GSC Advanced Research and Reviews

eISSN: 2582-4597 CODEN (USA): GARRC2

Cross Ref DOI: 10.30574/gscarr

Journal homepage: https://gsconlinepress.com/journals/gscarr/

(REVIEW ARTICLE)

Check for updates

A comprehensive systematic review of privacy and security issues in Satellite Networks

Ogweno Jeremiah Okeyo *

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

GSC Advanced Research and Reviews, 2024, 20(01), 349–375

Publication history: Received on 07 June 2024; revised on 19 July 2024; accepted on 22 July 2024

Article DOI: https://doi.org/10.30574/gscarr.2024.20.1.0267

Abstract

The recent advancements in satellite networks have garnered significant interest due to their extensive geographic coverage and flexible deployment capabilities, offering a promising solution for global communications and transforming traditional communication methods. Despite these advancements, current satellite systems face challenges such as high propagation delays and inadequate coverage of high-latitude regions, particularly in Geostationary (GEO) systems. Low Earth Orbit (LEO) systems, which can address these issues, are primarily used for voice services, as seen in the Iridium system, but have encountered financial difficulties. This study aims to address the security issues in satellite networks, a critical concern as these networks increasingly rely on IP protocols and hybrid configurations of terrestrial nodes and satellite links. Previous works have identified various potential security attacks on satellite networks and proposed different solutions, but these solutions often lack comprehensive effectiveness and robustness. Our methodology involves analyzing the security vulnerabilities in satellite networks similar to the Iridium system, which includes inter-satellite links (ISL) and routers on each satellite. We review and evaluate existing security measures and propose enhancements to improve their effectiveness. Our results indicate significant vulnerabilities in current systems, but also show that with targeted improvements, security can be substantially enhanced. The implications of this study are profound, suggesting that more secure satellite networks can better support critical global communications and services, including broadband Internet and data services, thereby enhancing their reliability and user trust

Keywords: Satellite Networks; Geostationary Satellites (GEO); Broadband Internet; Inter-Satellite Links (ISL); Security; Privacy

1. Introduction

The launch of the first artificial satellite, Sputnik 1, by the Soviet Union in 1957 marked a pivotal moment in human history, signaling the dawn of the Space Age and sparking the development of satellite networks [1] [2]. Sputnik 1, a metal sphere with a diameter of 58.5 cm (23 inches) equipped with four external antennas, emitted signals from its 1-watt radio transmitter that could be received by amateur radio enthusiasts within a 2000 km range. This groundbreaking event demonstrated the potential of satellites to revolutionize communications, despite Sputnik 1 not being designed specifically for data transmission. Its primary purpose was to explore space and rocket technology, laying the groundwork for future communications satellites [3].

The first notable communications satellite was Project SCORE, launched by the United States in 1958. This satellite utilized a tape recorder to store and forward voice messages, most famously delivering a Christmas greeting from U.S. President Dwight D. Eisenhower. Following this, NASA launched the Echo satellite in 1960, a large aluminized PET film balloon that acted as a passive reflector for radio communications. In the same year, Courier 1B, developed by Philco, became the world's first active repeater satellite, enhancing the capabilities of satellite communications. Sputnik 1's

* Corresponding author: Ogweno Jeremiah Okeyo

primary role was not for direct communications but as a crucial step toward the advancements that would define the satellite communications era. The true genesis of active communication satellites came with Telstar, launched in 1962 by AT&T. Telstar was the first active, direct relay communications satellite, a result of a multinational collaboration between AT&T, Bell Telephone Laboratories, NASA, the British General Post Office, and the French National PTT. Its successful launch and operation demonstrated the feasibility of satellite-based communication, leading to Relay 1, which achieved the first trans-Pacific broadcast in 1963.

The 1960s and 1970s witnessed rapid advancements in satellite performance and the emergence of a global satellite communications industry. Initially, satellites were primarily used for international and long-distance telephone traffic and the distribution of select television programming. A significant milestone was the Canadian Broadcasting Corporation's use of Telesat's Anik A satellite in 1973 to distribute video programming across Canada. This was soon followed by HBO's use of satellite technology in 1975 to deliver video programming to U.S. customers, marking the beginning of commercial satellite broadcasting.

By the 1990s, satellite communications had become the primary method for distributing television programs globally. This era saw a dramatic increase in the utilization of satellites for a wide range of communication services, including television, radio, and telephone. The success of these early ventures laid a robust foundation for the modern satellite communications infrastructure that supports today's interconnected world [4]-[6]. Despite these advancements, contemporary satellite networks still face significant challenges, particularly concerning security [7], [8]. As satellite systems increasingly rely on IP protocols and hybrid configurations comprising terrestrial nodes and satellite links, ensuring their security has become a critical issue. Current Low Earth Orbit (LEO) systems, like Iridium, primarily provide voice services but have struggled with financial sustainability and security vulnerabilities. This study aims to address these security challenges by analyzing the vulnerabilities in satellite networks similar to the Iridium system, which includes inter-satellite links (ISL) and routers on each satellite [9]-[12].

Previous research has identified various potential security attacks on satellite networks and proposed different solutions. However, these solutions often lack comprehensive effectiveness and robustness [13]-[18]. Satellite communication security issues are increasingly significant as reliance on satellite systems grows across various sectors, including defense, telecommunications, and navigation. One major concern is the susceptibility to cyberattacks, such as jamming, spoofing, and interception [19]-[24]. Jamming involves deliberately sending signals to disrupt communication, potentially leading to the loss of crucial data or services. Spoofing, on the other hand, entails sending false signals to deceive the receiver, which can mislead navigation systems or compromise data integrity. Interception of satellite signals can also result in unauthorized access to sensitive information, posing a severe threat to national security and commercial interests [25]-[30].

Another critical security issue is the physical vulnerability of satellites. Satellites are exposed to various threats, including space debris, anti-satellite weapons, and natural space weather phenomena like solar flares [31]. The destruction or incapacitation of a satellite can lead to significant disruptions in communication networks, impacting everything from everyday internet use to critical military operations [32]. Additionally, the complex supply chain involved in satellite manufacturing and launching presents security challenges, as components sourced from various global suppliers may introduce risks of sabotage or espionage. Addressing these security issues requires robust cybersecurity measures, international cooperation, and the development of resilient satellite technologies to ensure the continued reliability and safety of satellite communication systems [33]-[36].

This study reviews existing security measures and proposes enhancements to improve their effectiveness. The findings indicate significant vulnerabilities in current systems but also highlight that with targeted improvements, security can be substantially enhanced. These enhancements are crucial for supporting critical global communications and services, such as broadband Internet and data services, thereby enhancing their reliability and user trust. while the evolution of satellite communications from Sputnik 1 to modern systems has been marked by remarkable technological advancements and commercial successes, addressing the security challenges remains essential for the continued growth and reliability of satellite networks [37], [38]. This study contributes to this ongoing effort by providing a detailed analysis of current vulnerabilities and proposing effective solutions to safeguard the future of satellite communications.

1.1. Objectives of the Paper

The objective of this research paper is:

- To provide a comprehensive analysis of satellite networks, focusing on their general characteristics, privacy and security issues,
- Review current solutions addressing privacy and security concerns.
- Propose potential future research directions in satellite network security and privacy.

2. Methodology

This study aims to analyze and enhance the security mechanisms of Low Earth Orbit (LEO) satellite networks, focusing on a system architecture similar to the Iridium satellite network. The methodology began with a review of existing literature on satellite network security, analyzing current LEO systems, to understand their architecture, operational protocols, and known security vulnerabilities, along with previous research on potential security attacks and existing countermeasures. A detailed analysis of the Iridium system architecture was performed, focusing on its key components such as inter-satellite links (ISL), terrestrial gateways, and satellite routers to identify critical points of vulnerability. From this, a list of potential security threats specific to LEO satellite networks was compiled, including threats such as jamming, spoofing, eavesdropping, and cyber-attacks on satellite routers and gateways.

3. Satellite System infrastructure

There are many groups of items that enable a satellite infrastructure to work. A detailed examination is needed to understand the operation of the overall system [39]. An example diagram representation of a satellite system is shown in Figure 1, with numerous components shown explicitly [40].

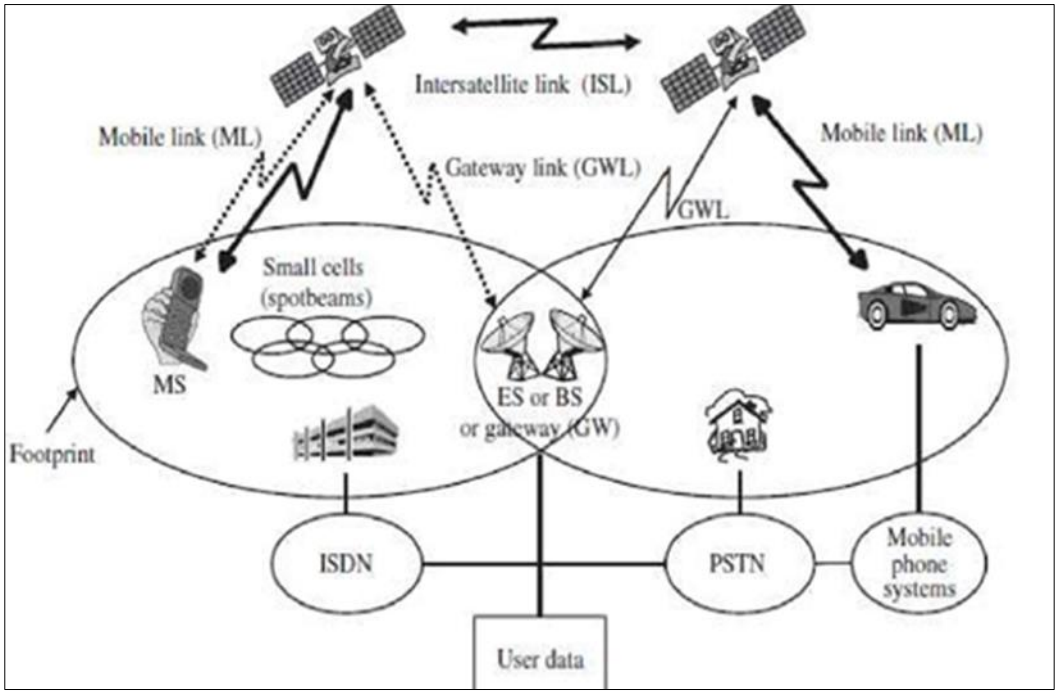

Figure 1 A representation of a satellite system

Once a contact has been established between a mobile system and a satellite using a LOS beam, almost everyone in the world can be accessed, using the underlying hardware backbone network [41] on the surface of the earth. The satellites are controlled by the base stations (BS) located at the surface of the earth [42], which serve as a gateway. Inter-satellite links can be used to relay information from one satellite to another, but they are still controlled by the ground BS (also known as earth station or ES). The illuminated area of a satellite beam, called a footprint, is the area within which a mobile user can communicate with the satellite; many beams are used to cover a wide area. In addition, satellites are constantly rotating around the earth, and a beam may be temporarily blocked either due to other flying objects or the

terrain of the earth's surface. Therefore, a redundancy concept, known as diversity, is used to transmit the same message through more than one satellite, as shown in the above figure.

The basic idea behind path diversity is to provide a mechanism that can combine two or more correlated information signals (primarily the same copy) traveling along different paths and hence having uncorrected noise and/or fading characteristics [43], [44]. Such a combination of two signals improves signal quality, which enables the receiver to have flexibility in selecting a better quality signal. The primary interest is with path diversity, though other forms of diversity such as antenna, time, frequency, field, or code, are possible. Path diversity will depend on the technology that is used to transmit and receive messages [45], [46]. The use of diversity can be initiated by either the MS or the BS located on earth. The diversity request from the BS (ES) enables the MS to locate and scan un-shadowed satellite paging channels for unobstructed communication.

The use of satellite path diversity may be primarily due to the following conditions: Elevation angle: Higher elevation angle decreases shadowing problems. One approach is to initiate path diversity when the elevation angle becomes less than a predefined threshold. Signal quality: If the average signal level (in DB), quality (in BER) [47], or fade duration goes beyond some threshold, then path diversity can be used. Signal quality is a function of parameters such as elevation angle, available capacity, current mobility pattern of the MS, or anticipated future demand. Stand-by option: A channel can be selected and reserved as a stand-by for diversity whenever a threshold crossing is detected by the MS [48]. Such a standby channel is used only when the primary channel is obstructed. Since the use of diversity is considered a rare event, several MSs can share the same standby channel. Emergency handoff: Whenever a connection of a MS with a satellite is lost, the MS tries to have an emergency handoff.

4. Architecture of Satellite Networks

The ES (BS) constitutes the heart of the overall system control, performing functions similar to the BSS of a cellular wireless system. The ES keeps track of all MSs located in the area and controls the allocation and de-allocation of radio resources, including the use of frequency bands or channels in FDMA, time slots for TDMA, and code assignments for CDMA [49]. Both MSC and VLR are important parts of the BS and provide functions akin to those in a cellular network. The database EIR (Equipment Identity Register), AUC (Authentication Center), and HLR also perform the same operations as in conventional wireless systems and are integral to the overall satellite system [50]. Figure 2 shows the block diagram of a typical satellite communication system.

