security Solutions	While AI and machine learning have potential, their application in LTE network security is still in nascent stages. *Research Need:* Explore and develop AI-driven intrusion detection and response systems that can adapt to new and sophisticated attack patterns.
Quantum-Resistant Security	The advent of quantum computing poses a future threat to current encryption algorithms.

	Research Need: Research and develop quantum-resistant cryptographic algorithms that can be implemented in LTE networks to ensure long-term security.
User Authentication	Existing user authentication methods may be vulnerable to attacks such as SIM swapping and phishing. *Research Need:* Develop multi-factor and biometric authentication methods that are more robust against such attacks.
Privacy gaps	
Privacy-Preserving Data Analytics	Techniques to perform data analytics while preserving user privacy are underdeveloped. *Research Need:* Develop and refine privacy-preserving data analytics methods, such as differential privacy and homomorphic encryption, for use in LTE networks.
Location Privacy	Protecting user location information remains a significant challenge. *Research Need:* Research methods to obfuscate location data and ensure that location-based services can function without compromising user privacy.
Identity Management	Current identity management systems can expose user identities to tracking and profiling. *Research Need:* Develop anonymous and pseudonymous identity management systems that provide privacy without sacrificing security or usability.
Data Minimization Techniques	LTE networks often collect more data than necessary for service provision, increasing privacy risks. *Research Need:* Research methods for data minimization that ensure only necessary data is collected and processed, reducing exposure of personal information.
Privacy Impact Assessments	Comprehensive frameworks for conducting privacy impact assessments in LTE networks are lacking. *Research Need:* Develop standardized methods for privacy impact assessments to identify and mitigate privacy risks associated with new technologies and services.
Performance gaps	
Latency Reduction	Current LTE networks still struggle with latency, especially for real-time applications. *Research Need:* Research novel techniques and protocols to reduce latency further, particularly for applications like AR/VR and autonomous vehicles.
Seamless Handover	Ensuring seamless handover between cells, especially in high-mobility scenarios, is challenging. *Research Need:* Investigate and develop improved handover mechanisms that ensure continuity and reliability of service for users on the move.
Energy Efficiency	Energy consumption in LTE networks remains high, particularly with the growing number of connected devices. *Research Need:* Develop energy-efficient algorithms and protocols that can reduce power consumption without compromising performance.
Network Slicing Optimization	Efficiently managing and optimizing network slices in a dynamic and scalable manner is not fully addressed. *Research Need:* Research advanced algorithms for dynamic resource allocation and optimization in network slicing to enhance performance.
Interference Mitigation	Interference, especially in densely populated areas, can significantly degrade network performance. *Research Need:* Develop advanced interference mitigation techniques, including enhanced ICIC (Inter-Cell Interference Coordination) and CoMP (Coordinated Multi-Point) strategies.

Based on the discussion above, it is clear that tacklingAddressing these research gaps requires a multidisciplinary approach, combining advances in cryptography, machine learning, network protocols, and data privacy. Collaborative efforts between academia, industry, and regulatory bodies are essential to develop robust solutions that ensure the security, privacy, and performance of 4G LTE networks continue to meet the growing demands and challenges of the digital age.

8. Future research scopes

Despite a plethora of research and technical studies that have been conducted for securing 4G/LTE wireless networks, there are several challenges that should be the focus of researchers in future that are discussed below. Designing a flexible and scalable 4G/LTE architecture that can address security and privacy issues is an arduous task. There are multiple devices and systems that are usually connected with 4G networks that result in vulnerabilities and loopholes in networks. Discovering DoS attacks that attempt to violate 4G wireless networks, as hackers frequently establish new sophisticated variants against eNodeB, UE, and discontinuous reception services. Location tracking denotes tracing the UE presence in a specific cell(s). While many portable devices could link to a 4G LTE wireless network, ensuring that location tracks of the devices are not breached is still a challenging issue, due to the considerations of operability and scalability. The utilization of an effective 4G wireless Software Denied Network (SDN) is a challenge. More specifically, there are technical gaps in the network scalability, security, and privacy issues with the SDN.

- *Advanced Security Mechanisms*: Future research in 4G LTE networks will focus on developing advanced security mechanisms to counteract increasingly sophisticated cyber threats. As cyber-attacks become more complex, leveraging AI and machine learning for real-time threat detection and response will be crucial. Research will also delve into quantum-resistant cryptography to prepare for the advent of quantum computing, which threatens current encryption methods. Moreover, securing the expanding Internet of Things (IoT) landscape within LTE networks will require comprehensive frameworks that ensure end-to-end security for a diverse range of connected devices.
- *Privacy-Enhancing Technologies*: Enhancing user privacy in 4G LTE networks remains a critical research area. Future work will likely concentrate on developing robust privacy-preserving data analytics techniques, such as differential privacy and homomorphic encryption, which allow data analysis without compromising individual privacy. Additionally, innovative identity management solutions that utilize pseudonyms or anonymous credentials can protect user identities from being tracked or profiled. Research will also focus on methods to obfuscate location data, ensuring that users can access location-based services without revealing their exact whereabouts.
- *Performance Optimization and Emerging Technologies*: Performance optimization continues to be a significant area for future research in 4G LTE networks. As the demand for higher data rates and lower latency grows, researchers will explore advanced techniques like dynamic spectrum sharing, carrier aggregation, and more efficient use of MIMO and beamforming technologies. The integration of edge computing to reduce latency for real-time applications and the development of more energy-efficient protocols will also be key areas of focus. Additionally, the rise of network slicing and its optimization will be critical for supporting diverse use cases and ensuring efficient resource allocation in increasingly complex network environments. These efforts will ensure that 4G LTE networks can continue to meet evolving user expectations and technological advancements.

9. Conclusions

The 4G LTE network technology has emerged as one of the networks which has enhanced a broadband performance and permitting different multimedia applications. The technology has been used for the Internet of Things (IoT) for connecting to Machine-to-Machine (M2M) systems and devices for instance in the In-Vehicle Multi-Carrier Router. The security, privacy, and performance of 4G LTE networks are pivotal to maintaining the efficacy and trustworthiness of mobile communications as we transition to more advanced technologies. This review has highlighted the critical security vulnerabilities within 4G LTE networks, such as the susceptibility to various cyber-attacks and the need for advanced encryption and authentication mechanisms. Addressing these issues requires ongoing research into robust security frameworks, including quantum-resistant cryptography and AI-driven threat detection systems. Privacy concerns in 4G LTE networks are equally pressing, with significant attention needed to safeguard user data and location information. Innovations in privacy-preserving technologies, such as differential privacy and secure identity management, are essential to mitigate risks associated with data collection and processing. Ensuring that privacy-enhancing measures are integrated into network operations and services will be crucial for maintaining user trust and regulatory compliance. Performance challenges in 4G LTE networks, including latency, interference, and capacity constraints, necessitate continuous optimization and the integration of emerging technologies. Future research should focus on enhancing network efficiency through advanced techniques like dynamic spectrum management, carrier aggregation, and edge computing. By addressing these key areas—security, privacy, and performance—4G LTE networks can be fortified to meet current demands and adapt to future advancements, ensuring a resilient and high-quality mobile communication infrastructure.

References

[1] Rodriguez I, Mogensen RS, Fink A, Raunholt T, Markussen S, Christensen PH, Berardinelli G, Mogensen P, Schou C, Madsen O. An experimental framework for 5G wireless system integration into industry 4.0 applications. Energies. 2021 Jul 23;14(15):4444.

[2] Narayanan A, Zhang X, Zhu R, Hassan A, Jin S, Zhu X, Zhang X, Rybkin D, Yang Z, Mao ZM, Qian F. A variegated look at 5G in the wild: performance, power, and QoE implications. InProceedings of the 2021 ACM SIGCOMM 2021 Conference 2021 Aug 9 (pp. 610-625).

[3] Subedi P, Alsadoon A, Prasad PW, Rehman S, Giweli N, Imran M, Arif S. Network slicing: A next generation 5G perspective. EURASIP Journal on Wireless Communications and Networking. 2021 Apr 23;2021(1):102.

[4] Wu TY, Lee Z, Obaidat MS, Kumari S, Kumar S, Chen CM. An authenticated key exchange protocol for multi-server architecture in 5G networks. IEEE Access. 2020 Jan 28;8:28096-108.

[5] Fang K, Yan G. Paging storm attacks against 4G/LTE networks from regional Android botnets: rationale, practicality, and implications. InProceedings of the 13th ACM Conference on Security and Privacy in Wireless and Mobile Networks 2020 Jul 8 (pp. 295-305).

[6] Oueis J, Conan V, Lavaux D, Stanica R, Valois F. Overview of LTE isolated E-UTRAN operation for public safety. IEEE Communications Standards Magazine. 2017 Jul 26;1(2):98-105.

[7] Al Sibahee MA, Abduljabbar ZA, Ngueilbaye A, Luo C, Li J, Huang Y, Zhang J, Khan N, Nyangaresi VO, Ali AH. Blockchain-Based Authentication Schemes in Smart Environments: A Systematic Literature Review. IEEE Internet of Things Journal. 2024 Jul 3.

[8] Yu C, Chen S, Wang F, Wei Z. Improving 4G/5G air interface security: A survey of existing attacks on different LTE layers. Computer Networks. 2021 Dec 24;201:108532.

[9] Cui Q, Shi Y, Tao X, Zhang P, Liu RP, Chen N, Hamalainen J, Dowhuszko A. A unified protocol stack solution for LTE and WLAN in future mobile converged networks. IEEE wireless communications. 2014 Dec;21(6):24-33.

[10] Bibi MJ, Kumar NC. Critical review of network architecture, mobile network evolution, standardization, LTE evolution and future evolution of 5G. IJECS. 2024;6(1):30-9.

[11] Moustafa N, Hu J. Security and Privacy in 4G/LTE Network. InEncyclopedia of Wireless Networks 2020 Aug 30 (pp. 1265-1271). Cham: Springer International Publishing.

[12] Mohapatra SK, Swain BR, Das P. Comprehensive survey of possible security issues on 4G networks. International Journal of Network Security & Its Applications. 2015 Mar 1;7(2):61.

[13] Sharma DA. 4g wireless technology and its standards taking consideration evolution of 4g technology. National Journal of Multidisciplinary Research and Development. 2018;3(1):1102-5.

[14] Nyangaresi VO, Al-Joboury IM, Al-sharhanee KA, Najim AH, Abbas AH, Hariz HM. A Biometric and Physically Unclonable Function-Based Authentication Protocol for Payload Exchanges in Internet of Drones. e-Prime-Advances in Electrical Engineering, Electronics and Energy. 2024 Feb 23:100471.

