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)

A comprehensive overview of privacy and security issues in deep space networks

Oroo Oyondi Felix *

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

GSC Advanced Research and Reviews, 2024, 20(02), 088–118

Publication history: Received on 25 June 2024; revised on 12 August 2024; accepted on 15 August 2024

Article DOI: https://doi.org/10.30574/gscarr.2024.20.2.0294

Abstract

The National Aeronautics and Space Administration (NASA) Deep Space Network (DSN), managed by the Jet Propulsion Laboratory's Interplanetary Network Directorate, is a critical international network facilitating communication for interplanetary spacecraft missions, radio astronomy, radar astronomy, and related observations. As the largest and most sophisticated telecommunications system globally, the DSN ensures vital communication and data transmission for space missions. This paper provides a comprehensive overview of the DSN's historical development, technical capabilities, and key facilities, emphasizing its essential role in past, present, and future space missions. It also addresses significant privacy, security, and performance issues within the network, evaluates current solutions, and identifies unresolved challenges and future research opportunities. The study reveals that while considerable advancements have been made, emerging threats and the evolving landscape of space exploration necessitate continuous improvements in security measures. The findings underscore the importance of innovative solutions to maintain the DSN's reliability and security, ensuring its effectiveness as a communication network for future space exploration.

Keywords: DSN; Interplanetary communication Space missions; Quantum Cryptography; Supply chain security; Privacy-preserving data sharing; Cyber-security workforce development

1. Introduction

The National Aeronautics and Space Administration (NASA) Deep Space Network (DSN) is vital for modern space exploration. Managed by the Jet Propulsion Laboratory's (JPL) Interplanetary Network Directorate, the DSN is a sophisticated telecommunications system that supports interplanetary spacecraft missions, radio astronomy, radar astronomy, and other space observations [1] - [7]. As the largest and most advanced network of its kind, the DSN helps maintain communication [8] with spacecraft exploring distant planets, moons, and other celestial bodies [9] - [11]. This introduction will explore the DSN's historical development, technical capabilities, and its crucial role in space missions, while also addressing privacy, security, and performance challenges. The DSN was established in 1958, soon after the launch of the first artificial satellite, Sputnik 1. It has been essential in supporting many space missions [12] - [14]. Initially, it was a collection of antennas scattered around the globe, but it quickly evolved into a coordinated and advanced system. The DSN's first major success was in 1964, supporting the Mariner 4 mission, which provided the first close-up images of Mars. Over the decades, the DSN has continued to support missions such as Voyager, Cassini, and the Mars Rover missions [15] - [16].

Technically, the DSN is known for its impressive infrastructure [17], which includes large radio antennas located around the world [18] - [20] as shown in Figure 1. These facilities are equipped with advanced signal processing and communication systems to ensure high-quality data transmission and reception [21]-[23]. The network's capabilities include tracking spacecraft, sending commands, and receiving scientific data, all of which are critical for the success of space missions. The DSN's infrastructure features 34-meter and 70-meter antennas, along with new technologies that promise higher data rates, better signal quality, and improved tracking precision. These advancements are important

* Corresponding author: Oroo Oyondi Felix

for supporting the increased data needs of modern missions, such as the James Webb Space Telescope (JWST) and upcoming Mars Sample Return missions [24], [25]. To manage the vast amount of data transmitted between Earth and spacecraft, the DSN employs cutting-edge technologies like deep-space transponders and highly sensitive receivers [26] - [29]. These technologies are designed to handle the weak signals received from distant spacecraft, ensuring that even the faintest signals are captured and processed. The DSN's data management systems are continually upgraded to keep pace with the increasing demands of space missions, incorporating new software and hardware to enhance data processing capabilities [30] - [32]. This ensures that scientists and engineers receive the most accurate and timely data possible, which is critical for mission planning and execution.

Despite its achievements, the DSN faces significant privacy and security challenges. The network's extensive reach and complex operations make it a potential target for cyber-attacks and other security threats [33] - [35]. It is crucial to maintain the integrity and confidentiality of the data transmitted across the network [36], [37].