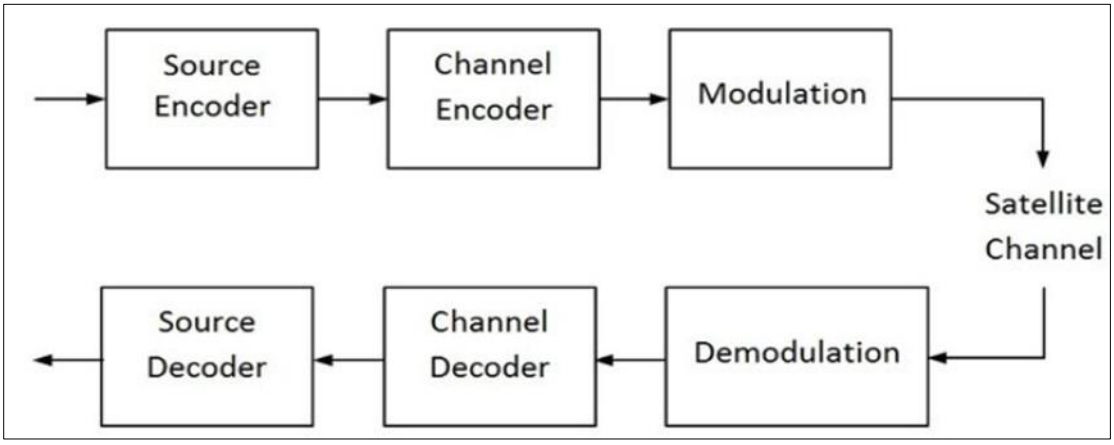

Figure 2 Satellite communication system block diagram

The HLR-VLR (Home Location Register - Visitor Location Register) pair supports the basic process of mobility management. A satellite user mapping register (SUMR) is maintained at the BS to track the locations of all satellites and indicate the satellite assigned to each MS [51], [52]. All these systems are associated with the BS to minimize the weight of satellites, which essentially function as relay stations with worldwide coverage, given that most of the intelligence and decision-making processes [53] are performed by the BS. These BSs are also connected to the PSTN (Public Switching Telephone Network) and ATM backbone through the appropriate gateway, enabling calls to regular household phones as well as cellular devices to be routed and established [54], [55].

Several additional situations are present for handoff in satellite systems as compared with cellular wireless networks, primarily due to the movement of satellites and the wider coverage area. Various types of handoff can be summarized as shown in Table 1 [56]:

Table 1 Handoff process and performance impact

Handoff types	**Performance Impact**
Intra - satellite handoff	There could be handoff from one spot beam to another due to relative movement of the MS with respect to the satellites because the MS needs to be in the footprint area to communicate with a satellite. Therefore MS moves to the footprint path of another beam, there would be an intra-satellite handoff [57].
Inter - satellite handoff	Since the MS is mobile and most satellites are not geosynchronous, the beam path may change periodically. Therefore, there could be a handoff from one satellite to another satellite under control of the BS [58].
BS handoff	A rearrangement in frequency may be desirable to balance the traffic in neighboring beams or the interference [59] with other systems. There could be situations in which satellite control may change from one BS to another because of their relative locations. This may cause a handoff at the BS level, even though the MS may still be in the footprint of current satellite [60]-[65].
Inter-system handoff	There could be a handoff from a satellite network to a terrestrial cellular network, which would be cheaper and would have a lower latency.

4.1. Hierarchical Layers

Satellite networks inherently have a hierarchical structure with satellites at the vertex. In this paper, we divide the satellite networks into three layers as shown in Figure 3 below.

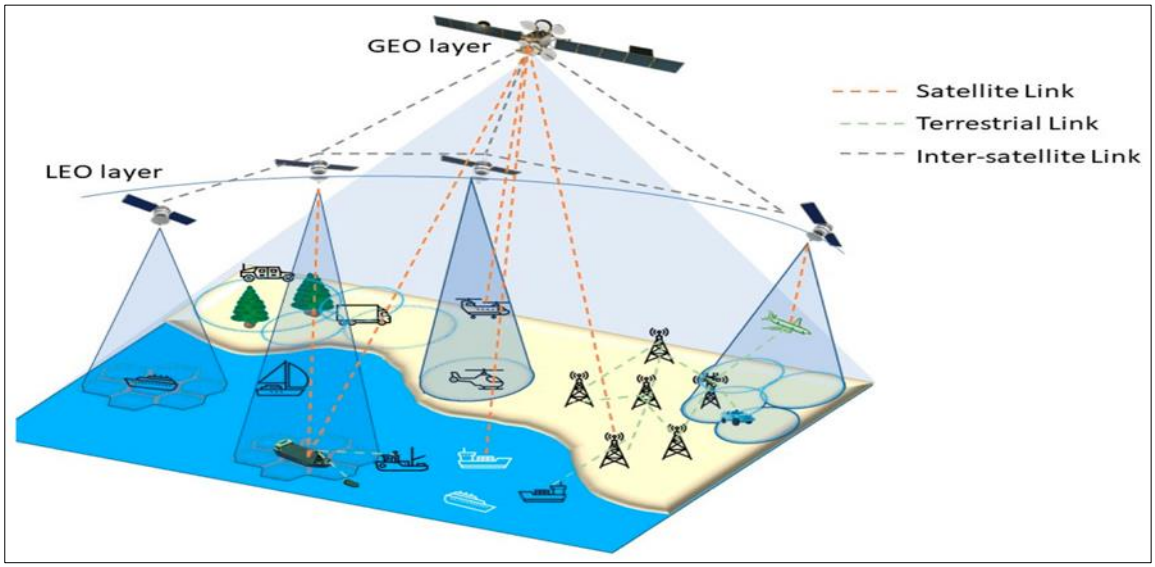

Figure 3 Satellite communication system hierarchical layers

Multi-layered satellite system concept consisting of GEO and LEO satellites. Users are shown to be aerial and ground-based vehicles and devices including ships. The GEO satellite provides coverage for the whole area while LEO system coverages are pointed to specific locations.

4.1.1. Satellite Layer

The first layer is the satellite layer, which consists of Low Earth Orbit (LEO) satellites interconnected by Inter-Satellite Links (ISLs). At any given point on Earth, there are at least two beams from different satellites covering the area [66],

[67]. This structure provides enhanced reliability and capacity. Despite being more expensive and complicated, redundancy, broadband, and security are necessary for future satellite networks. This may be one of the feasible structures we can adopt.

Generally, a satellite system contains no more than 100 satellites, and each satellite beam covers no more than 100 terrestrial users (TUs). Therefore, the routing table in each satellite is short, and the consumption of the root selection process is limited, resulting in low routing table traffic.

4.1.2. Terrestrial Unit Layer

The second layer is the terrestrial unit layer. It comprises microwave antennas, routers, and other auxiliary equipment. These units have wireless links connecting satellites to terrestrial units. As shown in Figure 1, each terrestrial unit has multiple Satellite-Earth links, establishing connections with different LEO satellites [68], [69]. Terrestrial units also maintain wireless or wired links to various terminals such as telephones, computers, and TV sets. Some terrestrial units have direct links to the Internet, making all satellite networks integral parts of the Internet.

There may be thousands of Terminal Links (TMLs) under one terrestrial unit (TU) [70], [71]. The computing power of a single TU can be substantial, allowing it to manage and coordinate TMLs efficiently, thus reducing the computational burden [72] on the satellites.

4.1.3. Terminal Layer

The third layer is the terminal layer, consisting of various mobile or fixed terminals supported by terrestrial units [73], [74]. These terminals include familiar devices such as telephones, computers, and TV sets, as well as other devices not yet prevalent but expected to become common in the future. A common feature of all these terminals is that they have protocol stacks to support various services. Mobile terminals within a limited distance can form ad hoc networks, allowing them to exchange information directly.

5. Security Issues in Satellite Networks

Satellite networks, essential for global communications, navigation, and data transmission, face significant security challenges. These challenges stem from the inherent vulnerabilities of satellite systems, which include the potential for cyber-attacks, signal jamming, and unauthorized access to sensitive data. The vast distances and reliance on complex infrastructure further complicate the implementation of robust security measures. Ensuring the security of satellite networks is crucial, as breaches can disrupt critical services, compromise national security, and impact commercial operations. Therefore, a comprehensive approach to cybersecurity is essential to safeguard these vital assets against an ever-evolving array of threats.

5.1. Security Threats

With the development of satellite communication networks, greater attention must be paid to their security as the satellite segment is vulnerable to various attacks [75]. These security-related challenges include considerations of confidentiality, availability, integrity, and non-repudiation [76]-[79]. Figure 4 shows typical security threats in satellite communication systems.

5.1.1. Eavesdropping and Confidentiality

Satellite channels are wireless broadcast media, making it easy for unauthorized users to intercept the signal and eavesdrop on the communication if it is not encrypted [80]-[82]. Therefore, data transferred via satellite networks must be encrypted. There are two types of encryption algorithms [83], [84]:

- *Symmetric Key Algorithms:* Examples include the well-known DES and AES algorithms [85].
- *Asymmetric Key Algorithms:* Examples include RSA, ECC, and ElGamal cryptography [86].

5.1.2. Sophistication and Integrity

When traffic traverses' open networks, an adversary can intercept data messages and modify them before sending them to the destination, which could be the satellite, ground terminals, or mobile users. The intended recipient would then believe the corrupted message is from the true source [87]-[89]. To prevent message modification, message-integrity check mechanisms should be appended to every message. Examples of these mechanisms include message authentication codes (MACs) [90]-[92]. Common algorithms used for message authentication are MD5 and SHA.

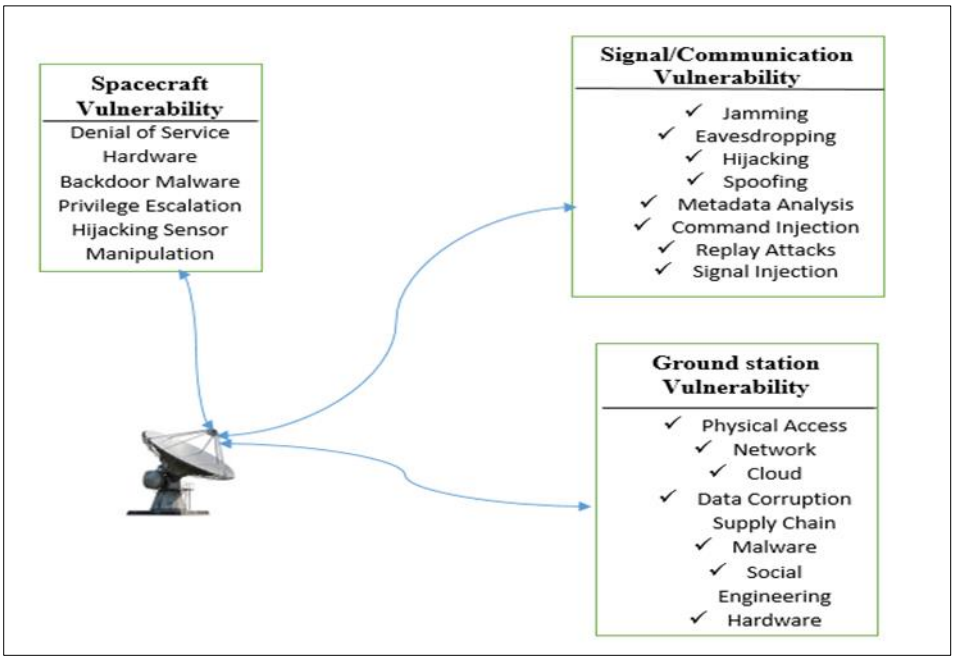

Figure 4 Satellite System Vulnerabilities and Related Threats

5.1.3. Masquerade or Repudiation and Digital Signature

An adversary with the appropriate equipment can impersonate legitimate users and send fraudulent messages to spacecraft, causing them to perform unintended operations [93], [94]. This can disrupt legitimate operations and communications within the network. Repudiation occurs when one party involved in a contract, particularly one agreed upon via the Internet, later denies their participation. These attacks can be prevented if the sources of the messages are properly authenticated by every receiver [95]-[98]. If the satellite authenticates the source of every message it receives, it will only transmit messages with verified sources. Suitable signature systems for this purpose include RSA, ElGamal, and Schnorr [99].

5.1.4. Denial-of-Service (DoS) Attack

Strong security mechanisms, such as those used for message integrity checks or user authentication, can sometimes facilitate other types of security attacks. For example, if a satellite performs authentication and integrity checks on all messages before broadcasting, an adversary can exploit this by sending a large number of spurious messages to the satellite [100], [101]. Figure 5 shows a typical DoS attack in satellite systems.