[15] Kareem KM. The Impact of IMSI Catcher Deployments on Cellular Network Security: Challenges and Countermeasures in 4G and 5G Networks. arXiv preprint arXiv:2405.00793. 2024 May 1.

[16] Fang D, Qian Y, Hu RQ. 5G Wireless Network Security and Privacy. John Wiley & Sons; 2023 Nov 2.

[17] Khan R, Kumar P, Jayakody DN, Liyanage M. A Survey on Security and Privacy of 5G Technologies: Potential Solutions, Recent Advancements. Khan, Rabia, Pardeep Kumar, Dushantha Nalin K. Jayakody, and Madhusanka Liyanage."A Survey on Security and Privacy of 5G Technologies: Potential Solutions, Recent Advancements and Future Directions" 22. 2019(1).

[18] Pandey D, Goyal S, Bhaumik K, Suneja S, Sharma M, Dadheech PD. A Systematic Review of Security Issues in 6G Networks and Communication. Security Issues and Solutions in 6G Communications and Beyond. 2024:1-1.

[19] Reshmi TR, Abhishek K. 5G and 6G Security Issues and Countermeasures. InSecure Communication in Internet of Things 2024 (pp. 300-310). CRC Press.

[20] Ali ZA, Abduljabbar ZA, AL-Asadi HA, Nyangaresi VO, Abduljaleel IQ, Aldarwish AJ. A Provably Secure Anonymous Authentication Protocol for Consumer and Service Provider Information Transmissions in Smart Grids. Cryptography. 2024 May 9;8(2):20.

[21] Qasem A, Tahat A. Machine learning-based detection of the man-in-the-middle attack in the physical layer of 5G networks. Simulation Modelling Practice and Theory. 2024 Jul 15:102998.

[22] Ma M, Cui B. Research and Implementation of TFTP Encrypted Traffic Analysis and Attack Technology Based on 4G Man-in-the-Middle. InInternational Conference on Emerging Internet, Data & Web Technologies 2024 Feb 14 (pp. 394-403). Cham: Springer Nature Switzerland.

[23] Chen Z, Cui B, Cheng Z. 4G Access Network Protection and Compliance Detection Based on Man-in-the-Middle Model. InInternational Conference on Emerging Internet, Data & Web Technologies 2024 Feb 14 (pp. 404-414). Cham: Springer Nature Switzerland.

[24] Wani MS, Rademacher M, Horstmann T, Kretschmer M. Security vulnerabilities in 5G non-stand-alone networks: A systematic analysis and attack taxonomy. Journal of Cybersecurity and Privacy. 2024 Jan 2;4(1):23-40.

[25] Iavich M. The Hybrid Detection Methodology of Attacks for 5G. InInternational Conference on Artificial Intelligence and Power Engineering 2021 Dec 17 (pp. 65-74). Cham: Springer International Publishing.

[26] Nyangaresi VO. Extended Chebyshev Chaotic Map Based Message Verification Protocol for Wireless Surveillance Systems. InComputer Vision and Robotics: Proceedings of CVR 2022 2023 Apr 28 (pp. 503-516). Singapore: Springer Nature Singapore.

[27] Hamici-Aubert V, Saint-Martin J, Navas RE, Papadopoulos GZ, Doyen G, Lagrange X. Leveraging Overshadowing for Time-Delay Attacks in 4G/5G Cellular Networks: An Empirical Assessment. InThe 19th International Conference on Availability, Reliability and Security (ARES 2024) 2024 Jul 30.

[28] Savadatti S, Kuldeep Dhariwal S, Krishnamoorthy S, Delhibabu R. An Extensive Classification of 5G Network Jamming Attacks. Security and Communication Networks. 2024;2024(1):2883082.

[29] Jover RP, Lackey J, Raghavan A. Enhancing the security of LTE networks against jamming attacks. EURASIP Journal on Information Security. 2014 Dec;2014:1-4.

[30] Vachhani K. Security threats against LTE networks: A survey. InSecurity in Computing and Communications: 6th International Symposium, SSCC 2018, Bangalore, India, September 19–22, 2018, Revised Selected Papers 6 2019 (pp. 242-256). Springer Singapore.

[31] Escudero-Andreu G, Kyriakopoulos K, Flint JA, Lambotharan S. Detecting signalling DoS attacks on LTE networks. InInternational Conference on Industrial Networks and Intelligent Systems 2019 Aug 17 (pp. 283-301). Cham: Springer International Publishing.

[32] Bulbul SS, Abduljabbar ZA, Mohammed RJ, Al Sibahee MA, Ma J, Nyangaresi VO, Abduljaleel IQ. A provably lightweight and secure DSSE scheme, with a constant storage cost for a smart device client. Plos one. 2024 Apr 25;19(4):e0301277.

[33] Wen YT, Wu SH, Chen CY, Hsu YY, Wang PH, Hsu SM, Chang CY, Kung BC. Real-Time Rogue Base Stations Detection System in Cellular Networks. InInternational Conference on Advanced Information Networking and Applications 2024 Apr 10 (pp. 465-474). Cham: Springer Nature Switzerland.

[34] Saedi M, Moore A, Perry P. Synthetic generation of realistic signal strength data to enable 5g rogue base station investigation in vehicular platooning. Applied Sciences. 2022 Dec 7;12(24):12516.

[35] Mubasshir KS, Karim I, Bertino E. FBSDetector: Fake Base Station and Multi Step Attack Detection in Cellular Networks using Machine Learning. arXiv preprint arXiv:2401.04958. 2024 Jan 10.

[36] Liu IH, Lee MH, Huang HC, Li JS. 5G-Based Smart Healthcare and Mobile Network Security: Combating Fake Base Stations. Applied Sciences. 2023 Oct 23;13(20):11565.

[37] Ludant N, Vomvas M, Noubir G. Unprotected 4G/5G Control Procedures at Low Layers Considered Dangerous. arXiv preprint arXiv:2403.06717. 2024 Mar 11.

[38] Nyangaresi VO. Provably secure authentication protocol for traffic exchanges in unmanned aerial vehicles. High-Confidence Computing. 2023 Sep 15:100154.

[39] Francois F, Abdelrahman OH, Gelenbe E. Towards assessment of energy consumption and latency of LTE UEs during signaling storms. InInformation Sciences and Systems 2015: 30th International Symposium on Computer and Information Sciences (ISCIS 2015) 2016 (pp. 45-55). Springer International Publishing.

[40] Asmare FM, Ayalew LG. Security challenges in the transition to 4G mobile systems in developing countries. Cogent Engineering. 2023 Dec 31;10(1):2166214.

[41] Alshouiliy K, Agrawal DP. Confluence of 4G LTE, 5G, fog, and cloud computing and understanding security issues. Fog/Edge Computing For Security, Privacy, and Applications. 2021:3-2.

[42] Francois F, Abdelrahman OH, Gelenbe E. Feasibility of signaling storms in 3G/UMTS operational networks. InInternet of Things. IoT Infrastructures: Second International Summit, IoT 360° 2015, Rome, Italy, October 27–29, 2015, Revised Selected Papers, Part I 2016 (pp. 187-198). Springer International Publishing.

[43] Fei T, Wang W. The vulnerability and enhancement of AKA protocol for mobile authentication in LTE/5G networks. Computer Networks. 2023 Jun 1;228:109685.

[44] Mutlaq KA, Nyangaresi VO, Omar MA, Abduljabbar ZA, Abduljaleel IQ, Ma J, Al Sibahee MA. Low complexity smart grid security protocol based on elliptic curve cryptography, biometrics and hamming distance. Plos one. 2024 Jan 23;19(1):e0296781.

[45] Cui Z, Cui B, Su L, Du H, Wang H, Fu J. Attacks against security context in 5g network. InInternational Symposium on Mobile Internet Security 2022 Dec 15 (pp. 3-17). Singapore: Springer Nature Singapore.

[46] Scalise P, Boeding M, Hempel M, Sharif H, Delloiacovo J, Reed J. A Systematic Survey on 5G and 6G Security Considerations, Challenges, Trends, and Research Areas. Future Internet. 2024 Feb 20;16(3):67.

[47] Rupprecht D, Kohls K, Holz T, Pöpper C. Breaking LTE on layer two. In2019 IEEE Symposium on Security and Privacy (SP) 2019 May 19 (pp. 1121-1136). IEEE.

[48] Ghannam R, Sharevski F, Chung A. User-targeted denial-of-service attacks in LTE mobile networks. In2018 14th International conference on wireless and mobile computing, networking and communications (WiMob) 2018 Oct 15 (pp. 1-8). IEEE.

[49] Kim H, Lee J, Lee E, Kim Y. Touching the untouchables: Dynamic security analysis of the LTE control plane. In2019 IEEE Symposium on Security and Privacy (SP) 2019 May 19 (pp. 1153-1168). IEEE.

[50] Nyangaresi VO. Target Tracking Area Selection and Handover Security in Cellular Networks: A Machine Learning Approach. InProceedings of Third International Conference on Sustainable Expert Systems: ICSES 2022 2023 Feb 23 (pp. 797-816). Singapore: Springer Nature Singapore.

[51] Karakoc B, Fürste N, Rupprecht D, Kohls K. Never let me down again: Bidding-down attacks and mitigations in 5g and 4g. InProceedings of the 16th ACM Conference on Security and Privacy in Wireless and Mobile Networks 2023 May 29 (pp. 97-108).

[52] Shaik A, Borgaonkar R, Asokan N, Niemi V, Seifert JP. Practical attacks against privacy and availability in 4G/LTE mobile communication systems. arXiv preprint arXiv:1510.07563. 2015 Oct 26.

[53] Hussain S, Chowdhury O, Mehnaz S, Bertino E. LTEInspector: A systematic approach for adversarial testing of 4G LTE. InNetwork and Distributed Systems Security (NDSS) Symposium 2018 2018 Feb.

[54] Tu GH, Li CY, Peng C, Lu S. How voice call technology poses security threats in 4G LTE networks. In2015 IEEE conference on communications and network security (CNS) 2015 Sep 28 (pp. 442-450). IEEE.

[55] Shaik A, Borgaonkar R, Park S, Seifert JP. New vulnerabilities in 4G and 5G cellular access network protocols: exposing device capabilities. InProceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks 2019 May 15 (pp. 221-231).

[56] Al Sibahee MA, Abduljabbar ZA, Luo C, Zhang J, Huang Y, Abduljaleel IQ, Ma J, Nyangaresi VO. Hiding scrambled text messages in speech signals using a lightweight hyperchaotic map and conditional LSB mechanism. Plos one. 2024 Jan 3;19(1):e0296469.