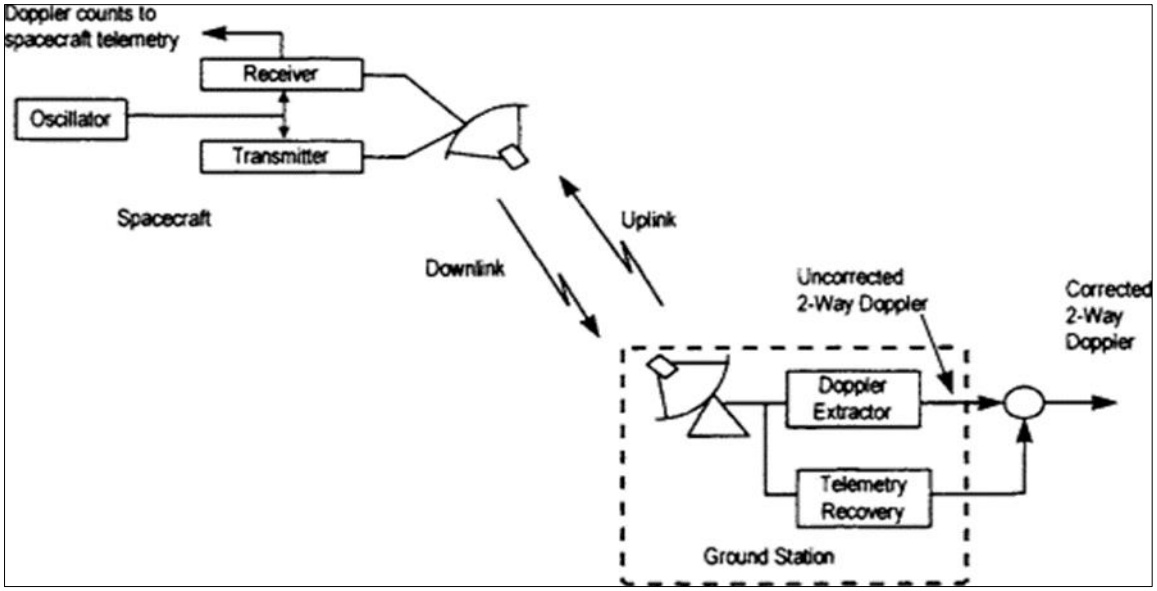

Figure 1 Deep Space Network

This paper will explore the privacy and security issues in the DSN's operations, assess current solutions, and identify areas for improvement. Key concerns include securing communication channels against eavesdropping and tampering, ensuring the authenticity of data and commands, and protecting ground stations and spacecraft from cyber-attacks. The performance of the DSN is another critical aspect. As missions become more ambitious and spacecraft travel further from Earth, the demands on the DSN's communication systems increase [38], [39]. Ensuring that the network can handle these demands while maintaining high levels of reliability and efficiency is essential. This paper will examine performance issues such as data throughput, latency, and system reliability. By evaluating these factors, the study aims to provide a comprehensive understanding of the network's operational challenges and propose solutions to optimize [40] its performance for future space missions. Innovations such as advanced signal processing algorithms, adaptive coding and modulation schemes, and next-generation antennas are being explored to enhance the DSN's capabilities. Additionally, strategies for improving network resilience, such as redundancy and fault-tolerant architectures, are being developed to ensure continuous, reliable communication with spacecraft.

Looking ahead, the DSN's role will become even more critical as space missions target more distant and challenging environments, such as the outer planets and potentially interstellar space [41]. The network will need to continue evolving, incorporating new technologies and methods to meet the demands of these ambitious missions. Ongoing investments in research and development are necessary to ensure that the DSN remains at the forefront of space communication technology. This includes exploring new frequency bands, enhancing ground station capabilities, and developing more efficient data transmission techniques.

In a nutshell, the DSN is a crucial element of NASA's space exploration efforts, providing essential communication links between Earth and spacecraft. Its advanced infrastructure and technological capabilities have enabled numerous successful missions, but it must continuously adapt to address the growing challenges of security, privacy, and

performance. By understanding the DSN's history, technical aspects, and the challenges it faces, we can better appreciate its importance and the need for ongoing innovation to support the future of space exploration.