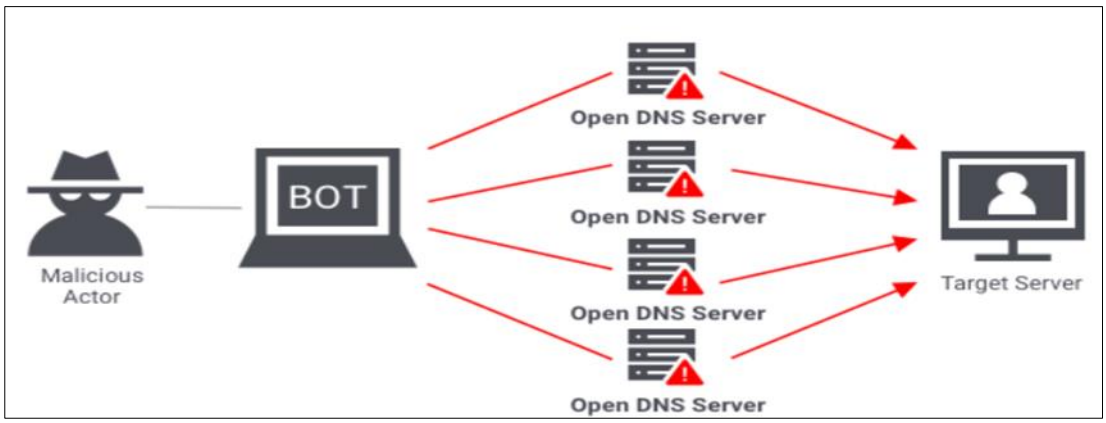

Figure 5 DoS attack in satellite systems

This would force the satellite to spend significant computational resources processing these fake messages. Given the satellite's limited processing power, such an attack can be highly effective, particularly if robust cryptographic

mechanisms like digital signatures are used for authentication and message integrity. This type of attack is known as a denial-of-service (Dos) attack [102]-[104].

6. Privacy issues in Satellite Networks

Privacy issues in satellite networks are a significant concern due to the vast amount of data transmitted and the potential for unauthorized access [105]-[106]. Satellite communications can be intercepted by unauthorized parties, as signals are broadcast over large areas and susceptible to eavesdropping by malicious entities with the necessary hardware. Unauthorized access to satellite networks can lead to data breaches, with hackers exploiting vulnerabilities in the satellite or ground station infrastructure [111]. Table 2 presents a summary of the privacy issues in satellite systems.

Table 2 Security Issues and Corresponding Solutions

Privacy issues	Description
Data Interception	Satellite communications can be intercepted by unauthorized parties. Since satellite signals are broadcast over large areas, they are susceptible to eavesdropping by malicious entities equipped with the necessary hardware to capture the signals [112]-[116].
Unauthorized Access	There is a risk of unauthorized access to satellite networks, which can lead to data breaches. Hackers can exploit vulnerabilities in the satellite or ground station infrastructure to gain access to sensitive information [117]-[122].
Signal Jamming and Spoofing	Jamming involves disrupting the communication signals between satellites and ground stations, while spoofing involves sending false signals to mislead receivers. Both activities can compromise the integrity and confidentiality of the data being transmitted [123]-[128].
Data Encryption	While encryption can protect data in transit, weaknesses in encryption protocols or key management can be exploited. If encryption keys are compromised, the confidentiality of the data is at risk [129]-[134].
Tracking and Surveillance	Satellites can be used to monitor and track individuals, vehicles, and other assets, raising concerns about surveillance and privacy [135]-[140]. The ability to gather detailed imagery and location data can be misused for unauthorized tracking
Data Storage and Retention	Satellite networks often involve storing large amounts of data, either in orbit or at ground stations [141], [142]. Ensuring that this data is stored securely and is not retained longer than necessary is crucial to maintaining privacy [143]-[146].
Physical Security	Ground stations and other infrastructure supporting satellite networks must be physically secure to prevent tampering or unauthorized access that could compromise the privacy and integrity of the network [147].

Addressing these privacy issues requires a multifaceted approach, including implementing robust encryption and authentication protocols, ensuring regulatory compliance, enhancing physical and cyber security measures, and fostering transparency and user awareness [148]. By taking these steps, the privacy of data transmitted via satellite networks can be better protected.

7. Performance issues in Satellite Networks

Performance issues in satellite networks stem from various factors that can affect the quality, reliability, and efficiency of communications. One major issue is latency, which is inherent in satellite communication due to the long distances signals must travel between the Earth and satellites [149], [150]-[152]. This delay can affect real-time applications such as voice calls, video conferencing, and online gaming. Bandwidth limitations are another concern, as the available spectrum for satellite communications is limited, leading to potential congestion and reduced data transmission speeds. Signal attenuation and degradation caused by atmospheric conditions like rain, snow, and storms can also impair performance, leading to intermittent connectivity or reduced signal quality [153], [154].

Interference from other electronic devices and competing signals in densely populated frequency bands can further degrade performance. The Doppler effect, caused by the relative motion between satellites and ground stations, can

impact the frequency of signals and require constant adjustment to maintain effective communication [155]. Additionally, the handoff process, where communication transitions from one satellite to another as they move in and out of range, can introduce brief interruptions or delays if not managed efficiently [156]. Figure 6 shows the interaction and interference in satellite-terrestrial communication systems. Interference in satellite-terrestrial communication systems arises when unwanted signals disrupt the transmission and reception of legitimate signals. This interference can stem from various sources, including other satellites, terrestrial wireless networks, and natural phenomena like solar flares. In densely populated frequency bands, the competition for spectrum usage intensifies the risk of interference, leading to signal degradation, loss of data, and reduced communication quality. Both intentional interference, such as jamming, and unintentional interference, caused by overlapping frequency channels or equipment malfunctions, pose significant challenges to maintaining reliable satellite-terrestrial communication. Managing interference requires a multifaceted approach involving technical, regulatory, and operational strategies. Technically, advancements in signal processing, adaptive filtering, and frequency coordination can mitigate interference effects. Regulatory bodies play a crucial role by establishing and enforcing spectrum management policies to minimize conflicts between satellite and terrestrial systems. Operationally, continuous monitoring and dynamic spectrum allocation help in identifying and addressing interference sources promptly. Collaboration among international organizations, governments, and industry stakeholders is essential to develop and implement effective solutions, ensuring the seamless coexistence of satellite and terrestrial communication networks.

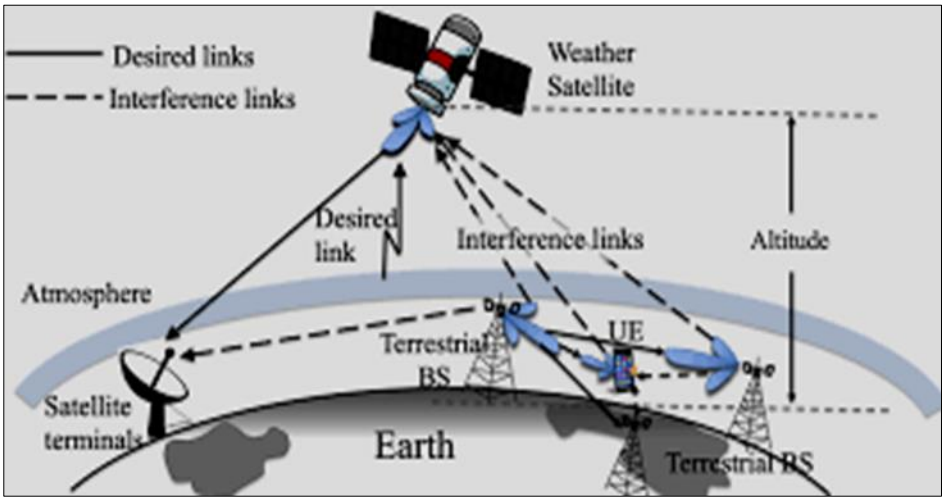

Figure 6 Interference in Satellite-Terrestrial Communication Systems

Power limitations on satellites restrict their ability to boost signal strength, impacting the range and reliability of communications. Network management challenges, including the allocation and de-allocation of resources, also play a critical role in ensuring optimal performance, especially as the number of users and devices grows [157]-[159]. Table 3 gives a summary of the performance issues in satellite systems.

Table 3 Performance issues and their causes

Issue	**Description**
Latency	Long distances between Earth and satellites
Bandwidth Limitations	Limited spectrum availability
Signal Attenuation	Atmospheric conditions (rain, snow, storms)
Interference	Competing signals, other electronic devices
Doppler Effect	Relative motion between satellites and ground stations
Handoff Interruptions	Transition of communication from one satellite to another
Power Limitations	Restricted power availability on satellites
Network Management	Resource allocation and deallocation challenges

Integration Issues	Synchronization and coordination with terrestrial networks

The integration and compatibility of satellite networks with terrestrial networks are crucial for seamless communication, yet they often face challenges in synchronization and coordination [160]. Addressing these performance issues requires advances in satellite technology, improved network management practices, better integration with terrestrial systems, and the development of adaptive algorithms to optimize resource allocation and signal management in dynamic conditions.

8. Discussion

The recent advancements in satellite networks have garnered significant interest due to their extensive geographic coverage and flexible deployment capabilities, offering a promising solution for global communications and transforming traditional communication methods. As shown in Figure 7, the ability to provide connectivity to remote and underserved regions has positioned satellite networks as a critical component in achieving global communication goals.

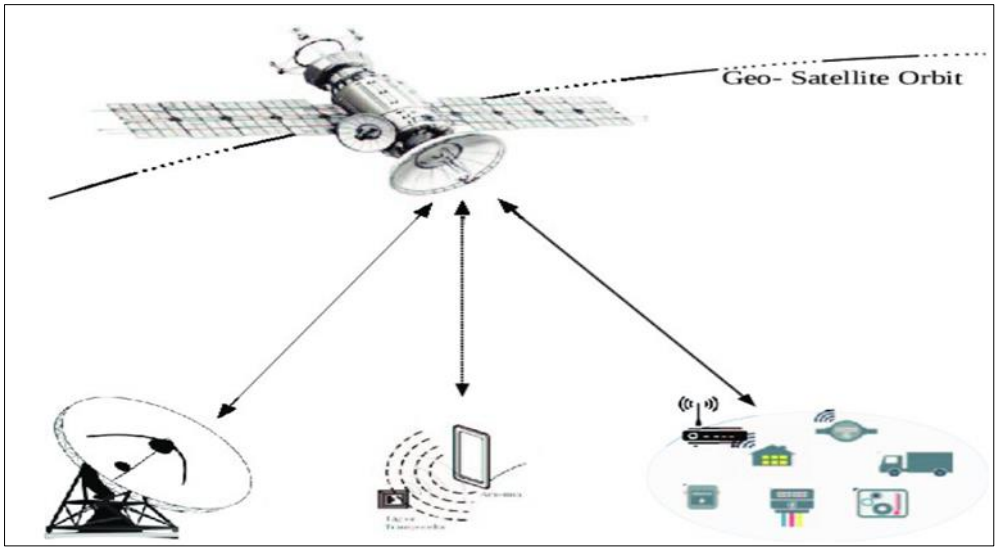

Figure 7 Satellite for remote communication

However, despite these advancements, current satellite systems face significant challenges that need to be addressed to maximize their potential [161], [162]. These challenges include high propagation delays, inadequate coverage of high-latitude regions, and various technical and financial constraints. Geostationary (GEO) satellite systems, which maintain a fixed position relative to the Earth's surface, are advantageous for providing continuous coverage over specific areas. However, they suffer from high propagation delays due to their distance from the Earth, which can be as much as 35,786 kilometers. This latency can be particularly problematic for real-time applications such as voice calls, video conferencing, and online gaming. Moreover, GEO systems struggle with providing adequate coverage in high-latitude regions due to the low elevation angles at which satellites appear in the sky, leading to signal degradation and increased susceptibility to atmospheric interference [163].

Low Earth Orbit (LEO) satellite systems, such as the Iridium network, offer a promising alternative to GEO systems by orbiting much closer to the Earth, typically at altitudes between 500 and 2,000 kilometers. This proximity significantly reduces propagation delays, making LEO systems more suitable for latency-sensitive applications. Additionally, LEO satellites provide better coverage at high latitudes, as their lower orbits allow for more favorable elevation angles. However, LEO systems face their own set of challenges, including the need for a large number of satellites to ensure continuous global coverage and the complexities associated with managing frequent handoffs as satellites move rapidly across the sky. Furthermore, financial difficulties have historically plagued LEO systems, as seen with the Iridium network, highlighting the significant investment required for deployment and maintenance [164]. Security issues in satellite networks have become increasingly critical as these networks adopt IP protocols and hybrid configurations that integrate terrestrial nodes and satellite links [165], [166]. The reliance on IP protocols exposes satellite networks to a wide range of cyber threats, including eavesdropping, data interception, jamming, spoofing, and denial-of-service

(DoS) attacks [167]-[171]. Eavesdropping and data interception are particularly concerning, given the broadcast nature of satellite communications, which makes it easier for unauthorized parties to capture and analyze transmitted data. To mitigate these threats, robust encryption mechanisms must be implemented to protect data integrity and confidentiality. However, encryption alone is not sufficient; comprehensive security frameworks are needed to address the diverse range of potential attacks.

Previous research has identified various potential security attacks on satellite networks and proposed different solutions. However, these solutions often lack comprehensive effectiveness and robustness. For instance, while encryption can protect data in transit, it does not address the risk of physical tampering with satellite hardware or ground stations [172]. Similarly, while authentication mechanisms can prevent unauthorized access, they can also introduce vulnerabilities if not properly managed. Denial-of-service (DoS) attacks, which can overwhelm satellite systems with spurious traffic, are particularly challenging to defend against due to the limited processing power of satellites [173]-[177]. To enhance the security of satellite networks, it is essential to adopt a multi-layered approach that combines encryption, authentication, intrusion detection, and response mechanisms. Our methodology involves analyzing the security vulnerabilities in satellite networks similar to the Iridium system, which includes inter-satellite links (ISL) and routers on each satellite. By conducting a detailed analysis of the Iridium system architecture, we aim to identify critical points of vulnerability and propose targeted improvements to enhance security. This includes evaluating existing security measures, such as encryption protocols and authentication mechanisms, and assessing their effectiveness in real-world scenarios. Additionally, we explore advanced security techniques, such as quantum cryptography and Blockchain technology, which have the potential to provide stronger protection against emerging threats.