[57] Lee G, Lee J, Lee J, Im Y, Hollingsworth M, Wustrow E, Grunwald D, Ha S. This is your president speaking: Spoofing alerts in 4G LTE networks. InProceedings of the 17th Annual International Conference on Mobile Systems, Applications, and Services 2019 Jun 12 (pp. 404-416).

[58] Fei T, Wang W. Lte is vulnerable: Implementing identity spoofing and denial-of-service attacks in lte networks. In2019 IEEE Global Communications Conference (GLOBECOM) 2019 Dec 9 (pp. 1-6). IEEE.

[59] Tu GH, Li CY, Peng C, Li Y, Lu S. New security threats caused by IMS-based SMS service in 4G LTE networks. InProceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security 2016 Oct 24 (pp. 1118-1130).

[60] Shaik A, Borgaonkar R, Park S, Seifert JP. On the impact of rogue base stations in 4g/lte self organizing networks. InProceedings of the 11th ACM Conference on Security & Privacy in Wireless and Mobile Networks 2018 Jun 18 (pp. 75-86).

[61] Zheng Y, Huang L, Shan H, Li J, Yang Q, Xu W. Ghost telephonist impersonates you: Vulnerability in 4G LTE CS fallback. In2017 IEEE Conference on Communications and Network Security (CNS) 2017 Oct 9 (pp. 1-9). IEEE.

[62] Nyangaresi VO, Moundounga AR. Secure data exchange scheme for smart grids. In2021 IEEE 6th International Forum on Research and Technology for Society and Industry (RTSI) 2021 Sep 6 (pp. 312-316). IEEE.

[63] Palamà I, Gringoli F, Bianchi G, Blefari-Melazzi N. IMSI Catchers in the wild: A real world 4G/5G assessment. Computer Networks. 2021 Jul 20;194:108137.

[64] Fraunholz D, Brunke D, Beidenhauser S, Berger S, Koenig H, Reti D. IMSI probing: Possibilities and limitations. InNordic Conference on Secure IT Systems 2022 Nov 30 (pp. 80-97). Cham: Springer International Publishing.

[65] Yazhinian S, Kathirvel N, Devarasu N, Sankar M. Security Enhancement for the 5G Network Concerns. In2023 International Conference on System, Computation, Automation and Networking (ICSCAN) 2023 Nov 17 (pp. 1-5). IEEE.

[66] de Carvalho Macedo LO, Campista ME. Attacks to mobile networks using SS7 vulnerabilities: a real traffic analysis. Telecommunication Systems. 2023 Jul;83(3):253-65.

[67] Singh PP, Borisagar K. Paging vulnerabilities in 5G new radio networks and mitigation to enhance security performance. In2022 IEEE World Conference on Applied Intelligence and Computing (AIC) 2022 Jun 17 (pp. 914-918). IEEE.

[68] Omollo VN, Musyoki S. Blue bugging Java Enabled Phones via Bluetooth Protocol Stack Flaws. International Journal of Computer and Communication System Engineering. 2015 Jun 9, 2 (4):608-613.

[69] Mimran D, Bitton R, Kfir Y, Klevansky E, Brodt O, Lehmann H, Elovici Y, Shabtai A. Security of open radio access networks. Computers & Security. 2022 Nov 1;122:102890.

[70] Agarwal B, Togou MA, Marco M, Muntean GM. A comprehensive survey on radio resource management in 5G HetNets: Current solutions, future trends and open issues. IEEE Communications Surveys & Tutorials. 2022 Sep 20;24(4):2495-534.

[71] Garbelini ME, Shang Z, Chattopadhyay S, Sun S, Kurniawan E. Towards automated fuzzing of 4g/5g protocol implementations over the air. InGLOBECOM 2022-2022 IEEE Global Communications Conference 2022 Dec 4 (pp. 86-92). IEEE.

[72] Liyanage M, Braeken A, Shahabuddin S, Ranaweera P. Open RAN security: Challenges and opportunities. Journal of Network and Computer Applications. 2023 May 1;214:103621.

[73] Nyangaresi VO. Masked Symmetric Key Encrypted Verification Codes for Secure Authentication in Smart Grid Networks. In2022 4th Global Power, Energy and Communication Conference (GPECOM) 2022 Jun 14 (pp. 427-432). IEEE.

[74] Abdelrazek L, Fuladi R, Kövér J, Karaçay L, Gülen U. Detecting IP DDoS Attacks Using 3GPP Radio Protocols. IEEE Access. 2024 Feb 14;12:24776-90.

[75] Gokul N, Sankaran S. Modeling and defending against resource depletion attacks in 5g networks. In2021 IEEE 18th India Council International Conference (INDICON) 2021 Dec 19 (pp. 1-7). IEEE.

[76] De Alwis C, Porambage P, Dev K, Gadekallu TR, Liyanage M. A Survey on Network Slicing Security: Attacks, Challenges, Solutions and Research Directions. IEEE Communications Surveys & Tutorials. 2023 Sep 6.

[77] Sagar D, Saidi Reddy M. A brief review on security issues and counter measure techniques for future generation communication system (LTE/LTE-A). Multimedia Tools and Applications. 2024 Feb;83(7):19327-68.

[78] Oğul M, Baktır S. Practical attacks on mobile cellular networks and possible countermeasures. Future Internet. 2013 Sep 30;5(4):474-89.

[79] Rashed AN, Ahammad SH, Daher MG, Sorathiya V, Siddique A, Asaduzzaman S, Rehana H, Dutta N, Patel SK, Nyangaresi VO, Jibon RH. Spatial single mode laser source interaction with measured pulse based parabolic index multimode fiber. Journal of Optical Communications. 2022 Jun 21.

[80] Son BD, Hoa NT, Van Chien T, Khalid W, Ferrag MA, Choi W, Debbah M. Adversarial Attacks and Defenses in 6G Network-Assisted IoT Systems. IEEE Internet of Things Journal. 2024 Mar 6.

[81] Cibin N, Guerar M, Merlo A, Migliardi M, Verderame L. Towards a SIP-based DDoS Attack to the 4G Network. InWeb, Artificial Intelligence and Network Applications: Proceedings of the Workshops of the 34th International Conference on Advanced Information Networking and Applications (WAINA-2020) 2020 (pp. 857-866). Springer International Publishing.

[82] Lu YH, Li CY, Li YY, Hsiao SH, Xie T, Tu GH, Chen WX. Ghost calls from operational 4G call systems: IMS vulnerability, call DoS attack, and countermeasure. InProceedings of the 26th Annual International Conference on Mobile Computing and Networking 2020 Apr 16 (pp. 1-14).

[83] Gao K, Wang H, Lv H. Surgical Strike on 5G Positioning: Selective-PRS-Spoofing Attacks and Its Defence. IEEE Journal on Selected Areas in Communications. 2024 Jun 14.

[84] Savadatti S, Dhariwal SK, Krishnamoorthy S, Delhibabu R. A Comprehensive Taxonomy of Jamming Attacks on 5G Networks. InConference Proceedings: Encryptcon-An International Research Conference on CyberSecurity 2024 Apr 1 (p. 25). Shashwat Publication.

[85] Nyangaresi VO, Morsy MA. Towards privacy preservation in internet of drones. In2021 IEEE 6th International Forum on Research and Technology for Society and Industry (RTSI) 2021 Sep 6 (pp. 306-311). IEEE.

[86] Basheer S, Kumar G, Nalband AH, Raveendran C. Securing 5G Networks: Strategies for Prevention, Detection, and Mitigation of Rogue Base Stations. In2023 Fourth International Conference on Smart Technologies in Computing, Electrical and Electronics (ICSTCEE) 2023 Dec 8 (pp. 1-7). IEEE.

[87] Cheng SM, Hong BK, Hung CF. Attack detection and mitigation in MEC-enabled 5G networks for AIoT. IEEE Internet of Things Magazine. 2022 Sep;5(3):76-81.

[88] Hoque N, Rahbari H. Countering relay and spoofing attacks in the connection establishment phase of Wi-Fi systems. InProceedings of the 16th ACM Conference on Security and Privacy in Wireless and Mobile Networks 2023 May 29 (pp. 275-285).

[89] Sethi R, Kadam A, Prabhu K, Kota N. Security considerations to enable time-sensitive networking over 5g. IEEE Open Journal of Vehicular Technology. 2022 Sep 8;3:399-407.

[90] Alhoraibi L, Alghazzawi D, Alhebshi R, Rabie OB. Physical layer authentication in wireless networks-based machine learning approaches. Sensors. 2023 Feb 6;23(4):1814.

[91] Ahmad AY, Verma N, Sarhan N, Awwad EM, Arora A, Nyangaresi VO. An IoT and Blockchain-Based Secure and Transparent Supply Chain Management Framework in Smart Cities Using Optimal Queue Model. IEEE Access. 2024 Mar 18.

[92] Bikos AN, Sklavos N. LTE/SAE security issues on 4G wireless networks. IEEE Security & Privacy. 2012 Oct 22;11(2):55-62.

[93] Mathi S, Dharuman L. Prevention of desynchronization attack in 4G LTE networks using double authentication scheme. Procedia Computer Science. 2016 Jan 1;89:170-9.

[94] Hussain SR, Echeverria M, Chowdhury O, Li N, Bertino E. Privacy attacks to the 4G and 5G cellular paging protocols using side channel information. Network and distributed systems security (NDSS) symposium2019. 2019 Jan.

[95] Jover RP. Security attacks against the availability of LTE mobility networks: Overview and research directions. In2013 16th international symposium on wireless personal multimedia communications (WPMC) 2013 Jun 24 (pp. 1-9). IEEE.

[96] Wu S, Yeoh PL, Hardjawana W, Vucetic B. Identifying security and privacy vulnerabilities in 4g lte and iot communications networks. In2021 IEEE 7th World Forum on Internet of Things (WF-IoT) 2021 Jun 14 (pp. 512-517). IEEE.

[97] Nyangaresi VO. Privacy Preserving Three-factor Authentication Protocol for Secure Message Forwarding in Wireless Body Area Networks. Ad Hoc Networks. 2023 Apr 1;142:103117.

[98] Erni S, Kotuliak M, Leu P, Roeschlin M, Capkun S. AdaptOver: adaptive overshadowing attacks in cellular networks. InProceedings of the 28th Annual International Conference on Mobile Computing And Networking 2022 Oct 14 (pp. 743-755).