1.1. Motivation of the Study

The motivation for this study, "A Comprehensive Overview of Privacy, Security, and Performance Issues in Deep Space Networks, "originates from the critical role the NASA Deep Space Network (DSN) plays in enabling communication for interplanetary missions [42], [43]. As the largest and most sophisticated telecommunications system globally, the DSN must continuously evolve to meet the demands of increasingly ambitious space exploration initiatives. This study aims to address the significant privacy, security, and performance challenges faced by the DSN, ensuring the integrity and confidentiality of data, protecting against cyber threats, and optimizing network efficiency. By identifying gaps in current solutions and proposing innovative improvements, the research seeks to enhance the DSN's resilience and reliability, thereby supporting the continued success of future space missions.

1.2. Research Contributions

This research paper provides a comprehensive understanding of the privacy, security, and performance issues within the NASA Deep Space Network (DSN). The study begins by outlining the historical development, technical capabilities, and essential role of the DSN in interplanetary missions. The findings of this study contribute significantly to the existing body of knowledge by offering researchers, industries, and policymakers a clear understanding of the challenges and potential solutions related to the DSN. This research aims to enhance the future design, development, and implementation of secure and efficient communication systems for space exploration:

- **Comprehensive Review:** The study provides an in-depth review of the unique privacy, security, and performance issues faced by the DSN, considering its extensive reach and complex operational environment.
- **Assessment of Current Solutions**: The research evaluates the strengths and limitations of existing solutions aimed at addressing the DSN's privacy, security, and performance challenges, including encryption methods, network security protocols, and system optimization techniques.
- **Identification of Gaps**: The research identifies critical gaps and unresolved issues within the current body of knowledge, highlighting areas that require further investigation and innovation.
- **Future Research Directions**: Building on these findings, the study proposes potential directions for future research, focusing on specialized designs and implementations to enhance the DSN's security, privacy, and overall performance.

2. Methodology

This research follows the methodologies were employed to review and analyze existing knowledge on privacy, security, and performance challenges in the NASA Deep Space Network (DSN):

- **Literature Review:** A thorough review of existing knowledge on privacy, security, and performance issues in the DSN, examining historical development, technical capabilities, and the network's role in space missions.
- **Security Evaluation:** This technique identifies security issues based on their nature and impact on DSN operations, evaluates common mitigation strategies, and highlights gaps that have not been adequately addressed.
- **Privacy Assessment:** The research assesses existing solutions to privacy issues within the DSN, analyzing their effectiveness, strengths, and limitations in addressing the identified challenges.
- **Performance Assessment**: The study delves into current performance challenges, evaluating the available solutions, and addressing the gaps identified in the DSN's operational efficiency.
- **Gap Analysis:** The research identifies significant gaps and unresolved issues in the current body of knowledge, emphasizing areas that require further investigation and innovation.
- **Proposal of Future Directions**: Based on the findings, the study proposes potential research directions aimed at providing enhanced security, improved privacy measures, and optimized performance for the DSN, ensuring its reliability and effectiveness for future space missions.

3. Deep State Networks Architecture

The Deep Space Network (DSN) is a crucial component of space exploration, enabling communication with spacecraft across the solar system and beyond [44]- [46]. Managed by NASA's Jet Propulsion Laboratory (JPL), the DSN supports a variety of missions including interplanetary exploration, radio astronomy, and space science observations. The DSN's

architecture is designed to handle the unique challenges of deep space communication, characterized by vast distances, signal attenuation [47], and the need for high precision [48] - [50]. This section provides an overview of the DSN's structure, including its global network of ground stations, antenna systems, and communication technologies.

3.1. Deep Space Network Components

3.1.1. Ground Stations

The DSN consists of three primary ground stations, each equipped with large, high-precision antennas located in different geographical regions [51], [52]. This global distribution ensures continuous coverage and communication [53] with spacecraft, regardless of their position relative to Earth.

- **Goldstone Deep Space Communications Complex (California, USA)**: Located in the Mojave Desert, this facility hosts some of the largest antennas in the DSN, including a 70-meter dish known as the "Deep Space Network's flagship." It provides critical support for missions across the solar system and beyond [54].
- **Madrid Deep Space Communication Complex (Spain)**: Situated near Madrid, this complex features both 70-meter and 34-meter antennas. Its strategic location allows for uninterrupted communication with spacecraft when those in California are not in view.
- **Canberra Deep Space Communication Complex (Australia):** Located in Tidbinbilla, near Canberra, this facility is equipped with 70-meter and 34-meter antennas, providing essential coverage for missions during periods when other stations are out of range. Table 1 presents a summary of the different ground stations.