The results indicate significant vulnerabilities in current systems but also show that with targeted improvements, security can be substantially enhanced. For example, the use of quantum cryptography can provide theoretically unbreakable encryption, ensuring data integrity and confidentiality even in the face of sophisticated cyber-attacks [178]-[181]. Similarly, Blockchain technology can enhance the security of satellite networks by providing a decentralized and tamper-proof ledger for tracking and verifying transactions. By integrating these advanced security techniques [182] with existing measures, it is possible to create a more resilient and robust security framework for satellite networks [183]. The implications of this study are profound, suggesting that more secure satellite networks can better support critical global communications and services, including broadband Internet and data services, thereby enhancing their reliability and user trust. Improved security can also enable the deployment of satellite networks in sensitive and high-risk environments, such as military operations and disaster recovery efforts, where the confidentiality and integrity of communications are paramount. Furthermore, enhancing the security of satellite networks can facilitate the development of new applications and services, such as remote healthcare, precision agriculture, and smart cities, which rely on reliable and secure connectivity.

8.1. Solutions to security issues in Satellite Networks

To address the security issues in satellite networks, various solutions can be implemented to enhance data protection, prevent unauthorized access, and ensure reliable communication. Strong encryption protocols such as AES and RSA, end-to-end encryption, and secure key management are essential to protect against data interception [184]-[188]. Multi-factor authentication, robust access control policies, and intrusion detection systems can mitigate unauthorized access.

To combat signal jamming, spread spectrum techniques, frequency hopping, and jamming detection and mitigation strategies are effective [189], [190]. Authenticating signal sources, employing cryptographic verification, and using robust signal processing algorithms can prevent signal spoofing. Regular updates of encryption standards, the use of quantum-resistant algorithms like lattice-based cryptography, and secure key distribution are necessary to address encryption weaknesses [191]-[194]. Implementing strict data access controls, anonymizing user data, and employing privacy-preserving technologies can reduce risks related to tracking and surveillance. Table 4 shows some of the security issues and their probable solutions.

Table 4 Security Issues and Corresponding Solutions

Security Issue	Solution(s)
Data Interception	Strong encryption protocols (e.g., AES, RSA), end-to-end encryption, and secure key management [195], [196].
Unauthorized Access	Multi-factor authentication (MFA), robust access control policies, and intrusion detection systems (IDS) [197].
Signal Jamming	Spread spectrum techniques, frequency hopping, and jamming detection and mitigation strategies [198].
Signal Spoofing	Authentication of signal sources, cryptographic verification, and robust signal processing algorithms [199]
Encryption Weaknesses	Regular updates of encryption standards, use of quantum-resistant algorithms, and secure key distribution [200].
Tracking and Surveillance	Implementing strict data access controls, anonymizing user data, and employing privacy-preserving technologies [201].
Data Storage Security	Encrypted storage, regular audits, and adherence to data retention policies [202].
Regulatory Compliance	Compliance with international standards (e.g., GDPR, HIPAA), and regular compliance audits [203].
Physical Security	Secure ground stations, physical access controls, and surveillance systems [204].

Ensuring secure data storage with encrypted storage solutions, regular audits, and adherence to data retention policies is crucial [205], [206]. Compliance with international standards such as GDPR and HIPAA [207], along with regular compliance audits, helps meet regulatory requirements [208]. Physical security measures, including secure ground stations, physical access controls, and surveillance systems, are vital to prevent unauthorized physical access. By adopting these comprehensive solutions, satellite network operators can significantly mitigate security risks and protect the integrity, confidentiality, and availability of their communications.

8.2. Solutions to privacy issues in satellite networks

To address privacy issues in satellite networks, various solutions can be implemented to protect data and ensure user privacy [209]-[212]. Implementing strong encryption protocols, such as AES and end-to-end encryption, is essential for safeguarding data transmissions from interception and unauthorized access. Employing multi-factor authentication and robust access control measures can prevent unauthorized access to network resources [213]. To minimize signal jamming and spoofing risks, spread spectrum techniques, frequency hopping, and signal authentication can be utilized. Anonymizing user data and employing privacy-preserving technologies can address concerns related to tracking and surveillance, ensuring that user identities and locations are protected [214]. Secure data storage practices, including encrypted storage and strict data retention policies, are crucial for maintaining data confidentiality and integrity [215] –[218].

Regular compliance with international data protection regulations, such as GDPR and HIPAA, ensures that satellite networks adhere to legal standards for data privacy and security [219], [220]. Implementing privacy-by-design principles, where privacy considerations are integrated into the design and operation of satellite networks from the outset, can further enhance data protection. Educating users about privacy practices and obtaining informed consent for data collection and usage can improve transparency and trust. Additionally, developing and deploying quantum-resistant encryption algorithms, such as lattice-based cryptography, can future-proof satellite networks against emerging threats posed by quantum computing [221], [222].

Network monitoring and intrusion detection systems can help detect and respond to potential privacy breaches in real-time [223]. Ensuring the physical security of ground stations and other infrastructure components through secure facilities, access controls [224], and surveillance systems is also vital. By adopting these comprehensive solutions, satellite network operators can effectively address privacy issues, ensuring the protection of user data and maintaining the privacy and security of communications.

8.3. Solutions to performance issues in satellite networks

Addressing performance issues in satellite networks requires a multifaceted approach that targets various aspects of network operation and infrastructure [225], [226]. Implementing advanced error correction and data compression techniques can mitigate latency and bandwidth limitations, ensuring more efficient use of available resources [227], [228]. Utilizing higher frequency bands, such as Ka and Ku bands [229], can provide greater bandwidth and improve data transmission speeds [230], though they require more sophisticated ground station equipment [231]. Adaptive modulation and coding (AMC) techniques can dynamically adjust the signal parameters based on real-time conditions, optimizing the trade-off between data rate and signal quality [232], [233]. Employing multiple-input multiple-output (MIMO) technology can enhance signal strength and reliability by using multiple antennas at both the transmitter and receiver ends [234], [235]. To counter signal attenuation caused by atmospheric conditions, techniques like adaptive power control and the use of diverse transmission paths can be employed, ensuring more robust communication during adverse weather conditions [236], [237].

Deploying inter-satellite links (ISLs) allows for the relay of data between satellites, reducing the dependency on ground stations and improving network resilience and efficiency [238]. Utilizing low Earth orbit (LEO) satellite constellations, which are closer to the Earth compared to geostationary satellites, can significantly reduce latency and enhance real-time communication capabilities [239]. Improving handoff mechanisms between satellites ensures seamless communication transitions, especially for users in high-mobility environments [240]. This can be achieved through predictive algorithms and machine learning techniques that anticipate and prepare for handoff events. Enhancing power efficiency on satellites through advanced solar power technology and energy-efficient hardware can extend the operational life of satellites and maintain consistent signal strength [241], [242].

Effective network management, including sophisticated load balancing and resource allocation algorithms, can prevent congestion and optimize network performance [243]. Integration with terrestrial networks through hybrid satellite-terrestrial architectures can leverage the strengths of both systems, providing seamless connectivity and improving overall performance [244]. Investing in research and development of new technologies, such as optical satellite communications (laser-based), can offer higher data rates and reduced interference compared to traditional radio frequency (RF) communications (140). Continuous monitoring and analysis of network performance metrics can help in identifying bottlenecks and implementing targeted improvements [245].

9. Research gaps

Addressing performance issues in satellite networks is crucial, but there remain significant research gaps that need to be explored to further enhance the reliability, efficiency, and quality of these networks [246]-[249]. While low Earth orbit (LEO) constellations help reduce latency, there is a need for more research on optimizing routing algorithms and protocols to minimize delays further, including combining LEO, medium Earth orbit (MEO), and geostationary orbit (GEO) satellites for optimal latency reduction. Research is also needed on advanced bandwidth allocation techniques that can dynamically adjust to changing network conditions and user demands, exploring new frequency bands and spectrum-sharing strategies to maximize bandwidth utilization. Further studies on adaptive modulation and coding (AMC) techniques [250] are essential to counteract signal degradation due to atmospheric conditions, and advanced materials and technologies for satellite antennas and ground stations could improve signal resilience. Additionally, more sophisticated interference detection and mitigation techniques, particularly as the number of satellites and frequency usage increases, are needed, including machine learning algorithms for real-time interference identification and mitigation [251].

10. Future research directions

Future research directions in satellite networks should focus on advancing several key areas to enhance performance, security, and overall effectiveness. One significant direction is the development of more sophisticated routing algorithms and protocols optimized for low Earth orbit (LEO), medium Earth orbit (MEO), and geostationary orbit (GEO) satellite constellations to further reduce latency and improve data transmission efficiency [252]-[254]. Researchers should also explore innovative bandwidth allocation techniques that dynamically adjust to network conditions and user demands, leveraging new frequency bands and spectrum-sharing strategies to maximize utilization. Advancements in adaptive modulation and coding (AMC) techniques, such as the one shown in Figure 8, are necessary to mitigate signal degradation caused by atmospheric conditions, while the exploration of advanced materials and technologies for satellite antennas and ground stations can enhance signal resilience. Investigating machine learning and artificial intelligence (AI)-based methods [255] for real-time interference detection and mitigation will be crucial as satellite networks become more congested. Improved handoff mechanisms using predictive analytics and machine learning can

ensure seamless transitions between satellites, reducing latency and packet loss, particularly in high-mobility environments [256].

Research should focus on developing energy-efficient hardware and power management systems for satellites, including advanced solar power technologies and novel energy storage solutions, to extend operational life and maintain consistent performance. Integrating satellite and terrestrial networks through standardized protocols and hybrid architectures, along with exploring the potential of 5G and future network technologies, will be vital for seamless connectivity [257]-[259]. Optical (laser-based) communication systems offer promising high data rates and reduced interference, but further research is needed to address challenges related to atmospheric interference and alignment precision [260].

The development of quantum-resistant encryption algorithms and advanced cybersecurity measures is essential to safeguard satellite communications against emerging threats, alongside privacy-preserving technologies and frameworks to protect user data [261]-[264]. Future research should also focus on advanced network management tools that utilize AI and machine learning for automated resource allocation, fault detection, and performance optimization, as well as the application of self-organizing networks (SON) in satellite communication systems [265].

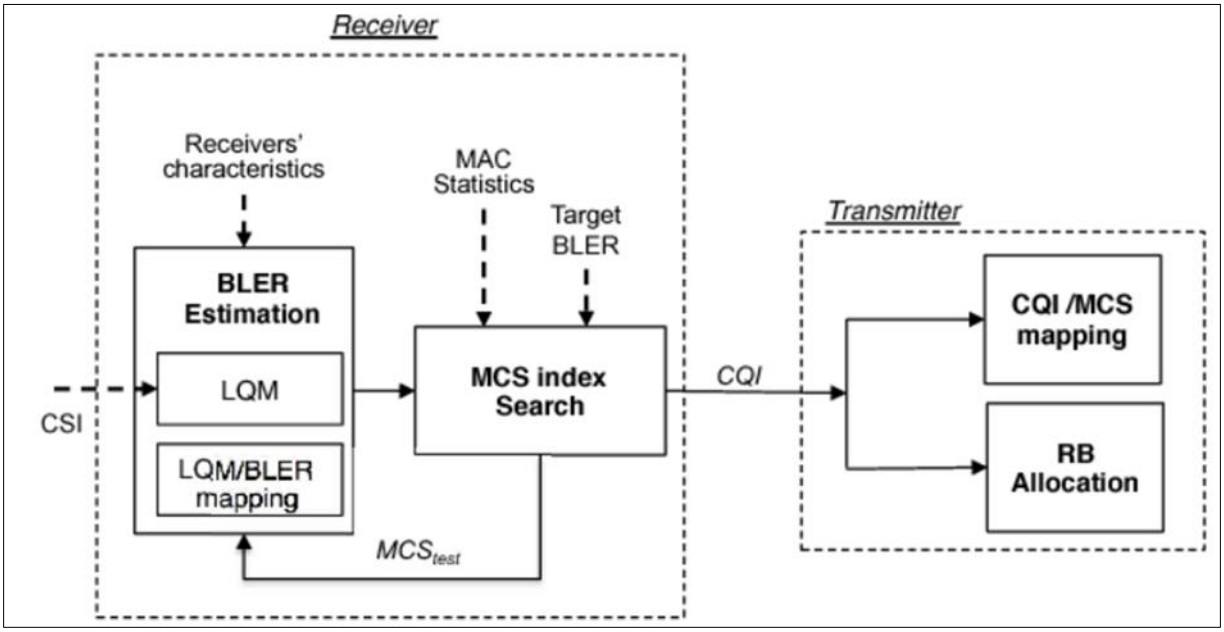

Figure 8 Advancements in adaptive modulation and coding

Innovations in user terminal designs that are affordable, efficient, and capable of handling higher data rates, including compact, energy-efficient antennas and advanced modulation schemes, will enhance user experience. Additionally, as the number of satellites and users' increases, scalable network architectures and protocols that can manage increased traffic without compromising performance must be developed, exploring decentralized network models and Blockchain technologies for satellite communication networks. By pursuing these future research directions, the satellite communication industry can achieve significant advancements, ensuring robust, efficient, and secure global connectivity.