[99] Seyi AB, Jafaar F, Ruhl R. Securing the authentication process of LTE base stations. In2020 International Conference on Electrical, Communication, and Computer Engineering (ICECCE) 2020 Jun 12 (pp. 1-6). IEEE.

[100] Yu C, Chen S. On effects of mobility management signalling based dos attacks against lte terminals. In2019 IEEE 38th International Performance Computing and Communications Conference (IPCCC) 2019 Oct 29 (pp. 1-8). IEEE.

[101] Grassi M, Chen X. Over the air baseband exploit: Gaining remote code execution on 5g smartphones. BlackHat USA 2021. 2021 Aug.

[102] Kim H. 5G core network security issues and attack classification from network protocol perspective. J. Internet Serv. Inf. Secur.. 2020 May;10(2):1-5.

[103] Al-Chaab W, Abduljabbar ZA, Abood EW, Nyangaresi VO, Mohammed HM, Ma J. Secure and Low-Complexity Medical Image Exchange Based on Compressive Sensing and LSB Audio Steganography. Informatica. 2023 May 31;47(6).

[104] Ferrag MA, Maglaras L, Argyriou A, Kosmanos D, Janicke H. Security for 4G and 5G cellular networks: A survey of existing authentication and privacy-preserving schemes. Journal of Network and Computer Applications. 2018 Jan 1;101:55-82.

[105] Behrad S, Bertin E, Crespi N. A survey on authentication and access control for mobile networks: from 4G to 5G. Annals of Telecommunications. 2019 Oct;74:593-603.

[106] Panda PK, Chattopadhyay S. An improved authentication and security scheme for LTE/LTE-A networks. Journal of Ambient Intelligence and Humanized Computing. 2020 May;11:2163-85.

[107] Alezabi KA, Hashim F, Hashim SJ, Ali BM, Jamalipour A. Efficient authentication and re-authentication protocols for 4G/5G heterogeneous networks. EURASIP Journal on Wireless Communications and Networking. 2020 Dec;2020:1-34.

[108] Fraunholz D, Schörghofer-Vrinssen R, König H, Zahoransky R. Show me your attach request and i'll tell you who you are: Practical fingerprinting attacks in 4g and 5g mobile networks. In2022 IEEE Conference on Dependable and Secure Computing (DSC) 2022 Jun 22 (pp. 1-8). IEEE.

[109] Nyangaresi VO. A Formally Verified Authentication Scheme for mmWave Heterogeneous Networks. Inthe 6th International Conference on Combinatorics, Cryptography, Computer Science and Computation (605-612) 2021.

[110] Thantharate A, Paropkari R, Walunj V, Beard C, Kankariya P. Secure5G: A deep learning framework towards a secure network slicing in 5G and beyond. In2020 10th annual computing and communication workshop and conference (CCWC) 2020 Jan 6 (pp. 0852-0857). IEEE.

[111] Dangi R, Jadhav A, Choudhary G, Dragoni N, Mishra MK, Lalwani P. Ml-based 5g network slicing security: A comprehensive survey. Future Internet. 2022 Apr 8;14(4):116.

[112] Wijethilaka S, Liyanage M. Survey on network slicing for Internet of Things realization in 5G networks. IEEE Communications Surveys & Tutorials. 2021 Mar 22;23(2):957-94.

[113] Botez R, Costa-Requena J, Ivanciu IA, Strautiu V, Dobrota V. SDN-based network slicing mechanism for a scalable 4G/5G core network: A kubernetes approach. Sensors. 2021 May 29;21(11):3773.

[114] Mohammed MJ, Ghazi A, Awad AM, Hassan SI, Jawad HM, Jasim KM, Nurmamatovna MA. A Comparison of 4G LTE and 5G Network Cybersecurity Performance. In2024 35th Conference of Open Innovations Association (FRUCT) 2024 Apr 24 (pp. 452-464). IEEE.

[115] Al Sibahee MA, Nyangaresi VO, Abduljabbar ZA, Luo C, Zhang J, Ma J. Two-Factor Privacy Preserving Protocol for Efficient Authentication in Internet of Vehicles Networks. IEEE Internet of Things Journal. 2023 Dec 7.

[116] Shakir Z, Mjhool AY, Al-Thaedan A, Al-Sabbagh A, Alsabah R. Key performance indicators analysis for 4 G-LTE cellular networks based on real measurements. International Journal of Information Technology. 2023 Mar;15(3):1347-55.

[117] Isabona J, Imoize AL, Ojo S, Venkatareddy P, Hinga SK, Sánchez-Chero M, Ancca SM. Accurate base station placement in 4G LTE networks using multiobjective genetic algorithm optimization. Wireless Communications and Mobile Computing. 2023;2023(1):7476736.

[118] Mahmood F. Smart Autonomous Location Tracking & HeAlth Monitoring of War Fighters Using NB-IoT/LTE-M with SATCOM. In2023 IEEE Future Networks World Forum (FNWF) 2023 Nov 13 (pp. 1-6). IEEE.

[119] Liu Z, Chen L, Zhou X, Shen N, Chen R. Multipath tracking with LTE signals for accurate TOA estimation in the application of indoor positioning. Geo-spatial Information Science. 2023 Jan 2;26(1):31-43.

[120] Iavich M, Akhalaia G, Bocu R. Device Tracking Threats in 5G Network. InInternational Conference on Advanced Information Networking and Applications 2023 Mar 15 (pp. 480-489). Cham: Springer International Publishing.

[121] Nyangaresi VO, Petrovic N. Efficient PUF based authentication protocol for internet of drones. In2021 International Telecommunications Conference (ITC-Egypt) 2021 Jul 13 (pp. 1-4). IEEE.

[122] Cook J, Rehman SU, Khan MA. Security and privacy for low power iot devices on 5g and beyond networks: Challenges and future directions. IEEE Access. 2023 Apr 18;11:39295-317.

[123] Malik A, Parihar V, Bhushan B, Chaganti R, Bhatia S, Astya PN. Security Services for Wireless 5G Internet of Things (IoT) Systems. In5G and Beyond 2023 Aug 30 (pp. 169-195). Singapore: Springer Nature Singapore.

[124] Khan SA, Chowdhury MM, Nandy U. LTE/LTE-A Based Advanced Wireless Networks. Journal of Engineering Research and Reports. 2023 Nov 2;25(10):195-9.

[125] Serôdio C, Cunha J, Candela G, Rodriguez S, Sousa XR, Branco F. The 6G ecosystem as support for IoE and private networks: Vision, requirements, and challenges. Future Internet. 2023 Oct 25;15(11):348.

[126] Singh P, Kumar P, Sivaraman A. Review of the Security Risks and Practical Concerns with Current and Future (6G) Communications Technology. InInternational Workshop on New Approaches for Multidimensional Signal Processing 2023 Jul 6 (pp. 145-158). Singapore: Springer Nature Singapore.

[127] Umran SM, Lu S, Abduljabbar ZA, Nyangaresi VO. Multi-chain blockchain based secure data-sharing framework for industrial IoTs smart devices in petroleum industry. Internet of Things. 2023 Dec 1;24:100969.

[128] Gorrepati U, Zavarsky P, Ruhl R. Privacy protection in LTE and 5G networks. In2021 2nd International Conference on Secure Cyber Computing and Communications (ICSCCC) 2021 May 21 (pp. 382-387). IEEE.

[129] Settembre M. A 5G core network challenge: Combining flexibility and security. In2021 AEIT International Annual Conference (AEIT) 2021 Oct 4 (pp. 1-6). IEEE.

[130] Holtrup G, Lacube W, David DP, Mermoud A, Bovet G, Lenders V. 5g system security analysis. arXiv preprint arXiv:2108.08700. 2021 Aug 19.

[131] Park S, Kim D, Park Y, Cho H, Kim D, Kwon S. 5G security threat assessment in real networks. Sensors. 2021 Aug 17;21(16):5524.

[132] Mahmoud D, Tóth AB, Kail E, Bánáti A. 5G Vulnarabilities from Security Operation Center's Perspective. In2021 IEEE 21st International Symposium on Computational Intelligence and Informatics (CINTI) 2021 Nov 18 (pp. 000229-000234). IEEE.

[133] Nyangaresi VO, Alsamhi SH. Towards secure traffic signaling in smart grids. In2021 3rd Global Power, Energy and Communication Conference (GPECOM) 2021 Oct 5 (pp. 196-201). IEEE.

[134] Cao J, Ma M, Li H, Zhang Y, Luo Z. A survey on security aspects for LTE and LTE-A networks. IEEE communications surveys & tutorials. 2013 Apr 19;16(1):283-302.

[135] Akyildiz IF, Gutierrez-Estevez DM, Balakrishnan R, Chavarria-Reyes E. LTE-Advanced and the evolution to Beyond 4G (B4G) systems. Physical Communication. 2014 Mar 1;10:31-60.

[136] Ramezanpour K, Jagannath J, Jagannath A. Security and privacy vulnerabilities of 5G/6G and WiFi 6: Survey and research directions from a coexistence perspective. Computer Networks. 2023 Feb 1;221:109515.

[137] Mamadou Mamadou A, Toussaint J, Chalhoub G. Survey on wireless networks coexistence: resource sharing in the 5G era. Mobile Networks and Applications. 2020 Oct;25(5):1749-64.

[138] Agiwal M, Kwon H, Park S, Jin H. A survey on 4G-5G dual connectivity: Road to 5G implementation. Ieee Access. 2021 Jan 18;9:16193-210.

[139] Zhang H, Ma J, Qiu Z, Yao J, Sibahee MA, Abduljabbar ZA, Nyangaresi VO. Multi-GPU Parallel Pipeline Rendering with Splitting Frame. InComputer Graphics International Conference 2023 Aug 28 (pp. 223-235). Cham: Springer Nature Switzerland.

[140] Moysen J, García-Lozano M. Learning-based tracking area list management in 4g and 5g networks. IEEE Transactions on Mobile Computing. 2019 May 6;19(8):1862-78.

[141] Holtmanns S, Rao SP, Oliver I. User location tracking attacks for LTE networks using the interworking functionality. In2016 IFIP Networking conference (IFIP Networking) and workshops 2016 May 17 (pp. 315-322). IEEE.

[142] Poosamani N, Rhee I. Towards a practical indoor location matching system using 4G LTE PHY layer information. In2015 IEEE International Conference on Pervasive Computing and Communication Workshops (PerCom Workshops) 2015 Mar 23 (pp. 284-287). IEEE.