Table 1 Ground Stations Summaries

Location	Antenna Size	Primary Function	Missions Undertaken
Goldstone, California	70m, 34m	Deep space communication, tracking, command, data	Voyager, Mars Rovers, Juno
Madrid, Spain	70m, 34m	Deep space communication, tracking, command, data	Cass ini, Mars Express, Hubble
Canberra, Australia	70m, 34m	Deep space communication, tracking, command, data	Voyager, Rosetta, Mars Science Laboratory

3.1.2. Antenna Systems

Antenna systems are integral to the Deep Space Network (DSN), providing the essential capability to communicate with spacecraft across vast distances [55], [56]. These systems are meticulously designed to handle the unique challenges of space communication, including signal attenuation and data transmission over long distances. The DSN employs a range of antennas, including High-Gain Antennas (HGAs) for high-sensitivity, long-range communication [57]-[60], Medium-Gain Antennas (MGAs) for intermediate distances [61], and Low-Gain Antennas (LGAs) for close-range and low-bandwidth needs [62], [63]. Each type of antenna is optimized for specific mission requirements, ensuring robust and reliable communication [64] for space missions spanning the solar system and beyond as shown in Figure 2[65].

The DSN's antennas are categorized based on their size and functionality:

- High-Gain Antennas (HGA): These are large parabolic dishes, crucial for deep space communication due to their high sensitivity and capability to receive weak signals from distant spacecraft. They are used for transmitting and receiving high-bandwidth data.
- Medium-Gain Antennas (MGA): These antennas are slightly smaller than HGAs and are used for intermediate-range communications. They provide a balance between sensitiviy and coverage area, suitable for spacecraft closer to Earth.
- Low-Gain Antennas (LGA): These are small, omnidirectional antennas used primarily for low-bandwidth communication and when spacecraft are in close proximity to Earth.