11. Conclusion

Addressing the performance issues in satellite networks necessitates a comprehensive and forward-thinking approach. Future research should focus on developing advanced routing algorithms, innovative bandwidth allocation techniques, and adaptive modulation and coding strategies to enhance signal resilience and optimize data transmission. Machine learning and artificial intelligence will play pivotal roles in real-time interference detection, handoff management, and network optimization. Energy efficiency and power management advancements are crucial for extending satellite operational life, while integrating satellite and terrestrial networks and exploring new communication technologies like optical systems will ensure seamless and high-speed connectivity. Robust cybersecurity measures, including quantum-resistant encryption and privacy-preserving frameworks, will protect user data and maintain the integrity of satellite

communications. Scalable network architectures and user-friendly terminal designs will accommodate the growing number of satellites and users, ensuring efficient and reliable performance. By focusing on these research directions, the satellite communication industry can achieve significant advancements, ensuring robust, efficient, and secure global connectivity for the future.

Compliance with ethical standards

Acknowledgments

I would like to thank all my friends who supported me when developing this paper.

References

[1] Sputnik [Internet]. Nasa.gov. 2024 [cited 2024 Jul 11]. Available from: https://www.nasa.gov/history/sputnik/index.html

[2] The Launch of Sputnik, 1957 [Internet]. State.gov. 2024 [cited 2024 Jul 11]. Available from: https://2001-2009.state.gov/r/pa/ho/time/lw/103729.htm

[3] The story of Sputnik: how one soviet satellite changed everything [Internet]. History Skills. 2014 [cited 2024 Jul 11]. https://www.historyskills.com/classroom/year-10/sputnik/

[4] Pelton JN. History of Satellite Communications. Springer eBooks [Internet]. 2015 Jan 1 [cited 2024 Jul 11], 1–41.

[5] Ahmad I, Suomalainen J, Porambage P, Gurtov A, Huusko J, Höyhtyä M. Security of satellite-terrestrial communications: Challenges and potential solutions. IEEE Access. 2022 Sep 8, 10:96038-52.

[6] Kumar S, Chinthaginjala R, Anbazhagan R, Nyangaresi VO, Pau G, Varma PS. Submarine Acoustic Target Strength Modelling at High-Frequency Asymptotic Scattering. IEEE Access. 2024 Jan 1.

[7] Kang M, Park S, Lee Y. A Survey on Satellite Communication System Security. Sensors. 2024 May 1, 24(9):2897.

[8] Ali A, Ali A. Securing Space-Based Satellite Networks: Challenges and Solutions. EasyChair, 2024 Jan 20.

[9] Security Attacks Against the Availability of Low Earth Orbit Satellite Networks [Internet]. Acm.org.2023[cited2024Jul11].Availablefrom:https://dl.acm.org/doi/fullHtml/10.1145/3638837.3638847

[10] Satellite Communications, Globalization, and the Cold War on JSTOR [Internet]. Jstor.org. 2024 [cited 2024 Jul 11]. Available from: https://www.jstor.org/stable/25147905

[11] Satellite System Infrastructure - Javatpoint [Internet]. www.javatpoint.com. 2021 [cited 2024 Jul 11]. Available from: https://www.javatpoint.com/satellite-system-infrastructure

[12] 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.

[13] Kota S, Pahlavan K, Leppanen PA. Broadband Satellite Communications for Internet Access [Internet]. ResearchGate. Kluwer, 2004 [cited 2024 Jul 11]. Available from: https://www.researchgate.net/publication/220693238_Broadband_Satellite_Communications_for_Internet_Access

[14] Suf Barzam. SATELLITE INFRASTRUCTURE [Internet]. ISI. 2022 [cited 2024 Jul 11]. Available from: https://imagesatintl.com/satellite-infrastructure/

[15] Salim S, Moustafa N, Reisslein M. Cybersecurity of Satellite Communications Systems: A Comprehensive Survey of the Space, Ground, and Links Segments. IEEE Communications Surveys & Tutorials. 2024 Jun 3.

[16] Okafor ES, Akinrinola O, Usman FO, Amoo OO, Ochuba NA. Cybersecurity analytics in protecting satellite telecommunications networks: a conceptual development of current trends, challenges, and strategic responses. International Journal of Applied Research in Social Sciences. 2024 Mar 8, 6(3):254-66.

[17] Ashraf I, Narra M, Umer M, Majeed R, Sadiq S, Javaid F, Rasool N. A deep learning-based smart framework for cyber-physical and satellite system security threats detection. Electronics. 2022 Feb 21, 11(4):667.

[18] 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).

[19] Chang E. Introduction to Satellite Network Architecture – Telecomworld101.com [Internet]. Telecomworld101.com. 2024 [cited 2024 Jul 11]. Available from: https://telecomworld101.com/introduction-satellite-network/

[20] Dharma Prakash Agrawal. Embedded Sensor Systems. SpringerLink [Internet]. 2017 [cited 2024 Jul 11], Available from: https://link.springer.com/book/10.1007/978-981-10-3038-3

[21] Esho AO, Iluyomade TD, Olatunde TM, Igbinenikaro OP. A comprehensive review of energy-efficient design in satellite communication systems. International Journal of Engineering Research Updates. 2024, 6(02):013-25.

[22] Höyhtyä M, Boumard S, Yastrebova A, Järvensivu P, Kiviranta M, Anttonen A. Sustainable satellite communications in the 6G era: A European view for multilayer systems and space safety. IEEE Access. 2022 Sep 15, 10:99973-100005.

[23] Jhanjhi NZ, Gaur L, Khan NA. Global Navigation Satellite Systems for Logistics: Cybersecurity Issues and Challenges. Cybersecurity in the Transportation Industry. 2024 Jul 10:49-67.

[24] Nyangaresi VO. Exten ded 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.

[25] Huso I, Olivieri M, Galgano L, Rashid A, Piro G, Boggia G. Design and implementation of a looking-forward Lawful Interception architecture for future mobile communication systems. Computer Networks. 2024 Jul 1, 249:110518.

[26] Shaikhanov Z, Badran S, Guerboukha H, Jornet J, Mittleman D, Knightly E. MetaFly: Wireless Backhaul Interception via Aerial Wavefront Manipulation. In2024 IEEE Symposium on Security and Privacy (SP) 2024 Feb 1 (pp. 154-154). IEEE Computer Society.

[27] Pu H, He L, Cheng P, Chen J, Sun Y. CORMAND2: A Deception Attack Against Industrial Robots. Engineering. 2024 Jan 1, 32:186-201.

[28] Omar AA, Soudan B, Altaweel A. UOS_IOTSH_2024: A Comprehensive Network Traffic Dataset for Sinkhole Attacks in Diverse RPL IoT Networks. Data in Brief. 2024 Jun 22:110650.

[29] Skraparlis AN, Ntalianis KS, Tsapatsoulis N. A novel framework to intercept GPS-denied, bomb-carrying, non-military, kamikaze drones: Towards protecting critical infrastructures. Defence Technology. 2024 May 9.

[30] 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.

[31] Righini M, Gatti I, Taramelli A, Arosio M, Valentini E, Sapio S, Schiavon E. Integrated Flood Impact and Vulnerability Assessment Using a Multi-Sensor Earth Observation Mission with the Perspective of an Operational Service in Lombardy, Italy. Land. 2024 Jan 26, 13(2):140.

[32] Büyüksalih G, Gazioğlu C. Editorial for a Special Issue: Assessment of Coastal Vulnerability to Sea Level Rise Using Remote Sensing. PFG–Journal of Photogrammetry, Remote Sensing and Geoinformation Science. 2024 Jul 4:1-2.

[33] Vizzarri A, Mazzenga F, Giuliano R. Future technologies for train communication: the role of LEO HTS satellites in the adaptable communication system. Sensors. 2022 Dec 21, 23(1):68.

[34] Ochuba NA, Olutimehin DO, Odunaiya OG, Soyombo OT. Sustainable business models in satellite telecommunications. Engineering Science & Technology Journal. 2024 Mar 24, 5(3):1047-59.

[35] Turner LA, Jahankhani H. An investigation into an approach to updating the governance of satellite communications to enhance cyber security. InCybersecurity, Privacy and Freedom Protection in the Connected World: Proceedings of the 13th International Conference on Global Security, Safety and Sustainability, London, January 2021 2021 May 21 (pp. 23-33). Cham: Springer International Publishing.

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

[37] Olariu S, Ali Rizvi SR, Shirhatti R, Todorova P. Q-Win–A new admission and handoff management scheme for multimedia LEO satellite networks. Telecommunication systems. 2003 Jan, 22:151-68.

[38] Aris S, Sadouni S, Benslama M. A new concept of Satellite Telecommunication Mobility scenarios with the context of intra-handover control management. International journal of Communications. 2018 Jan 15, 3.

[39] Liu S, Lin J, Xu L, Gao X, Liu L, Jiang L. A dynamic beam shut off algorithm for LEO multibeam satellite constellation network. IEEE Wireless Communications Letters. 2020 Jun 16, 9(10):1730-3.

[40] Deng X, Chang L, Zeng S, Cai L, Pan J. Distance-based back-pressure routing for load-balancing leo satellite networks. IEEE Transactions on Vehicular Technology. 2022 Sep 14, 72(1):1240-53.

[41] 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.

[42] Höyhtyä M, Anttonen A, Majanen M, Yastrebova-Castillo A, Varga M, Lodigiani L, Corici M, Zope H. Multi-Layered Satellite Communications Systems for Ultra-High Availability and Resilience. Electronics. 2024 Mar 29, 13(7):1269.

[43] Ouyang M, Zhang R, Wang B, Liu J, Huang T, Liu L, Tong J, Xin N, Yu FR. Network Coding-Based Multi-Path Transmission for LEO Satellite Networks With Domain Cluster. IEEE Internet of Things Journal. 2024 Mar 19.

[44] Xu W, Jiang M, Tang F, Yang Y. Network coding-based multi-path routing algorithm in two-layered satellite networks. Iet Communications. 2018 Jan, 12(1):2-8.

[45] Bhosale V, Saeed A, Bhardwaj K, Gavrilovska A. A characterization of route variability in leo satellite networks. InInternational Conference on Passive and Active Network Measurement 2023 Mar 10 (pp. 313-342). Cham: Springer Nature Switzerland.

[46] Wrona A, Tantucci A. Artificial intelligence-based data path control in low Earth orbit satellites-driven optical communications. International Journal of Satellite Communications and Networking. 2024.

[47] 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).

[48] Radhakrishnan R, Edmonson WW, Afghah F, Rodriguez-Osorio RM, Pinto F, Burleigh SC. Survey of inter-satellite communication for small satellite systems: Physical layer to network layer view. IEEE Communications Surveys & Tutorials. 2016 May 9, 18(4):2442-73.

[49] Kopacz JR, Herschitz R, Roney J. Small satellites an overview and assessment. Acta Astronautica. 2020 May 1, 170:93-105.

[50] Kong Q, Wang Y, Ma M, Qu X, Bao H. A secure location management scheme in an LEO-satellite network with dual-mobility. Peer-to-Peer Networking and Applications. 2024 Jun 21:1-3.

[51] Jiang B, Hu X. Security issues in satellite networks. InSecond International Conference on Space Information Technology 2007 Nov 10 (Vol. 6795, pp. 1157-1163). SPIE.

[52] Box F, Snow RE, Chen A, Bodie SR, Globus L, Luc TS. Frequency assignment function for unmanned-aircraft command and control links. In2018 Integrated Communications, Navigation, Surveillance Conference (ICNS) 2018 Apr 10 (pp. 4C2-1). IEEE.

[53] 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.

[54] Naser ZL, Murih BK, Alhamd MW. Qualitative Indicator of Growth of Segments of the Network with Various Service Disciplines. InInternational Conference on Frontiers of Intelligent Computing: Theory and Applications 2023 Apr 11 (pp. 433-440). Singapore: Springer Nature Singapore.

[55] Ali SR, Ali SR. Reliability analysis of VoIP system. Next Generation and Advanced Network Reliability Analysis: Using Markov Models and Software Reliability Engineering. 2019:211-44.

[56] Kodheli X, Solaija MS, Arslan H. Performance Comparison of Handover Mechanisms for LEO Networks in S and Ka-bands. In2024 IEEE Wireless Communications and Networking Conference (WCNC) 2024 Apr 21 (pp. 1-6). IEEE.

[57] Li B, Fei Z, Zhou C, Zhang Y. Physical-layer security in space information networks: A survey. IEEE Internet of things journal. 2019 Sep 26, 7(1):33-52.

[58] Sahu DN. Cutting-Edge Communication: Integrated Satellite Aerial for 6G Networks. In2024 IEEE International Conference on Big Data & Machine Learning (ICBDML) 2024 Feb 24 (pp. 79-85). IEEE.

[59] 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.

[60] Mahajan P, Zaheeruddin. Handoffs in Next-Generation Wireless Networks. InProceedings of International Conference on Communication and Artificial Intelligence: ICCAI 2021 2022 May 10 (pp. 49-59). Singapore: Springer Nature Singapore.

[61] Warrier A, Aljaburi L, Whitworth H, Al-Rubaye S, Tsourdos A. Future 6G communications powering vertical handover in non-terrestrial networks. IEEE Access. 2024 Feb 29.

[62] Zhang Y, Wang J, Li Q, Chen J, Feng H, He S. Joint Communication, Sensing, and Computing in Space–Air–Ground Integrated Networks: System Architecture and Handover Procedure. IEEE Vehicular Technology Magazine. 2024 Mar 18.