[143] Rao SP, Kotte BT, Holtmanns S. Privacy in LTE networks. InProceedings of the 9th EAI International Conference on Mobile Multimedia Communications 2016 Jun 18 (pp. 176-183).

[144] Jover RP. LTE security, protocol exploits and location tracking experimentation with low-cost software radio. arXiv preprint arXiv:1607.05171. 2016 Jul 18.

[145] Nyangaresi VO, Mohammad Z. Session Key Agreement Protocol for Secure D2D Communication. InThe Fifth International Conference on Safety and Security with IoT: SaSeIoT 2021 2022 Jun 12 (pp. 81-99). Cham: Springer International Publishing.

[146] Mjølsnes SF, Olimid RF. Easy 4G/LTE IMSI catchers for non-programmers. InComputer Network Security: 7th International Conference on Mathematical Methods, Models, and Architectures for Computer Network Security, MMM-ACNS 2017, Warsaw, Poland, August 28-30, 2017, Proceedings 7 2017 (pp. 235-246). Springer International Publishing.

[147] Van Den Broek F, Verdult R, De Ruiter J. Defeating IMSI catchers. InProceedings of the 22Nd ACM SIGSAC Conference on Computer and Communications Security 2015 Oct 12 (pp. 340-351).

[148] Palamà I, Gringoli F, Bianchi G, Melazzi NB. The diverse and variegated reactions of different cellular devices to IMSI catching attacks. InProceedings of the 14th International Workshop on Wireless Network Testbeds, Experimental evaluation & Characterization 2020 Sep 21 (pp. 80-86).

[149] Dabrowski A, Petzl G, Weippl ER. The messenger shoots back: Network operator based IMSI catcher detection. InResearch in Attacks, Intrusions, and Defenses: 19th International Symposium, RAID 2016, Paris, France, September 19-21, 2016, Proceedings 19 2016 (pp. 279-302). Springer International Publishing.

[150] Chlosta M, Rupprecht D, Pöpper C, Holz T. 5G SUCI-Catchers: Still catching them all?. InProceedings of the 14th ACM Conference on Security and Privacy in Wireless and Mobile Networks 2021 Jun 28 (pp. 359-364).

[151] Yenurkar G, Mal S, Nyangaresi VO, Kamble S, Damahe L, Bankar N. Revolutionizing Chronic Heart Disease Management: The Role of IoT-Based Ambulatory Blood Pressure Monitoring System. Diagnostics. 2024 Jun 19;14(12):1297.

[152] Karim I, Hussain SR, Bertino E. Prochecker: An automated security and privacy analysis framework for 4g lte protocol implementations. In2021 IEEE 41st International Conference on Distributed Computing Systems (ICDCS) 2021 Jul 7 (pp. 773-785). IEEE.

[153] Aceto G, Palumbo F, Persico V, Pescapé A. Available bandwidth vs. achievable throughput measurements in 4G mobile networks. In2018 14th International Conference on Network and Service Management (CNSM) 2018 Nov 5 (pp. 125-133). IEEE.

[154] Apruzzese G, Vladimirov R, Tastemirova A, Laskov P. Wild networks: Exposure of 5G network infrastructures to adversarial examples. IEEE Transactions on Network and Service Management. 2022 Jul 6;19(4):5312-32.

[155] Lake D, Wang N, Tafazolli R, Samuel L. Softwarization of 5G networks–implications to open platforms and standardizations. IEEE access. 2021 Apr 8;9:88902-30.

[156] Shanapinda S, Shanapinda S. The Legal Scheme for Mobile Telecommunications Companies and Social Media Platforms to Retain Location Information. Advance Metadata Fair: The Retention and Disclosure of 4G, 5G and Social Media Location Information, for Law Enforcement and National Security, and the Impact on Privacy in Australia. 2020:15-28.

[157] Nyangaresi VO, Ma J. A Formally Verified Message Validation Protocol for Intelligent IoT E-Health Systems. In2022 IEEE World Conference on Applied Intelligence and Computing (AIC) 2022 Jun 17 (pp. 416-422). IEEE.

[158] Michclinakis F, Doroud H, Razaghpanah A, Lutu A, Vallina-Rodriguez N, Gill P, Widmer J. The cloud that runs the mobile internet: A measurement study of mobile cloud services. InIEEE INFOCOM 2018-IEEE Conference on Computer Communications 2018 Apr 16 (pp. 1619-1627). IEEE.

[159] Saldžiūnas K, Skyrius R. The challenges of big data analytics in the mobile communications sector. Ekonomika. 2017 Nov 2;96(2):110-21.

[160] Obaidat MA, Obeidat S, Holst J, Al Hayajneh A, Brown J. A comprehensive and systematic survey on the internet of things: Security and privacy challenges, security frameworks, enabling technologies, threats, vulnerabilities and countermeasures. Computers. 2020 May 30;9(2):44.

[161] Al-Dulaimi MK, Al-Dulaimi AM, Al-Dulaimi OM, Abdulqader AF, Zakharzhevskyi A. Threats in Cloud Computing System and Security Enhancement. In2024 35th Conference of Open Innovations Association (FRUCT) 2024 Apr 24 (pp. 82-93). IEEE.

[162] Anand D, Khemchandani V. Data security and privacy in 5g-enabled IoT. Blockchain for 5G-Enabled IoT: The new wave for Industrial Automation. 2021:279-301.

[163] Abduljabbar ZA, Abduljaleel IQ, Ma J, Al Sibahee MA, Nyangaresi VO, Honi DG, Abdulsada AI, Jiao X. Provably secure and fast color image encryption algorithm based on s-boxes and hyperchaotic map. IEEE Access. 2022 Feb 11;10:26257-70.

[164] Bhavana SU, Miriam DD, Robin CR. Understanding the Implications of SIM Card Swap Fraud in India: A Comprehensive Study. In2024 International Conference on Communication, Computing and Internet of Things (IC3IoT) 2024 Apr 17 (pp. 1-8). IEEE.

[165] Kalyana Abenanth G, Harish K, Sachin V, Rushyendra A, Mohankumar N. Enhancing the Security for Smart Card-Based Embedded Systems. InComputer Networks and Inventive Communication Technologies: Proceedings of Fourth ICCNCT 2021 2022 (pp. 673-686). Springer Singapore.

[166] Sarker K, Islam KM. Embedded Subscriber Identity Module with Context Switching. InInternational Conference on Information, Communication and Computing Technology 2019 May 11 (pp. 84-97). Singapore: Springer Singapore.

[167] Abdelazim MT, Abdelbaki N, Shosha AF. Experimental Digital Forensics of Subscriber Identification Module (SIM) Card. Computer and Network Security Essentials. 2018:391-405.

[168] Yang Y, Zhang Y, Wan T, Wang C, Duan H, Chen J, Li Y. Uncovering Security Vulnerabilities in Real-world Implementation and Deployment of 5G Messaging Services. InProceedings of the 17th ACM Conference on Security and Privacy in Wireless and Mobile Networks 2024 May 27 (pp. 265-276).

[169] Nyangaresi VO. Provably Secure Pseudonyms based Authentication Protocol for Wearable Ubiquitous Computing Environment. In2022 International Conference on Inventive Computation Technologies (ICICT) 2022 Jul 20 (pp. 1-6). IEEE.

[170] Bin Q, Ziwen C, Yong X, Liang H, Sheng S. Rogue base stations detection for advanced metering infrastructure based on signal strength clustering. Ieee Access. 2019 Aug 9;8:158798-805.

[171] Ma B, Guo W, Zhang J. A survey of online data-driven proactive 5G network optimisation using machine learning. IEEE access. 2020 Feb 19;8:35606-37.

[172] Leliopoulos P, Drigas A. Big data and data analytics in 5G mobile networks. Global Journal of Engineering and Technology Advances. 2023;15(3):165-90.

[173] Lemieux F. Cyber Threats, Intelligence Operations, and Mass Surveillance. InIntelligence and State Surveillance in Modern Societies 2018 Dec 3 (pp. 139-163). Emerald Publishing Limited.

[174] Xie T, Tu GH, Li CY, Peng C. How can IoT services pose new security threats in operational cellular networks?. IEEE Transactions on Mobile Computing. 2020 Apr 2;20(8):2592-606.

[175] Abood EW, Abdullah AM, Al Sibahe MA, Abduljabbar ZA, Nyangaresi VO, Kalafy SA, Ghrabta MJ. Audio steganography with enhanced LSB method for securing encrypted text with bit cycling. Bulletin of Electrical Engineering and Informatics. 2022 Feb 1;11(1):185-94.

[176] De Domenico A, Liu YF, Yu W. Optimal virtual network function deployment for 5G network slicing in a hybrid cloud infrastructure. IEEE Transactions on Wireless Communications. 2020 Aug 25;19(12):7942-56.

[177] Kotulski Z, Nowak T, Sepczuk M, Tunia M, Artych R, Bocianiak K, Osko T, Wary JP. On end-to-end approach for slice isolation in 5G networks. Fundamental challenges. In2017 Federated conference on computer science and information systems (FedCSIS) 2017 Sep 3 (pp. 783-792). IEEE.

[178] Wichary T, Mongay Batalla J, Mavromoustakis CX, Żurek J, Mastorakis G. Network slicing security controls and assurance for verticals. Electronics. 2022 Jan 11;11(2):222.

[179] Madi T, Jarraya Y, Alimohammadifar A, Majumdar S, Wang Y, Pourzandi M, Wang L, Debbabi M. ISOTOP: auditing virtual networks isolation across cloud layers in OpenStack. ACM Transactions on Privacy and Security (TOPS). 2018 Oct 23;22(1):1-35.

[180] Binns R, Lyngs U, Van Kleek M, Zhao J, Libert T, Shadbolt N. Third party tracking in the mobile ecosystem. InProceedings of the 10th ACM Conference on Web Science 2018 May 15 (pp. 23-31).

[181] Nyangaresi VO. Lightweight anonymous authentication protocol for resource-constrained smart home devices based on elliptic curve cryptography. Journal of Systems Architecture. 2022 Dec 1;133:102763.

[182] Chlosta M, Rupprecht D, Holz T, Pöpper C. LTE security disabled: misconfiguration in commercial networks. InProceedings of the 12th conference on security and privacy in wireless and mobile networks 2019 May 15 (pp. 261-266).

[183] Lounis K, Zulkernine M. Attacks and defenses in short-range wireless technologies for IoT. IEEE Access. 2020 May 11;8:88892-932.

[184] He L, Yan Z, Atiquzzaman M. LTE/LTE-A network security data collection and analysis for security measurement: A survey. IEEE Access. 2018 Jan 12;6:4220-42.