[63] Haldorai A, Lincy RB, Suriya M, Balakrishnan M. Satellite-terrestrial Integrated Computing and Artificial Intelligence as a Means of Achieving Handover Management. In2024 IEEE International Conference on Computing, Power and Communication Technologies (IC2PCT) 2024 Feb 9 (Vol. 5, pp. 874-877). IEEE.

[64] Chen K, Zhang L, Zhong J. Vertical Handover Strategy in Satellite-Aerial Based Emergency Communication Networks. InProceeding of 11th International Conference on Wireless Networks and Mobile Communications 2024 May 7. IEEE.

[65] Nyangaresi VO, Al Sibahee MA, Abduljabbar ZA, Alhassani A, Abduljaleel IQ, Abood EW. Intelligent Target Cell Selection Algorithm for Low Latency 5G Networks. InAdvances in Computational Intelligence and Communication: Selected Papers from the 2nd EAI International Conference on Computational Intelligence and Communications (CICom 2021) 2022 Dec 14 (pp. 79-97). Cham: Springer International Publishing.

[66] Hamamreh JM, Furqan HM, Arslan H. Classifications and applications of physical layer security techniques for confidentiality: A comprehensive survey. IEEE Communications Surveys & Tutorials. 2018 Oct 25, 21(2):1773-828.

[67] Driessen B. Eavesdropping on satellite telecommunication systems. Cryptology EPrint Archive. 2012.

[68] Gebotys CH, Gebotys CH. Data Integrity and Message Authentication. Security in Embedded Devices. 2010:143-61.

[69] Hou Y, Li M, Chauhan R, Gerdes RM, Zeng K. Message integrity protection over wireless channel by countering signal cancellation: Theory and practice. InProceedings of the 10th ACM Symposium on Information, Computer and Communications Security 2015 Apr 14 (pp. 261-272).

[70] [42] Wu X, Du Y, Fan T, Guo J, Ren J, Wu R, Zheng T. Threat analysis for space information network based on network security attributes: a review. Complex & Intelligent Systems. 2023 Jun, 9(3):3429-68.

[71] [43] Diro A, Kaisar S, Vasilakos AV, Anwar A, Nasirian A, Olani G. Anomaly detection for space information networks: A survey of challenges, techniques, and future directions. Computers & Security. 2024 Apr 1, 139:103705.

[72] 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.

[73] Mahjabin T, Xiao Y, Sun G, Jiang W. A survey of distributed denial-of-service attack, prevention, and mitigation techniques. International Journal of Distributed Sensor Networks. 2017 Dec, 13(12):1550147717741463.

[74] Kua J, Loke SW, Arora C, Fernando N, Ranaweera C. Internet of things in space: a review of opportunities and challenges from satellite-aided computing to digitally-enhanced space living. Sensors. 2021 Dec 4, 21(23):8117.

[75] Qu Z, Zhang G, Cao H, Xie J. LEO satellite constellation for Internet of Things. IEEE access. 2017 Aug 4, 5:18391-401.

[76] Baselt G, Strohmeier M, Pavur J, Lenders V, Martinovic I. Security and privacy issues of satellite communication in the avlatlon domain. In2022 14th International Conference on Cyber Conflict: Keep Moving!(CyCon) 2022 May 31 (Vol. 700, pp. 285-307). IEEE.

[77] Roy-Chowdhury A, Baras JS, Hadjitheodosiou M, Papademetriou S. Security issues in hybrid networks with a satellite component. IEEE wireless communications. 2005 Dec 19, 12(6):50-61.

[78] Oyewole OO, Fakeyede OG, Okeleke EC, Apeh AJ, Adaramodu OR. Security considerations and guidelines for augmented reality implementation in corporate environments. Computer Science & IT Research Journal. 2023, 4(2):69-84.

[79] 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.

[80] Ahmed S, Khan M. Securing the Internet of Things (IoT): A comprehensive study on the intersection of cybersecurity, privacy, and connectivity in the IoT ecosystem. AI, IoT and the Fourth Industrial Revolution Review. 2023 Sep 16, 13(9):1-7.

[81] Kota SL. Multimedia satellite networks: Issues and challenges. Multimedia Systems and Applications. 1999 Jan 22, 3528:600-18.

[82] Kota SL. Broadband satellite networks: trends and challenges. InIEEE Wireless Communications and Networking Conference, 2005 2005 Mar 13 (Vol. 3, pp. 1472-1478). IEEE.

[83] Tornatore M, Andre J, Babarczi P, Braun T, Folstad E, Poul Heegaard, et al. A survey on network resiliency methodologies against weather-based disruptions. The Digital Library of Polytechnic Institute of Bragança (Polytechnic Institute of Bragança) [Internet]. 2016 Sep 1 [cited 2024 Jul 11], Available from: https://ieeexplore.ieee.org/abstract/document/7608264

[84] Katayama M, Ogawa A, Morinaga N. Earth satellite communication systems with low orbits, and effects of the doppler shift. Electronics and Communications in Japan (Part I: Communications). 1994 Aug, 77(8):59-69.

[85] 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.

[86] Kapoor J, Thakur D. Analysis of symmetric and asymmetric key algorithms. InICT analysis and applications 2022 (pp. 133-143). Springer Singapore.

[87] Mass J, Vassy E. Doppler effect of artificial satellites. InAdvances in Space Science and Technology 1962 Jan 1 (Vol. 4, pp. 1-38). Elsevier.

[88] Shayea I, Dushi P, Banafaa M, Rashid RA, Ali S, Sarijari MA, Daradkeh YI, Mohamad H. Handover management for drones in future mobile networks—A survey. Sensors. 2022 Aug 25, 22(17):6424.

[89] Rao UH. Challenges of implementing network management solution. International Journal of Distributed and Parallel Systems. 2011 Sep 1, 2(5):67.

[90] Javed F, Afzal MK, Sharif M, Kim BS. Internet of Things (IoT) operating systems support, networking technologies, applications, and challenges: A comparative review. IEEE Communications Surveys & Tutorials. 2018 Mar 21, 20(3):2062-100.

[91] Wang P, Zhang J, Zhang X, Yan Z, Evans BG, Wang W. Convergence of satellite and terrestrial networks: A comprehensive survey. IEEE access. 2019 Dec 31, 8:5550-88.

[92] 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.

[93] Roy-Chowdhury A, Baras JS, Hadjitheodosiou M, Papademetriou S. Security issues in hybrid networks with a satellite component. IEEE wireless communications. 2005 Dec 19, 12(6):50-61.

[94] Ahmad I, Suomalainen J, Porambage P, Gurtov A, Huusko J, Höyhtyä M. Security of satellite-terrestrial communications: Challenges and potential solutions. IEEE Access. 2022 Sep 8, 10:96038-52.

[95] Banerjee K, Saha S. Blockchain Signatures to Ensure Information Integrity and Non-Repudiation in the Digital Era: A comprehensive study. International Journal of Computing and Digital Systems. 2024 Mar 23, 16(1):1-2.

[96] Rakhra M, Singh A, Singh D. Digital Signature Verification In Cloud Computing. In2024 11th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions)(ICRITO) 2024 Mar 14 (pp. 1-6). IEEE.

[97] Zhu L, Liu D, Yu L, Xie Y, Wang M. Content integrity and non-repudiation preserving audio-hiding scheme based on robust digital signature. Security and Communication Networks. 2013 Nov, 6(11):1331-43.

[98] 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.

[99] Liu Y, Ning P, Dai H. Authenticating primary users' signals in cognitive radio networks via integrated cryptographic and wireless link signatures. In2010 IEEE symposium on security and privacy 2010 May 16 (pp. 286-301). IEEE.

[100] Panigrahi L, Pattanayak BK, Mohanty B, Pattnaik S, Habboush AK. A Smart Secure model for Detection of DDoS Malicious Traces in Integrated LEO Satellite-Terrestrial Communications. International Journal of Electrical and Electronics Research. 2024 May 30, 12(2):503-11.

[101] Toubi A, Hajami A. Vulnerability Assessment and Mitigation Strategies for Satellite Communication Systems Under DDoS Attacks. In2024 International Conference on Global Aeronautical Engineering and Satellite Technology (GAST) 2024 Apr 24 (pp. 1-8). IEEE.

[102] Tedeschi P, Sciancalepore S, Di Pietro R. Satellite-based communications security: A survey of threats, solutions, and research challenges. Computer Networks. 2022 Oct 24, 216:109246.

[103] Lu T, Ding X, Shang J, Zhao P, Zhang H. DoSat: A DDoS Attack on the Vulnerable Time-Varying Topology of LEO Satellite Networks. InInternational Conference on Applied Cryptography and Network Security 2024 Feb 29 (pp. 265-282). Cham: Springer Nature Switzerland.

[104] 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.

[105] Ahmad I, Suomalainen J, Porambage P, Gurtov A, Huusko J, Höyhtyä M. Security of satellite-terrestrial communications: Challenges and potential solutions. IEEE Access. 2022 Sep 8, 10:96038-52.

[106] Fareed M, Yassin AA. Privacy-preserving multi-factor authentication and role-based access control scheme for the E-healthcare system. Bulletin of Electrical Engineering and Informatics. 2022 Aug 1, 11(4):2131-41.

[107] Alturki N, Aljrees T, Umer M, Ishaq A, Alsubai S, Saidani O, Djuraev S, Ashraf I. An Intelligent Framework for Cyber–Physical Satellite System and IoT-Aided Aerial Vehicle Security Threat Detection. Sensors. 2023 Aug 14, 23(16):7154.

[108] Tedeschi P, Al Nuaimi FA, Awad AI, Natalizio E. Privacy-aware remote identification for unmanned aerial vehicles: current solutions, potential threats, and future directions. IEEE Transactions on Industrial Informatics. 2023 Jun 5, 20(2):1069-80.

[109] 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.

[110] 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.

[111] Sodagari S. Integrating quantum and satellites: A new era of connectivity. IEEE Access. 2023 Dec 18.

[112] Oliveira S, Cunha J, Nóbrega RL, Gash JH, Valente F. Enhancing global rainfall interception loss estimation through vegetation structure modeling. Journal of Hydrology. 2024 Mar 1, 631:130672.

[113] Galliford K. Legalities of Spying From Satellites and High Altitude Balloons. Contemporary Issues in Air and Space Power. 2024 Jan 29, 2(1):bp35753434.

[114] Dong M, Liu S, Jiang R, Qi J, de Solan B, Comar A, Li L, Li W, Ding Y, Baret F. Comparing and combining data-driven and model-driven approaches to monitor wheat green area index with high spatio-temporal resolution satellites. Remote Sensing of Environment. 2024 May 1, 305:114118.

[115] Li J, Li X, Li C, Wang C, He J. A Review of LEO Satellite Network Security Research. In2023 2nd International Conference on Data Analytics, Computing and Artificial Intelligence (ICDACAI) 2023 Oct 17 (pp. 496-501). IEEE.

[116] 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.

[117] Casaril F, Galletta L. Securing SatCom user segment: A study on cybersecurity challenges in view of IRIS2. Computers & Security. 2024 May 1, 140:103799.

[118] Bace B, Gökce Y, Tatar U. Law in orbit: International legal perspectives on cyberattacks targeting space systems. Telecommunications Policy. 2024 May 1, 48(4):102739.

[119] Willbold J, Sciberras F, Strohmeier M, Lenders V. Satellite Cybersecurity Reconnaissance: Strategies and their Real-world Evaluation. In2024 IEEE Aerospace Conference 2024 Mar 2 (pp. 1-13). IEEE.

[120] Varadharajan V, Suri N. Security challenges when space merges with cyberspace. Space Policy. 2024 Feb 1, 67:101600.

[121] Madani P, McGregor C. Cybersecurity Issues in Space Optical Communication Networks and Future of Secure Space Health Systems. In2024 IEEE Aerospace Conference 2024 Mar 2 (pp. 1-8). IEEE.

[122] 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.

[123] Radoš K, Brkić M, Begušić D. Recent Advances on Jamming and Spoofing Detection in GNSS. Sensors. 2024 Jun 28, 24(13):4210.

[124] Zhang J, Cui X, Xu H, Lu M. A two-stage interference suppression scheme based on antenna array for GNSS jamming and spoofing. Sensors. 2019 Sep 7, 19(18):3870.

[125] Morrison A, Sokolova N, Solberg A, Gerrard N, Rødningsby A, Hauglin H, Rødningen T, Dahlø T. Jammertest 2022: Jamming and Spoofing Lessons Learned. Engineering Proceedings. 2023 Oct 29, 54(1):22.

[126] Naganawa J, Chomel C, Koga T, Miyazaki H, Kakubari Y. Jamming and spoofing protection for ADS-B mode S receiver through array signal processing. InAir Traffic Management and Systems III: Selected Papers of the 5th ENRI International Workshop on ATM/CNS (EIWAC2017) 5 2019 (pp. 184-204). Springer Singapore.

[127] Khan SZ, Mohsin M, Iqbal W. On GPS spoofing of aerial platforms: a review of threats, challenges, methodologies, and future research directions. PeerJ Computer Science. 2021 May 6, 7:e507.

[128] 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.

[129] Yin Y, Liu J, Cong D, Wei Z, Liu L, Sun D. Design of Geographic Information Data Transmission System Based on Satellite Communication. In2024 IEEE 6th Advanced Information Management, Communicates, Electronic and Automation Control Conference (IMCEC) 2024 May 24 (Vol. 6, pp. 421-429). IEEE.

[130] Murtaza A, Pirzada SJ, Hasan MN, Xu T, Jianwei L. An Efficient Encryption Algorithm for Perfect Forward Secrecy in Satellite Communication. InAdvances in Cyber Security: First International Conference, ACeS 2019, Penang, Malaysia, July 30–August 1, 2019, Revised Selected Papers 1 2020 (pp. 289-302). Springer Singapore.

[131] Hanke F, Unruh J, Karl M, Köster F. Secure Dataspace Approach for Interorbital Satellite Links. InAIAA Scitech 2024 Forum 2024 (p. 0269).

[132] Poomagal CT, Sathish Kumar GA. ECC based lightweight secure message conveyance protocol for satellite communication in internet of vehicles (IoV). Wireless Personal Communications. 2020 Jul, 113(2):1359-77.

[133] Makhloufi AE, Adib SE, Raissouni N. Hardware pipelined architecture with reconfigurable key based on the AES algorithm and hamming code for the earth observation satellite application: Sentinel-2 satellite data case. e-Prime-Advances in Electrical Engineering, Electronics and Energy. 2024 Jun 1, 8:100548.

[134] 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.

[135] ElMarady AA, Rahouma K. High accuracy next generation air traffic surveillance system with potential cyber-attacks. Journal of Advanced Engineering Trends. 2024 Jan 1, 43(1):123-32.

[136] Li W, Li Y, Li H, Chen Y, Wang Y, Lan J, Wu J, Wu Q, Liu J, Lai Z. The dark side of scale: Insecurity of direct-to-cell satellite mega-constellations. In2024 IEEE Symposium on Security and Privacy (SP) 2024 Feb 1 (pp. 149-149). IEEE Computer Society.

[137] Al-Hawawreh M, Moustafa N, Slay J. A threat intelligence framework for protecting smart satellite-based healthcare networks. Neural Computing and Applications. 2024 Jan, 36(1):15-35.

[138] Abro GE, Zulkifli SA, Masood RJ, Asirvadam VS, Laouiti A. Comprehensive review of UAV detection, security, and communication advancements to prevent threats. Drones. 2022 Oct 1, 6(10):284.

[139] Samalla K, Kumar PN. Global Navigation Satellite System in the Civil Surveillance. ACS Journal for Science and Engineering. 2024 Mar 1, 4(1):1-0.

[140] 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.

[141] Guadalupi M, Ferrús R, Ferrer J, Redolfi G, Bernard S. Applications and Business Prospects of Integrated Machine-Type Communications and Satellite Networks. Integration of MTC and Satellites for IoT toward 6G Era. 2024 Jul 4.

[142] Periola A, Alonge A, Ogudo K. Future dynamic multimedia content access via aerial computing system. Multimedia Tools and Applications. 2024 Jan, 83(3):6975-99.

[143] Esho AO, Iluyomade TD, Olatunde TM, Igbinenikaro OP. Nextgeneration materials for space electronics: A conceptual review. Open Access Research Journal of Engineering and Technology. 2024, 6(02):051-62.

[144] Alandihallaj MA, Hein AM. Exploring the Potential of Fractionated Spacecraft for Enhanced Satellite Connectivity: Application to the Satellite-to-Cell Case. Acta Astronautica. 2024 Jul 4.

[145] Bing L, Xiaoyan Y, Tao S, Fuli M, Guangjian Y, Qinsi Y, Lingtong M. A Data Cleaning Algorithm Based on Two-Layer Index for Satellite Big Data. In2024 9th International Conference on Cloud Computing and Big Data Analytics (ICCCBDA) 2024 Apr 25 (pp. 242-250). IEEE.

[146] 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.

[147] Talgat A, Wang R, Kishk MA, Alouini MS. Enhancing Physical Layer Security in LEO Satellite-Enabled IoT Network Communications. arXiv preprint arXiv:2407.04077. 2024 Jul 4.

[148] Sodagari S. Integrating quantum and satellites: A new era of connectivity. IEEE Access. 2023 Dec 18.

[149] Ott D, Peikert C, participants, other workshop. Identifying Research Challenges in Post Quantum Cryptography Migration and Cryptographic Agility [Internet]. arXiv.org. 2019 [cited 2024 Jul 11]. Available from: https://arxiv.org/abs/1909.07353

[150] Anwar S, Mohamad Zain J, Zolkipli MF, Inayat Z, Khan S, Anthony B, Chang V. From intrusion detection to an intrusion response system: fundamentals, requirements, and future directions. algorithms. 2017 Mar 27, 10(2):39.

[151] Pokhrel SR, Choi J. Data-driven satellite communication and control for future iot: Principles and opportunities. IEEE Transactions on Aerospace and Electronic Systems. 2024 Feb 1.

[152] Qiu Z, Ma J, Zhang H, Al Sibahee MA, Abduljabbar ZA, Nyangaresi VO. Concurrent pipeline rendering scheme based on GPU multi-queue and partitioning images. InInternational Conference on Optics and Machine Vision (ICOMV 2023) 2023 Apr 14 (Vol. 12634, pp. 143-149). SPIE.

[153] Niksefat S, Kaghazgaran P, Sadeghiyan B. Privacy issues in intrusion detection systems: A taxonomy, survey and future directions. Computer Science Review. 2017 Aug 1, 25:69-78.

[154] Xu S, Wang XW, Huang M. Software-defined next-generation satellite networks: Architecture, challenges, and solutions. IEEE Access. 2018 Jan 15, 6:4027-41.

[155] Jayasankar U, Thirumal V, Ponnurangam D. A survey on data compression techniques: From the perspective of data quality, coding schemes, data type and applications. Journal of King Saud University-Computer and Information Sciences. 2021 Feb 1, 33(2):119-40. 11], 33(2):119–40.

[156] Abdelsadek MY, Chaudhry AU, Darwish T, Erdogan E, Karabulut-Kurt G, Madoery PG, Yahia OB, Yanikomeroglu H. Future space networks: Toward the next giant leap for humankind. IEEE Transactions on Communications. 2022 Dec 12, 71(2):949-1007.

[157] Zhang L, Wu Z. Machine Learning–Based Adaptive Modulation and Coding Design. Machine Learning for Future Wireless Communications. 2020 Feb 3:157-80.

[158] Chen Y, Davis LM. A cross-layer adaptive modulation and coding scheme for energy efficient software defined radio. Journal of Signal Processing Systems. 2012 Oct, 69:23-30.

[159] 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.

[160] Ishteyaq I, Muzaffar K. Multiple input multiple output (MIMO) and fifth generation (5G): An indispensable technology for sub-6 GHz and millimeter wave future generation mobile terminal applications. International Journal of Microwave and Wireless Technologies. 2022 Sep, 14(7):932-48.

[161] Höyhtyä M, Anttonen A, Majanen M, Yastrebova-Castillo A, Varga M, Lodigiani L, Corici M, Zope H. Multi-Layered Satellite Communications Systems for Ultra-High Availability and Resilience. Electronics. 2024 Mar 29, 13(7):1269.

[162] Fourati F, Alouini MS. Artificial intelligence for satellite communication: A review. Intelligent and Converged Networks. 2021 Sep, 2(3):213-43.

[163] Qu Z, Zhang G, Cao H, Xie J. LEO satellite constellation for Internet of Things. IEEE access. 2017 Aug 4, 5:18391-401.

[164] Yue P, An J, Zhang J, Ye J, Pan G, Wang S, Xiao P, Hanzo L. Low earth orbit satellite security and reliability: Issues, solutions, and the road ahead. IEEE Communications Surveys & Tutorials. 2023 Aug 4.

[165] 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).

[166] Al-Hraishawi H, Chougrani H, Kisseleff S, Lagunas E, Chatzinotas S. A survey on nongeostationary satellite systems: The communication perspective. IEEE Communications Surveys & Tutorials. 2022 Aug 9, 25(1):101-32.

[167] Kumar S, Sharma N. Emerging military applications of free space optical communication technology: A detailed review. InJournal of Physics: Conference Series 2022 (Vol. 2161, No. 1, p. 012011). IOP Publishing.

[168] Pärssinen A, Alouini MS, Berg M, Kürner T, Kyösti P, Leinonen ME, Matinmikko-Blue M, McCune E, Pfeiffer U, Wambacq P. White paper on RF enabling 6G: opportunities and challenges from technology to spectrum.

[169] Manulis M, Bridges CP, Harrison R, Sekar V, Davis A. Cyber security in new space: analysis of threats, key enabling technologies and challenges. International Journal of Information Security. 2021 Jun, 20:287-311.

[170] Yan Y, Han G, Xu H. A survey on secure routing protocols for satellite network. Journal of Network and Computer Applications. 2019 Nov 1, 145:102415.

[171] 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.

[172] Fritz J. Satellite hacking: A guide for the perplexed. Culture Mandala. 2013 Jan 1, 10(1):5906.

[173] Guo W, Xu J, Pei Y, Yin L, Jiang C, Ge N. A distributed collaborative entrance Defense framework against DDoS attacks on satellite internet. IEEE Internet of Things Journal. 2022 May 18, 9(17):15497-510.

[174] Guo H, Li J, Liu J, Tian N, Kato N. A survey on space-air-ground-sea integrated network security in 6G. IEEE Communications Surveys & Tutorials. 2021 Nov 30, 24(1):53-87.

[175] Willis JM, Mills RF, Mailloux LO, Graham SR. Considerations for secure and resilient satellite architectures. In2017 International Conference on Cyber Conflict (CyCon US) 2017 Nov 7 (pp. 16-22). IEEE.

[176] Caini C, Cruickshank H, Farrell S, Marchese M. Delay-and disruption-tolerant networking (DTN): an alternative solution for future satellite networking applications. Proceedings of the IEEE. 2011 Jul 21, 99(11):1980-97.

[177] 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.

[178] Jogenfors J. Breaking the Unbreakable: Exploiting Loopholes in Bell's Theorem to Hack Quantum Cryptography. Linköping University Electronic Press, 2017 Oct 23.

[179] Renner R, Wolf R. Quantum advantage in cryptography. AIAA Journal. 2023 May, 61(5):1895-910.

[180] Sergienko AV. Quantum Cryptography. InQuantum Communications and Cryptography 2018 Oct 3 (pp. 12-26). CRC Press.

[181] Mitra S, Jana B, Bhattacharya S, Pal P, Poray J. Quantum cryptography: Overview, security issues and future challenges. In2017 4th International Conference on Opto-Electronics and Applied Optics (Optronix) 2017 Nov 2 (pp. 1-7). IEEE.

[182] 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.

[183] Kumbhar M, Ng AH, Bandaru S. A digital twin based framework for detection, diagnosis, and improvement of throughput bottlenecks. Journal of manufacturing systems. 2023 Feb 1, 66:92-106.

[184] Yue P, An J, Zhang J, Ye J, Pan G, Wang S, Xiao P, Hanzo L. Low earth orbit satellite security and reliability: Issues, solutions, and the road ahead. IEEE Communications Surveys & Tutorials. 2023 Aug 4.

[185] Çelikbilek K, Saleem Z, Morales Ferre R, Praks J, Lohan ES. Survey on optimization methods for LEO-satellite-based networks with applications in future autonomous transportation. Sensors. 2022 Feb 12, 22(4):1421.

[186] Nabeel M. The many faces of end-to-end encryption and their security analysis. In2017 IEEE international conference on edge computing (EDGE) 2017 Jun 25 (pp. 252-259). IEEE.

[187] Abdmeziem MR, Tandjaoui D. An end-to-end secure key management protocol for e-health applications. Computers & Electrical Engineering. 2015 May 1, 44:184-97.

[188] 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.

[189] Chen S, Sun S, Kang S. System integration of terrestrial mobile communication and satellite communication—the trends, challenges and key technologies in B5G and 6G. China communications. 2020 Dec, 17(12):156-71.

[190] Yuan S, Peng M, Sun Y, Liu X. Software defined intelligent satellite-terrestrial integrated networks: Insights and challenges. Digital Communications and Networks. 2022 Jun 21.

[191] Javaid S, Khalil RA, Saeed N, He B, Alouini MS. Leveraging Large Language Models for Integrated Satellite-Aerial-Terrestrial Networks: Recent Advances and Future Directions. arXiv preprint arXiv:2407.04581. 2024 Jul 5.

[192] Asif R. Post-quantum cryptosystems for Internet-of-Things: A survey on lattice-based algorithms. IoT. 2021 Mar, 2(1):71-91.

[193] Sharma S, Ramkumar KR, Kaur A, Hasija T, Mittal S, Singh B. Post-quantum cryptography: A solution to the challenges of classical encryption algorithms. Modern Electronics Devices and Communication Systems: Select Proceedings of MEDCOM 2021. 2023 Feb 19:23-38.

[194] 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.

[195] Blaise OO, Awodele O, Yewande O. An Understanding and Perspectives of End-To-End Encryption. Int. Res. J. Eng. Technol.(IRJET). 2021, 8(04):1086.

[196] Pérez S, Hernández-Ramos JL, Raza S, Skarmeta A. Application layer key establishment for end-to-end security in IoT. IEEE Internet of Things Journal. 2019 Dec 13, 7(3):2117-28.

[197] Sain M, Normurodov O, Hong C, Hui KL. A survey on the security in cyber physical system with multi-factor authentication. In2021 23rd international conference on advanced communication technology (ICACT) 2021 Feb 7 (pp. 1-8). IEEE.