[185] Fang D, Qian Y, Hu RQ. Security for 5G mobile wireless networks. IEEE access. 2017 Dec 4;6:4850-74.

[186] Altulaihan E, Almaiah MA, Aljughaiman A. Cybersecurity threats, countermeasures and mitigation techniques on the IoT: Future research directions. Electronics. 2022 Oct 16;11(20):3330.

[187] Mohammad Z, Nyangaresi V, Abusukhon A. On the Security of the Standardized MQV Protocol and Its Based Evolution Protocols. In2021 International Conference on Information Technology (ICIT) 2021 Jul 14 (pp. 320-325). IEEE.

[188] Mashtalyar N, Ntaganzwa UN, Santos T, Hakak S, Ray S. Social engineering attacks: Recent advances and challenges. InInternational Conference on Human-Computer Interaction 2021 Jul 3 (pp. 417-431). Cham: Springer International Publishing.

[189] Ekene OE, Ruhl R, Zavarsky P. Enhanced user security and privacy protection in 4G LTE network. In2016 IEEE 40th Annual Computer Software and Applications Conference (COMPSAC) 2016 Jun 10 (Vol. 2, pp. 443-448). IEEE.

[190] Fan CI, Shih YT, Huang JJ, Chiu WR. Cross-network-slice authentication scheme for the 5 th generation mobile communication system. IEEE Transactions on Network and Service Management. 2021 Jan 18;18(1):701-12.

[191] Yadav AK, Wijethilaka S, Braeken A, Misra M, Liyanage M. An Enhanced Cross-Network-Slice Authentication Protocol for 5G. IEEE Transactions on Sustainable Computing. 2023 Jun 7;8(4):555-73.

[192] He Y, Zhang C, Wu B, Yang Y, Xiao K, Li H. Cross-Chain Trusted Service Quality Computing Scheme for Multichain-Model-Based 5G Network Slicing SLA. IEEE Internet of Things Journal. 2021 Dec 3;10(14):12126-39.

[193] Nyangaresi VO. Lightweight key agreement and authentication protocol for smart homes. In2021 IEEE AFRICON 2021 Sep 13 (pp. 1-6). IEEE.

[194] Sneps-Sneppe M, Namiot D. On Open Gateway from GSMA–Is It a Revolutionary or Too Little and Too Late Deal?. In2023 33rd Conference of Open Innovations Association (FRUCT) 2023 May 24 (pp. 283-289). IEEE.

[195] Henrydoss J, Boult T. Critical security review and study of DDoS attacks on LTE mobile network. In2014 IEEE Asia Pacific Conference on Wireless and Mobile 2014 Aug 28 (pp. 194-200). IEEE.

[196] Eliyan LF, Di Pietro R. DoS and DDoS attacks in Software Defined Networks: A survey of existing solutions and research challenges. Future Generation Computer Systems. 2021 Sep 1;122:149-71.

[197] Huseinović A, Mrdović S, Bicakci K, Uludag S. A survey of denial-of-service attacks and solutions in the smart grid. IEEE Access. 2020 Sep 25;8:177447-70.

[198] Mavoungou S, Kaddoum G, Taha M, Matar G. Survey on threats and attacks on mobile networks. IEEE Access. 2016 Aug 18;4:4543-72.

[199] Al Sibahee MA, Abdulsada AI, Abduljabbar ZA, Ma J, Nyangaresi VO, Umran SM. Lightweight, Secure, Similar-Document Retrieval over Encrypted Data. Applied Sciences. 2021 Jan;11(24):12040.

[200] Lee H, Vahid S, Moessner K. A survey of radio resource management for spectrum aggregation in LTE-advanced. IEEE Communications Surveys & Tutorials. 2013 Nov 7;16(2):745-60.

[201] Drira W, Ahn K, Rakha H, Filali F. Development and testing of a 3G/LTE adaptive data collection system in vehicular networks. IEEE Transactions on Intelligent Transportation Systems. 2015 Aug 27;17(1):240-9.

[202] Villegas MM, Orellana C, Astudillo H. A study of over-the-air (OTA) update systems for CPS and IoT operating systems. InProceedings of the 13th European Conference on Software Architecture-Volume 2 2019 Sep 9 (pp. 269-272).

[203] Elbamby MS, Perfecto C, Liu CF, Park J, Samarakoon S, Chen X, Bennis M. Wireless edge computing with latency and reliability guarantees. Proceedings of the IEEE. 2019 Jun 11;107(8):1717-37.

[204] Caiazza C, Giordano S, Luconi V, Vecchio A. Edge computing vs centralized cloud: Impact of communication latency on the energy consumption of LTE terminal nodes. Computer Communications. 2022 Oct 1;194:213-25.

[205] Nyangaresi VO, Ahmad M, Alkhayyat A, Feng W. Artificial neural network and symmetric key cryptography based verification protocol for 5G enabled Internet of Things. Expert Systems. 2022 Dec;39(10):e13126.

[206] Putra D, Yuhanef A, Chandra D. Comparative Analysis Of 4G LTE Network Quality At 900 Mhz And 2100 Mhz Frequencies. International Journal of Wireless And Multimedia Communications. 2024 Jan 31;1(1):39-46.

[207] Briscoe B, Brunstrom A, Petlund A, Hayes D, Ros D, Tsang J, Gjessing S, Fairhurst G, Griwodz C, Welzl M. Reducing internet latency: A survey of techniques and their merits. IEEE Communications Surveys & Tutorials. 2014 Nov 26;18(3):2149-96.

[208] Afzal SR, Stuijk S, Nabi M, Basten T. Effective link quality estimation as a means to improved end-to-end packet delivery in high traffic mobile ad hoc networks. Digital Communications and Networks. 2017 Aug 1;3(3):150-63.

[209] Hajlaoui E, Zaier A, Khlifi A, Ghodhbane J, Hamed MB, Sbita L. 4G and 5G technologies: A Comparative Study. In2020 5th International Conference on Advanced Technologies for Signal and Image Processing (ATSIP) 2020 Sep 2 (pp. 1-6). IEEE.

[210] Yang Y, Hanzo L. Permutation-based TCP and UDP transmissions to improve goodput and latency in the Internet of Things. IEEE Internet of Things Journal. 2021 Mar 23;8(18):14276-86.

[211] Zaki Rashed AN, Ahammad SH, Daher MG, Sorathiya V, Siddique A, Asaduzzaman S, Rehana H, Dutta N, Patel SK, Nyangaresi VO, Jibon RH. Signal propagation parameters estimation through designed multi layer fibre with higher dominant modes using OptiFibre simulation. Journal of Optical Communications. 2022 Jun 23(0).

[212] Wan L, Guo Z, Wu Y, Bi W, Yuan J, Elkashlan M, Hanzo L. 4G\/5G spectrum sharing: efficient 5G deployment to serve enhanced mobile broadband and internet of things applications. ieee vehicular technology magazine. 2018 Sep 20;13(4):28-39.

[213] Clarke RN. Expanding mobile wireless capacity: The challenges presented by technology and economics. Telecommunications Policy. 2014 Sep 1;38(8-9):693-708.

[214] Akhtar T, Tselios C, Politis I. Radio resource management: approaches and implementations from 4G to 5G and beyond. Wireless Networks. 2021 Jan;27:693-734.

[215] Olwal TO, Djouani K, Kurien AM. A survey of resource management toward 5G radio access networks. IEEE Communications Surveys & Tutorials. 2016 Apr 5;18(3):1656-86.

[216] Demestichas P, Georgakopoulos A, Karvounas D, Tsagkaris K, Stavroulaki V, Lu J, Xiong C, Yao J. 5G on the horizon: Key challenges for the radio-access network. IEEE vehicular technology magazine. 2013 Jul 25;8(3):47-53.

[217] Eid MM, Arunachalam R, Sorathiya V, Lavadiya S, Patel SK, Parmar J, Delwar TS, Ryu JY, Nyangaresi VO, Zaki Rashed AN. QAM receiver based on light amplifiers measured with effective role of optical coherent duobinary transmitter. Journal of Optical Communications. 2022 Jan 17(0).

[218] Safdar GA, Ur-Rehman M, Muhammad M, Imran MA, Tafazolli R. Interference mitigation in D2D communication underlaying LTE-A network. IEEE Access. 2016 Oct 25;4:7967-87.

[219] Yassin M, AboulHassan MA, Lahoud S, Ibrahim M, Mezher D, Cousin B, Sourour EA. Survey of ICIC techniques in LTE networks under various mobile environment parameters. Wireless Networks. 2017 Feb;23:403-18.

[220] Elbamby MS, Perfecto C, Bennis M, Doppler K. Toward low-latency and ultra-reliable virtual reality. IEEE network. 2018 Apr 2;32(2):78-84.

[221] Molner N, de la Oliva A, Stavrakakis I, Azcorra A. Optimization of an integrated fronthaul/backhaul network under path and delay constraints. Ad Hoc Networks. 2019 Feb 1;83:41-54.

[222] Wang T, Xu H, Liu F. Multi-resource load balancing for virtual network functions. In2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS) 2017 Jun 5 (pp. 1322-1332). IEEE.

[223] Al Sibahee MA, Ma J, Nyangaresi VO, Abduljabbar ZA. Efficient Extreme Gradient Boosting Based Algorithm for QoS Optimization in Inter-Radio Access Technology Handoffs. In2022 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA) 2022 Jun 9 (pp. 1-6). IEEE.

[224] Fernández Z, Martín A, Pérez J, García M, Velez G, Murciano F, Peters S. Challenges and solutions for service continuity in inter-plmn handover for vehicular applications. IEEE Access. 2023 Jan 25;11:8904-19.

[225] Fernando R. The impact of Planned Special Events (PSEs) on urban traffic congestion. EAI Endorsed Transactions on Scalable Information Systems. 2019 Jul 24;6(23):e4-.

[226] Bouraqia K, Sabir E, Sadik M, Ladid L. Quality of experience for streaming services: measurements, challenges and insights. IEEE Access. 2020 Jan 9;8:13341-61.

[227] Cabrera-Castellanos DF, Aragón-Zavala A, Castañón-Ávila G. Closing connectivity gap: An overview of mobile coverage solutions for not-spots in rural zones. Sensors. 2021 Dec 1;21(23):8037.

[228] Alsaeedy AA, Chong EK. A review of mobility management entity in LTE networks: Power consumption and signaling overhead. International Journal of Network Management. 2020 Jan;30(1):e2088.

[229] Nyangaresi VO. Terminal independent security token derivation scheme for ultra-dense IoT networks. Array. 2022 Sep 1;15:100210.

[230] Zhong ZD, Ai B, Zhu G, Wu H, Xiong L, Wang FG, Lei L, Ding JW, Guan K, He RS. Dedicated mobile communications for high-speed railway. Heidelberg: Springer; 2018.

[231] Xu Y, Gui G, Gacanin H, Adachi F. A survey on resource allocation for 5G heterogeneous networks: Current research, future trends, and challenges. IEEE Communications Surveys & Tutorials. 2021 Feb 17;23(2):668-95.

[232] Jameel F, Hamid Z, Jabeen F, Zeadally S, Javed MA. A survey of device-to-device communications: Research issues and challenges. IEEE Communications Surveys & Tutorials. 2018 Apr 18;20(3):2133-68.

[233] Khan MA, Mittal S, West S, Wuest T. Review on upgradability–A product lifetime extension strategy in the context of product service systems. Journal of cleaner production. 2018 Dec 10;204:1154-68.

[234] Richart M, Baliosian J, Serrat J, Gorricho JL, Agüero R. Slicing with guaranteed quality of service in wifi networks. IEEE Transactions on Network and Service Management. 2020 Jun 30;17(3):1822-37.

[235] Abood EW, Hussien ZA, Kawi HA, Abduljabbar ZA, Nyangaresi VO, Ma J, Al Sibahee MA, Kalafy A, Ahmad S. Provably secure and efficient audio compression based on compressive sensing. International Journal of Electrical & Computer Engineering (2088-8708). 2023 Feb 1;13(1).

[236] Sari A, Caglar E. Load balancing algorithms and protocols to enhance quality of service and performance in data of wsn. InSecurity and Resilience in Intelligent Data-Centric Systems and Communication Networks 2018 Jan 1 (pp. 143-178). Academic Press.

[237] Liu J, Sheng M, Liu L, Li J. Network densification in 5G: From the short-range communications perspective. IEEE Communications Magazine. 2017 Dec 13;55(12):96-102.

[238] Habeeb RA, Nasaruddin F, Gani A, Hashem IA, Ahmed E, Imran M. Real-time big data processing for anomaly detection: A survey. International Journal of Information Management. 2019 Apr 1;45:289-307.

[239] Kanwal K, Safdar GA, Ur-Rehman M, Yang X. Energy management in LTE networks. IEEE Access. 2017 Mar 28;5:4264-84.

[240] Linguaglossa L, Lange S, Pontarelli S, Rétvári G, Rossi D, Zinner T, Bifulco R, Jarschel M, Bianchi G. Survey of performance acceleration techniques for network function virtualization. Proceedings of the IEEE. 2019 Mar 13;107(4):746-64.

[241] Nyangaresi VO. A Formally Validated Authentication Algorithm for Secure Message Forwarding in Smart Home Networks. SN Computer Science. 2022 Jul 9;3(5):364.

[242] Seddigh N, Nandy B, Makkar R, Beaumont JF. Security advances and challenges in 4G wireless networks. In2010 Eighth International Conference on Privacy, Security and Trust 2010 Aug 17 (pp. 62-71). IEEE.

[243] Zhang S, Wang Y, Zhou W. Towards secure 5G networks: A Survey. Computer Networks. 2019 Oct 24;162:106871.

[244] Sultan I, Mir BJ, Banday MT. Analysis and optimization of advanced encryption standard for the internet of things. In2020 7th International Conference on Signal Processing and Integrated Networks (SPIN) 2020 Feb 27 (pp. 571-575). IEEE.

[245] Li N, Liu D, Nepal S. Lightweight mutual authentication for IoT and its applications. IEEE Transactions on Sustainable Computing. 2017 Jun 19;2(4):359-70.

[246] Lin C, He D, Huang X, Choo KK, Vasilakos AV. BSeIn: A blockchain-based secure mutual authentication with fine-grained access control system for industry 4.0. Journal of network and computer applications. 2018 Aug 15;116:42-52.

[247] Alsamhi SH, Shvetsov AV, Kumar S, Shvetsova SV, Alhartomi MA, Hawbani A, Rajput NS, Srivastava S, Saif A, Nyangaresi VO. UAV computing-assisted search and rescue mission framework for disaster and harsh environment mitigation. Drones. 2022 Jun 22;6(7):154.

[248] Azeez NA, Bada TM, Misra S, Adewumi A, Van der Vyver C, Ahuja R. Intrusion detection and prevention systems: an updated review. Data Management, Analytics and Innovation: Proceedings of ICDMAI 2019, Volume 1. 2020:685-96.

[249] Bhardwaj A, Kaushik K, Alshehri M, Mohamed AA, Keshta I. ISF: Security analysis and assessment of smart home IoT-based firmware. ACM Transactions on Sensor Networks. 2023 Jan.

[250] Pradeep KV, Vijayakumar V, Subramaniyaswamy V. An efficient framework for sharing a file in a secure manner using asymmetric key distribution management in cloud environment. Journal of Computer Networks and Communications. 2019;2019(1):9852472.

[251] Ahmad S, Mehfuz S, Beg J. Hybrid cryptographic approach to enhance the mode of key management system in cloud environment. The Journal of Supercomputing. 2023 May;79(7):7377-413.

[252] Rao PM, Deebak BD. A comprehensive survey on authentication and secure key management in internet of things: Challenges, countermeasures, and future directions. Ad Hoc Networks. 2023 Jul 1;146:103159.

[253] Nyangaresi VO. Hardware assisted protocol for attacks prevention in ad hoc networks. InEmerging Technologies in Computing: 4th EAI/IAER International Conference, iCETiC 2021, Virtual Event, August 18–19, 2021, Proceedings 4 2021 (pp. 3-20). Springer International Publishing.

[254] Elsaadany M, Ali A, Hamouda W. Cellular LTE-A technologies for the future Internet-of-Things: Physical layer features and challenges. IEEE Communications Surveys & Tutorials. 2017 Jul 18;19(4):2544-72.

[255] Al Shebli HM, Beheshti BD. A study on penetration testing process and tools. In2018 IEEE Long Island Systems, Applications and Technology Conference (LISAT) 2018 May 4 (pp. 1-7). IEEE.

[256] Butun I, Österberg P, Song H. Security of the Internet of Things: Vulnerabilities, attacks, and countermeasures. IEEE Communications Surveys & Tutorials. 2019 Nov 13;22(1):616-44.

[257] Bécue A, Praça I, Gama J. Artificial intelligence, cyber-threats and Industry 4.0: Challenges and opportunities. Artificial Intelligence Review. 2021 Jun;54(5):3849-86.

[258] Tirfe D, Anand VK. A survey on trends of two-factor authentication. InContemporary Issues in Communication, Cloud and Big Data Analytics: Proceedings of CCB 2020 2022 (pp. 285-296). Springer Singapore.

[259] Abduljabbar ZA, Nyangaresi VO, Jasim HM, Ma J, Hussain MA, Hussien ZA, Aldarwish AJ. Elliptic Curve Cryptography-Based Scheme for Secure Signaling and Data Exchanges in Precision Agriculture. Sustainability. 2023 Jun 28;15(13):10264.

[260] Khan M, Ginzboorg P, Järvinen K, Niemi V. Defeating the downgrade attack on identity privacy in 5G. InSecurity Standardisation Research: 4th International Conference, SSR 2018, Darmstadt, Germany, November 26-27, 2018, Proceedings 4 2018 (pp. 95-119). Springer International Publishing.

[261] Sanwald S, Kaneti L, Stöttinger M, Böhner M. Secure boot revisited: challenges for secure implementations in the automotive domain. SAE International Journal of Transportation Cybersecurity and Privacy. 2020 Aug 13;2(11-02-02-0008):69-81.

[262] Qiu J, Tian Z, Du C, Zuo Q, Su S, Fang B. A survey on access control in the age of internet of things. IEEE Internet of Things Journal. 2020 Jan 24;7(6):4682-96.

[263] Mavridis I, Karatza H. Combining containers and virtual machines to enhance isolation and extend functionality on cloud computing. Future Generation Computer Systems. 2019 May 1;94:674-96.

[264] Salim MM, Kang J, Pan Y, Park JH. A Lightweight authentication scheme for IoT against Rogue Base Station Attacks. Mathematical Biosciences and Engineering. 2022 Aug 1;19(11):11735-55.

[265] Karbasi AH, Shahpasand S. A post-quantum end-to-end encryption over smart contract-based blockchain for defeating man-in-the-middle and interception attacks. Peer-to-peer networking and applications. 2020 Sep;13:1423-41.

[266] Thompson EC, Thompson EC. Continuous Monitoring. Designing a HIPAA-Compliant Security Operations Center: A Guide to Detecting and Responding to Healthcare Breaches and Events. 2020:95-163.

[267] Pirayesh H, Zeng H. Jamming attacks and anti-jamming strategies in wireless networks: A comprehensive survey. IEEE communications surveys & tutorials. 2022 Mar 14;24(2):767-809.

[268] Park S, Shaik A, Borgaonkar R, Seifert JP. Anatomy of commercial IMSI catchers and detectors. InProceedings of the 18th ACM Workshop on Privacy in the Electronic Society 2019 Nov 11 (pp. 74-86).

[269] Weichbroth P, Łysik Ł. Mobile security: Threats and best practices. Mobile Information Systems. 2020;2020(1):8828078.

[270] Nyangaresi VO, Mohammad Z. Privacy preservation protocol for smart grid networks. In2021 International Telecommunications Conference (ITC-Egypt) 2021 Jul 13 (pp. 1-4). IEEE.

[271] Hasan K, Shetty S, Oyedare T. Cross layer attacks on GSM mobile networks using software defined radios. In2017 14th IEEE Annual Consumer Communications & Networking Conference (CCNC) 2017 Jan 8 (pp. 357-360). IEEE.

[272] Nguyen VL, Lin PC, Cheng BC, Hwang RH, Lin YD. Security and privacy for 6G: A survey on prospective technologies and challenges. IEEE Communications Surveys & Tutorials. 2021 Aug 30;23(4):2384-428.

[273] Lohan ES, Alén-Savikko A, Chen L, Järvinen K, Leppäkoski H, Kuusniemi H, Korpisaari P. 5G positioning: Security and privacy aspects. A Comprehensive Guide to 5G Security. 2018 Mar 1:281-320.

[274] Pedraja D, Baliosian J, Betarte G. Offloading cryptographic services to the SIM card. In2018 Eighth Latin-American Symposium on Dependable Computing (LADC) 2018 Oct 8 (pp. 47-56). IEEE.