[198] Xu H, Cheng Y, Wang P. Jamming detection in broadband frequency hopping systems based on multi-segment signals spectrum clustering. IEEE Access. 2021 Feb 16, 9:29980-92.

[199] Zhao C, Huang M, Huang L, Du X, Guizani M. A robust authentication scheme based on physical-layer phase noise fingerprint for emerging wireless networks. Computer networks. 2017 Dec 9, 128:164-71.

[200] 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.

[201] Majeed A, Lee S. Anonymization techniques for privacy preserving data publishing: A comprehensive survey. IEEE access. 2020 Dec 18, 9:8512-45.

[202] Pasquier T, Singh J, Powles J, Eyers D, Seltzer M, Bacon J. Data provenance to audit compliance with privacy policy in the Internet of Things. Personal and Ubiquitous Computing. 2018 Apr, 22:333-44.

[203] Chen JQ, Benusa A. HIPAA security compliance challenges: The case for small healthcare providers. International Journal of Healthcare Management. 2017 Apr 3, 10(2):135-46.

[204] Makri R, Karaivazoglou P, Kyritsis A, Skitsas M, Koutras N, Valera J, Sanchez JM. Modern Innovative Detectors of Physical Threats for Critical Infrastructures. Cyber-physical threat intelligence for critical infrastructures security. 2020:397.

[205] Ahmad I, Suomalainen J, Porambage P, Gurtov A, Huusko J, Höyhtyä M. Security of satellite-terrestrial communications: Challenges and potential solutions. IEEE Access. 2022 Sep 8, 10:96038-52.

[206] 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.

[207] Li B, Fei Z, Zhou C, Zhang Y. Physical-layer security in space information networks: A survey. IEEE Internet of things journal. 2019 Sep 26, 7(1):33-52.

[208] Han S, Li J, Meng W, Guizani M, Sun S. Challenges of physical layer security in a satellite-terrestrial network. IEEE Network. 2022 May 24, 36(3):98-104.

[209] Housen-Couriel D. Cybersecurity threats to satellite communications: Towards a typology of state actor responses. Acta Astronautica. 2016 Nov 1, 128:409-15.

[210] Jianwei L, Weiran L, Qianhong W, Dawei L, Shigang C. Survey on key security technologies for space information networks. Journal of communications and information networks. 2016 Jun, 1(1):72-85.

[211] Kodheli O, Lagunas E, Maturo N, Sharma SK, Shankar B, Montoya JF, Duncan JC, Spano D, Chatzinotas S, Kisseleff S, Querol J. Satellite communications in the new space era: A survey and future challenges. IEEE Communications Surveys & Tutorials. 2020 Oct 1, 23(1):70-109.

[212] 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.

[213] Sharma SK, Chatzinotas S, Arapoglou PD. Satellite communications in the 5G era. Institution of Engineering and Technology, 2018 Sep 7.

[214] Guidotti A, Cioni S, Colavolpe G, Conti M, Foggi T, Mengali A, Montorsi G, Piemontese A, Vanelli-Coralli A. Architectures, standardisation, and procedures for 5G Satellite Communications: A survey. Computer Networks. 2020 Dec 24, 183:107588.

[215] Kodheli O, Lagunas E, Maturo N, Sharma SK, Shankar B, Montoya JF, Duncan JC, Spano D, Chatzinotas S, Kisseleff S, Querol J. Satellite communications in the new space era: A survey and future challenges. IEEE Communications Surveys & Tutorials. 2020 Oct 1, 23(1):70-109.

[216] Xiao Z, Han Z, Nallanathan A, Dobre OA, Clerckx B, Choi J, He C, Tong W. Antenna array enabled space/air/ground communications and networking for 6G. IEEE Journal on Selected Areas in Communications. 2022 Aug 4, 40(10):2773-804.

[217] Panwar N, Sharma S, Gupta P, Ghosh D, Mehrotra S, Venkatasubramanian N. IoT expunge: Implementing verifiable retention of IoT data. InProceedings of the Tenth ACM Conference on Data and Application Security and Privacy 2020 Mar 16 (pp. 283-294).

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

[219] Mao M, Raether Jr R, Lin Y, Pham S, Yee J, Mirza S, Hoffmann J, DiRago M, Witte M, Hoffmeister J. Data privacy: the current legal landscape. Annual Compendium, Ver.. 2018, 1:1.

[220] Koren A, Prasad R. Iot health data in electronic health records (ehr): Security and privacy issues in era of 6g. Journal of ICT Standardization. 2022, 10(1):63-84.

[221] Bi Z, Yung KL, Ip AW, Tang YM, Zhang CW, Da Xu L. The state of the art of information integration in space applications. IEEE Access. 2022 Oct 17, 10:110110-35.

[222] Fidler F, Knapek M, Horwath J, Leeb WR. Optical communications for high-altitude platforms. IEEE Journal of selected topics in quantum electronics. 2010 May 17, 16(5):1058-70.

[223] Gregory M, Heine F, Kämpfner H, Lange R, Lutzer M, Meyer R. Commercial optical inter-satellite communication at high data rates. Optical Engineering. 2012 Mar 1, 51(3):031202-.

[224] 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.

[225] Quantum Computing's Cyber-Threat to National Security on JSTOR [Internet]. Jstor.org. 2020 [cited 2024 Jul 12]. Available from: https://www.jstor.org/stable/26940159

[226] Kumar A, Rathor K, Vaddi S, Patel D, Vanjarapu P, Maddi M. ECG Based Early Heart Attack Prediction Using Neural Networks. In2022 3rd International Conference on Electronics and Sustainable Communication Systems (ICESC) 2022 Aug 17 (pp. 1080-1083). IEEE.

[227] Ajala OA, Arinze CA, Ofodile OC, Okoye CC, Daraojimba AI. Exploring and reviewing the potential of quantum computing in enhancing cybersecurity encryption methods. Magna Scientia Advanced Research and Reviews, 2024, 10(01), 321–329

[228] Chamola V, Jolfaei A, Chanana V, Parashari P, Hassija V. Information security in the post quantum era for 5G and beyond networks: Threats to existing cryptography, and post-quantum cryptography. Computer Communications. 2021 Aug 1, 176:99-118.

[229] Shah SM, Nasir A, Ahmed H. A survey paper on security issues in satellite communication network infrastructure. International Journal of Engineering Research and General Science. 2014 Oct, 2(6):887-900.

[230] 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.

[231] Ahmmed MF, Abdullah AA, Rahman W, Tarek J. Impact of 5g technology on satellite communication: a paradigm shift in telecommunications with a focus on cybersecurity challenges and solutions. International Journal of Science and Engineering. 2024 May 13, 1(2):11-25.

[232] Raghuvanshi D, Kumar S. Cyber and quantum threats to space systems–A study of the restructuring of a modern armed forces. Comparative Strategy. 2024 May 3, 43(3):206-22.

[233] Mukherjee J, Ramamurthy B. Communication technologies and architectures for space network and interplanetary internet. IEEE communications surveys & tutorials. 2012 Jul 25, 15(2):881-97.

[234] Sharawi MS. Advancements in MIMO antenna systems. InDevelopments in antenna analysis and synthesis 2018 (pp. 109-127). IET.

[235] Hussain R, Sharawi MS. 5G MIMO antenna designs for base station and user equipment: Some recent developments and trends. IEEE Antennas and Propagation Magazine. 2021 Jul 9, 64(3):95-107.

[236] 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.

[237] Kaushik S, Agrawal M, Mondal HK, Gade SH, Deb S. Path loss-aware adaptive transmission power control scheme for energy-efficient wireless noc. In2017 IEEE 60th International Midwest Symposium on Circuits and Systems (MWSCAS) 2017 Aug 6 (pp. 132-135). IEEE.

[238] Chen Q, Giambene G, Yang L, Fan C, Chen X. Analysis of inter-satellite link paths for LEO mega-constellation networks. IEEE Transactions on Vehicular Technology. 2021 Feb 9, 70(3):2743-55.

[239] Lai Z, Wu Q, Li H, Lv M, Wu J. Orbitcast: Exploiting mega-constellations for low-latency earth observation. In2021 IEEE 29th International Conference on Network Protocols (ICNP) 2021 Nov 1 (pp. 1-12). IEEE.

[240] Pelton JN, Madry S, Camacho-Lara S. Handbook of satellite applications. Springer Publishing Company, Incorporated, 2017 Jan 3.

[241] Karunanithi V, Rajan RT, Sundaramoorthy P, Verma M, Verhoeven C, Bentum M, McCune EW, Karunanithi V, Rajan RT, Verma M, Verhoeven C. High Data-Rate Inter-Satellite Link (ISL) For Space-Based Interferometry. In70th International Astronautical Congress (IAC), Washington DC 2019 Oct 27.

[242] Grootjans R, Bentum MJ, Brethouwer MF, de Vries RA, van Langen SK. Inter-satellite communication link for a space based interferometer. In64th International Astronautical Congress, IAC 2013 2013 Sep 26 (pp. 1-5). International Astronautical Federation (IAF).

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

[244] Arnon S, Gill E. The optical communication link outage probability in satellite formation flying. Acta Astronautica. 2014 Feb 1, 95:133-40.

[245] Rinaldi L, Camponeschi F, Bogoni A. Space-Grade Analogue and Digital Photonics for Satellite Communications in Europe. Journal of Lightwave Technology. 2023 Nov 6.

[246] Wei T, Feng W, Chen Y, Wang CX, Ge N, Lu J. Hybrid satellite-terrestrial communication networks for the maritime Internet of Things: Key technologies, opportunities, and challenges. IEEE Internet of things journal. 2021 Feb 2, 8(11):8910-34.

[247] Wang P, Zhang J, Zhang X, Yan Z, Evans BG, Wang W. Convergence of satellite and terrestrial networks: A comprehensive survey. IEEE access. 2019 Dec 31, 8:5550-88.

[248] Saeed N, Almorad H, Dahrouj H, Al-Naffouri TY, Shamma JS, Alouini MS. Point-to-point communication in integrated satellite-aerial 6G networks: State-of-the-art and future challenges. IEEE Open Journal of the Communications Society. 2021 Jun 29, 2:1505-25.

[249] 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.

[250] Shanthi KG, Manikandan A. An improved adaptive modulation and coding for cross layer design in wireless networks. Wireless Personal Communications. 2019 Sep, 108:1009-20.

[251] Fraire JA, Céspedes S, Accettura N. Direct-to-satellite IoT-a survey of the state of the art and future research perspectives: Backhauling the IoT through LEO satellites. InInternational Conference on Ad-Hoc Networks and Wireless 2019 Sep 25 (pp. 241-258). Cham: Springer International Publishing.

[252] Zhao N, Long X, Wang J. A multi-constraint optimal routing algorithm in LEO satellite networks. Wireless Networks. 2021 Jun 11:1-2.

[253] Ravishankar C, Gopal R, BenAmmar N, Zakaria G, Huang X. Next-generation global satellite system with mega-constellations. International journal of satellite communications and networking. 2021 Jan, 39(1):6-28.

[254] Li C, Zhang Y, Cui Z, Zhang Y, Liu J, Yu Z, Zhang P. An Overview Of Low Earth Orbit Satellite Routing Algorithms. 2023 International Wireless Communications and Mobile Computing (IWCMC). 2023 Jun 19:866-70.

[255] 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.

[256] Attar A, Tang H, Vasilakos AV, Yu FR, Leung VC. A survey of security challenges in cognitive radio networks: Solutions and future research directions. Proceedings of the IEEE. 2012 Aug 29, 100(12):3172-86.

[257] Zhu X, Jiang C. Integrated satellite-terrestrial networks toward 6G: Architectures, applications, and challenges. IEEE Internet of Things Journal. 2021 Nov 10, 9(1):437-61.

[258] Darwish T, Kurt GK, Yanikomeroglu H, Bellemare M, Lamontagne G. LEO satellites in 5G and beyond networks: A review from a standardization perspective. IEEE Access. 2022 Mar 25, 10:35040-60.

[259] Sun Y, Peng M, Zhang S, Lin G, Zhang P. Integrated satellite-terrestrial networks: Architectures, key techniques, and experimental progress. IEEE Network. 2022 Jul 25, 36(6):191-8.

[260] Kaushal H, Kaddoum G. Applications of lasers for tactical military operations. IEEE Access. 2017 Sep 22, 5:20736-53.

[261] Thanalakshmi P, Rishikhesh A, Marion Marceline J, Joshi GP, Cho W. A quantum-resistant blockchain system: a comparative analysis. Mathematics. 2023 Sep 17, 11(18):3947.

[262] Käppler SA, Schneider B. Post-quantum cryptography: An introductory overview and implementation challenges of quantum-resistant algorithms. Proceedings of the Society. 2022 Jun 20, 84:61-71.

[263] Mao S, Zhang H, Wu W, Liu J, Li S, Wang H. A resistant quantum key exchange protocol and its corresponding encryption scheme. China Communications. 2014 Sep, 11(9):124-34.

[264] Bansod S, Ragha L. Secured and Quantum Resistant key Exchange Cryptography Methods–A Comparison. In2022 Interdisciplinary Research in Technology and Management (IRTM) 2022 Feb 24 (pp. 1-5). IEEE.

[265] Sartori C, Holma H. Self-Organizing Networks (SON). LTE-Advanced: 3GPP Solution for IMT-Advanced. 2012 Aug 24:135-52.