[275] Tomasin S, Centenaro M, Seco-Granados G, Roth S, Sezgin A. Location-privacy leakage and integrated solutions for 5G cellular networks and beyond. Sensors. 2021 Jul 30;21(15):5176.

[276] Kotulski Z, Nowak TW, Sepczuk M, Tunia MA. 5G networks: Types of isolation and their parameters in RAN and CN slices. Computer Networks. 2020 Apr 22;171:107135.

[277] Abd Razak S, Nazari NH, Al-Dhaqm A. Data anonymization using pseudonym system to preserve data privacy. Ieee Access. 2020 Feb 28;8:43256-64.

[278] Omollo VN, Musyoki S. Global Positioning System Based Routing Algorithm for Adaptive Delay Tolerant Mobile Adhoc Networks. International Journal of Computer and Communication System Engineering. 2015 May 11; 2(3): 399-406.

[279] Politou E, Alepis E, Virvou M, Patsakis C. Privacy and data protection challenges in the distributed era. Heidelberg, Germany: Springer; 2022.

[280] Xu L, Jiang C, Wang J, Yuan J, Ren Y. Information security in big data: privacy and data mining. Ieee Access. 2014 Oct 9;2:1149-76.

[281] El Jaouhari S, Bouvet E. Secure firmware Over-The-Air updates for IoT: Survey, challenges, and discussions. Internet of Things. 2022 May 1;18:100508.

[282] Pramanik MI, Lau RY, Hossain MS, Rahoman MM, Debnath SK, Rashed MG, Uddin MZ. Privacy preserving big data analytics: A critical analysis of state-of-the-art. Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery. 2021 Jan;11(1):e1387.

[283] Zhang Y, Zheng D, Deng RH. Security and privacy in smart health: Efficient policy-hiding attribute-based access control. IEEE Internet of Things Journal. 2018 Apr 10;5(3):2130-45.

[284] Oetzel MC, Spiekermann S. A systematic methodology for privacy impact assessments: a design science approach. European Journal of Information Systems. 2014 Mar 1;23(2):126-50.

[285] Jayalaxmi PL, Saha R, Kumar G, Conti M, Kim TH. Machine and deep learning solutions for intrusion detection and prevention in IoTs: A survey. IEEE Access. 2022 Nov 7;10:121173-92.

[286] Ranaweera P, Jurcut AD, Liyanage M. Survey on multi-access edge computing security and privacy. IEEE Communications Surveys & Tutorials. 2021 Feb 26;23(2):1078-124.

[287] Nyangaresi VO. Provably secure protocol for 5G HetNets. In2021 IEEE International Conference on Microwaves, Antennas, Communications and Electronic Systems (COMCAS) 2021 Nov 1 (pp. 17-22). IEEE.

[288] Moreno RT, García-Rodríguez J, Bernabé JB, Skarmeta A. A trusted approach for decentralised and privacy-preserving identity management. IEEE Access. 2021 Jul 26;9:105788-804.

[289] Kalloniatis C, Lambrinoudakis C, Musahl M, Kanatas A, Gritzalis S. Incorporating privacy by design in body sensor networks for medical applications: A privacy and data protection framework. Computer Science and Information Systems. 2021;18(1):323-47.

[290] Assaderaghi F, Chindalore G, Ibrahim B, de Jong H, Joye M, Nassar S, Steinbauer W, Wagner M, Wille T. Privacy and security: Key requirements for sustainable IoT growth. In2017 Symposium on VLSI Technology 2017 Jun 5 (pp. T8-T13). IEEE.

[291] Barb G, Alexa F, Otesteanu M. Dynamic spectrum sharing for future LTE-NR networks. Sensors. 2021 Jun 19;21(12):4215.

[292] Alsharif MH, Albreem MA, Solyman AA, Kim S. Toward 6G communication networks: Terahertz frequency challenges and open research issues. Computers, Materials & Continua. 2021.

[293] Khan AS, Sattar MA, Nisar K, Ibrahim AA, Annuar NB, Abdullah JB, Karim Memon S. A survey on 6G enabled light weight authentication protocol for UAVs, security, open research issues and future directions. Applied Sciences. 2022 Dec 26;13(1):277.

[294] Al-Dulaimi OM, Al-Dulaimi AM, Alexandra MO, Al-Dulaimi MK. Strategy for non-orthogonal multiple access and performance in 5G and 6G networks. Sensors. 2023 Feb 3;23(3):1705.

[295] Al-Dulaimi OM, Al-Dulaimi AM, Alexandra MO, Al-Dulaimi MK. Strategy for non-orthogonal multiple access and performance in 5G and 6G networks. Sensors. 2023 Feb 3;23(3):1705.

[296] Mihovska A, Prasad R. Overview of 5G new radio and carrier aggregation: 5G and beyond networks. In2020 23rd international symposium on wireless personal multimedia communications (WPMC) 2020 Oct 19 (pp. 1-6). IEEE.

[297] Al Sibahee MA, Nyangaresi VO, Ma J, Abduljabbar ZA. Stochastic Security Ephemeral Generation Protocol for 5G Enabled Internet of Things. InIoT as a Service: 7th EAI International Conference, IoTaaS 2021, Sydney, Australia, December 13–14, 2021, Proceedings 2022 Jul 8 (pp. 3-18). Cham: Springer International Publishing.

[298] Ali E, Ismail M, Nordin R, Abdulah NF. Beamforming techniques for massive MIMO systems in 5G: overview, classification, and trends for future research. Frontiers of Information Technology & Electronic Engineering. 2017 Jun;18:753-72.

[299] Al-Turjman F, Ever E, Zahmatkesh H. Small cells in the forthcoming 5G/IoT: Traffic modelling and deployment overview. IEEE Communications Surveys & Tutorials. 2018 Aug 10;21(1):28-65.

[300] Khan LU, Yaqoob I, Tran NH, Han Z, Hong CS. Network slicing: Recent advances, taxonomy, requirements, and open research challenges. IEEE Access. 2020 Feb 19;8:36009-28.

[301] Zhao Y, Wang W, Li Y, Meixner CC, Tornatore M, Zhang J. Edge computing and networking: A survey on infrastructures and applications. IEEE Access. 2019 Jul 9;7:101213-30.

[302] Irram F, Ali M, Maqbool Z, Qamar F, Rodrigues JJ. Coordinated multi-point transmission in 5G and beyond heterogeneous networks. In2020 IEEE 23rd international multitopic conference (INMIC) 2020 Nov 5 (pp. 1-6). IEEE.

[303] Al-Shammari BK, Al-Aboody N, Al-Raweshidy HS. IoT traffic management and integration in the QoS supported network. IEEE Internet of Things Journal. 2017 Dec 19;5(1):352-70.

[304] Moysen J, Giupponi L. From 4G to 5G: Self-organized network management meets machine learning. Computer Communications. 2018 Sep 1;129:248-68.

[305] Rosa C, Pedersen K, Wang H, Michaelsen PH, Barbera S, Malkamäki E, Henttonen T, Sébire B. Dual connectivity for LTE small cell evolution: Functionality and performance aspects. IEEE Communications Magazine. 2016 Jun 23;54(6):137-43.

[306] Nyangaresi VO. ECC based authentication scheme for smart homes. In2021 International Symposium ELMAR 2021 Sep 13 (pp. 5-10). IEEE.

[307] King D, Farrel A, Georgalas N. The role of SDN and NFV for flexible optical networks: Current status, challenges and opportunities. In2015 17th international conference on transparent optical networks (ICTON) 2015 Jul 5 (pp. 1-6). IEEE.

[308] Ghomi EJ, Rahmani AM, Qader NN. Load-balancing algorithms in cloud computing: A survey. Journal of Network and Computer Applications. 2017 Jun 15;88:50-71.

[309] Mitnala VN, Reed MJ, Kegel I, Bicknell J. Avoiding handover interruptions in pervasive communication applications through machine learning. In2021 IEEE International Conference and Expo on Real Time Communications at IIT (RTC) 2021 Oct 12 (pp. 1-8). IEEE.

[310] Shabalov MY, Zhukovskiy YL, Buldysko AD, Gil B, Starshaia VV. The influence of technological changes in energy efficiency on the infrastructure deterioration in the energy sector. Energy Reports. 2021 Nov 1;7:2664-80.

[311] Abdelfatah M, ElSayed S, Zekry A. A Study on the Basics Processes of Massive MIMO. J. Commun.. 2022 Mar;17(3):167-79.

[312] Zeng H, Natale MD, Zhu Q. Minimizing stack and communication memory usage in real-time embedded applications. ACM Transactions on Embedded Computing Systems (TECS). 2014 Jul 23;13(5s):1-25.

[313] Alawe I, Ksentini A, Hadjadj-Aoul Y, Bertin P. Improving traffic forecasting for 5G core network scalability: A machine learning approach. IEEE Network. 2018 Nov 29;32(6):42-9.

[314] Abduljabbar ZA, Omollo Nyangaresi V, Al Sibahee MA, Ghrabat MJ, Ma J, Qays Abduljaleel I, Aldarwish AJ. Session-Dependent Token-Based Payload Enciphering Scheme for Integrity Enhancements in Wireless Networks. Journal of Sensor and Actuator Networks. 2022 Sep 19;11(3):55.

[315] Yunas SF, Valkama M, Niemelä J. Cell planning for outdoor distributed antenna systems in dense urban areas. In2014 16th International Telecommunications Network Strategy and Planning Symposium (Networks) 2014 Sep 17 (pp. 1-7). IEEE.

[316] Atawia R, Ashour M, El Shabrawy T, Hammad H. Indoor distributed antenna system planning with optimized antenna power using genetic algorithm. In2013 IEEE 78th Vehicular Technology Conference (VTC Fall) 2013 Sep 2 (pp. 1-6). IEEE.

[317] Heath R, Peters S, Wang Y, Zhang J. A current perspective on distributed antenna systems for the downlink of cellular systems. IEEE Communications Magazine. 2013 Apr 11;51(4):161-7.

[318] Shakya S, Poon K, Ouali A. A GA based network optimization tool for passive in-building distributed antenna systems. InProceedings of the Genetic and Evolutionary Computation Conference 2018 Jul 2 (pp. 1371-1378).

[319] Johnson J. Designing with the mind in mind: simple guide to understanding user interface design guidelines. Morgan Kaufmann; 2020 Aug 14.

[320] Buyya R, Ilager S, Arroba P. Energy-efficiency and sustainability in new generation cloud computing: A vision and directions for integrated management of data centre resources and workloads. Software: Practice and Experience. 2024 Jan;54(1):24-38.