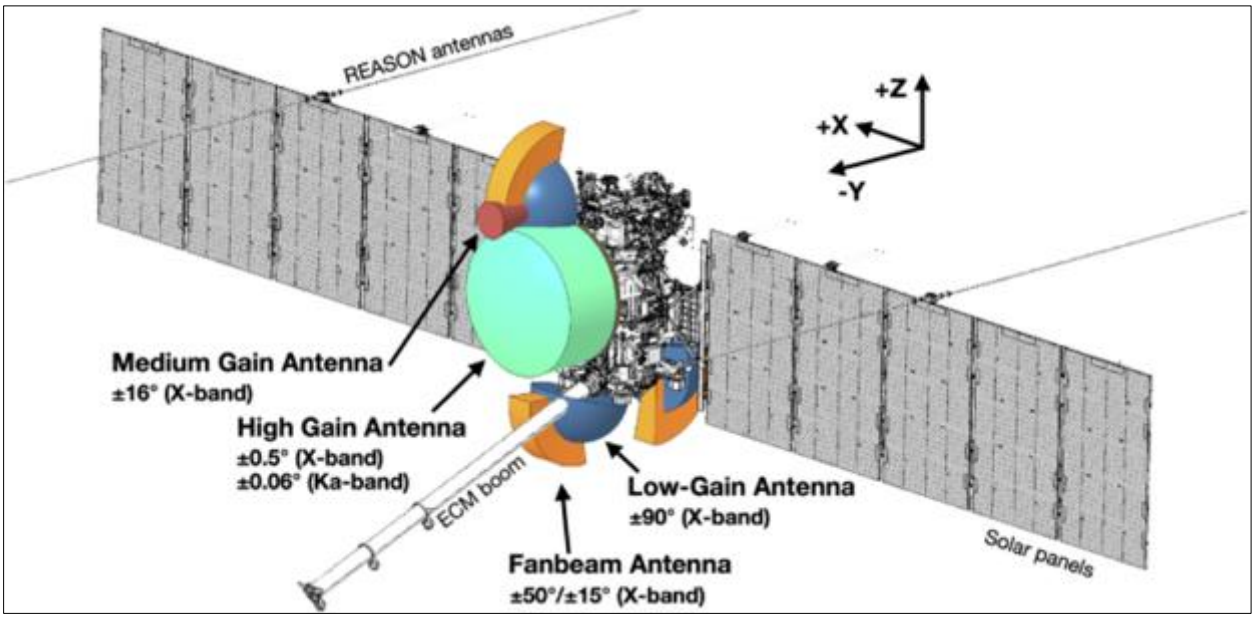

Figure 2 Types of Antenna in DSN

3.1.3. Communication Systems

Communication systems are the backbone of the Deep Space Network (DSN), enabling seamless data transmission between Earth and distant spacecraft. These systems encompass advanced technologies and components designed to handle the complex demands of deep space communication. Key elements include signal processing equipment for decoding and interpreting faint signals, tracking systems for precise antenna alignment, and command systems for managing spacecraft operations [66] - [70]. Together, these components ensure high-quality data transmission [71], reliable command execution, and effective mission support across the solar system and beyond; as evident in Figure 3 [72].

The DSN's communication systems are sophisticated and include several key components [73] - [75]:

- Signal Processing Equipment: This includes digital signal processors (DSPs) and modems that decode and interpret the signals received from spacecraft. Advanced algorithms are used to filter and process data [76], ensuring accuracy.
- Tracking Systems: These systems use servo motors and optical sensors to maintain precise alignment of antennas with spacecraft. GPS systems assist in tracking the position of antennas and adjusting their orientation.
- Command and Control Systems: These systems manage the sending of commands to spacecraft and the receipt of telemetry data. They are crucial for mission operations, including adjustments to spacecraft trajectories and data collection. Table 2 gives a summary of the various communication system components.

Table 2 Communication systems components

Component	Function	Key Technologies
Signal Processors	Decode and process signals from spacecraft	Digital Signal Processing (DSP), Modems
Tracking Systems	Maintain antenna alignment with spacecraft	Servo Motors, GPS, Optical Sensors
Command Systems	Send commands and receive telemetry	Telemetry Systems, Command and Control Units

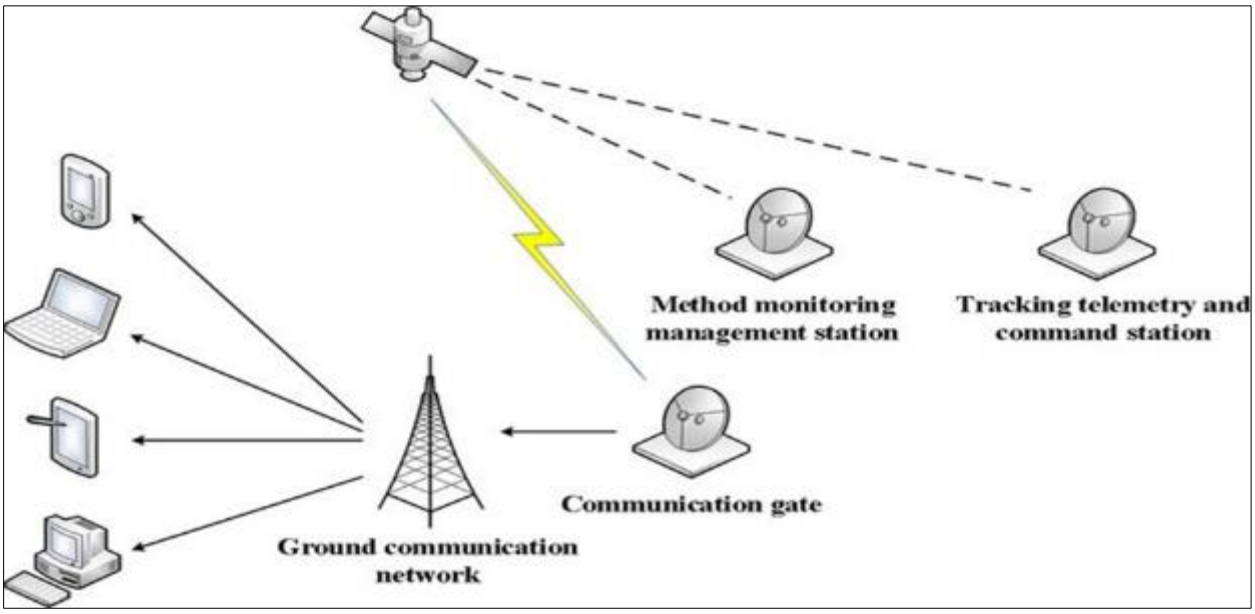

Figure 3 DSN Communication Systems

3.1.4. Data Handling and Transmission

Data Flow

Data flow within the DSN involves several stages:

- Reception: Antennas receive signals from spacecraft, which include telemetry, science data, and command signals [77].
- Processing: Signals are processed by signal processing equipment to decode and interpret the data. This involves filtering, amplification, and demodulation [78], [79].
- Transmission: Processed data is sent to mission control centers and scientific teams for analysis. This stage also includes the transmission of commands to spacecraft [80]-[84]. Figure 4 below depicts how data flow within the DSN architecture [85].

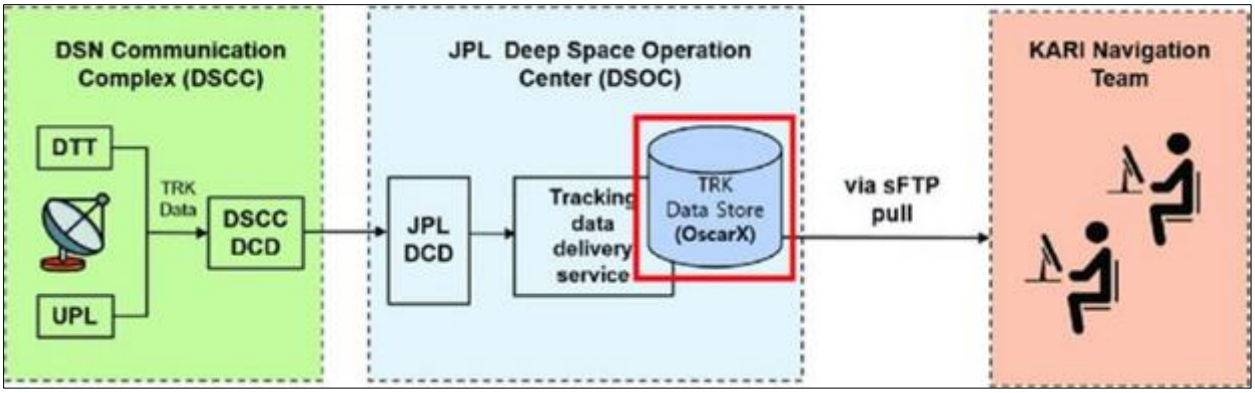

Figure 4 Data Flow in DSN

3.1.5. Data Transmission Rates

Data rates are determined by the spacecraft's distance from Earth and the capabilities of the communication systems [86], [87]. Typical data rates include:

- High Data Rate (HDR): Up to 1 Mbps, used for close-range missions where high-bandwidth communication is required.

- Low Data Rate (LDR): Up to 100 kbps, suitable for deep space missions where signal strength is weaker and data rates are lower. Table 3 below summarizes some of the typical data rates for DSNs.

Table 3 Typical Data Rates for DSN

Mission Type	Distance from Earth	Data Rate	Description
Close-Range	< 1 AU	1 Mbps	High-bandwidth communication
Mid-Range	1-10 AU	500 kbps	Intermediate data rate
Deep Space	> 10 AU	100 kbps	Lower data rate due to increased distance

3.2. Applications of Deep Space Networks

Deep Space Networks (DSNs) are crucial for a wide range of space exploration and scientific activities. They support interplanetary missions by facilitating communication with spacecraft exploring other planets, moons, and celestial bodies [88]. DSNs are used for tracking and sending commands to spacecraft, receiving scientific data from distant missions, and conducting radio and radar astronomy to study celestial phenomena [89], [90]. They also play a vital role in monitoring [91] and supporting space telescopes and observatories, enabling the collection of valuable astronomical data. Additionally, DSNs are essential for the navigation and trajectory adjustments of spacecraft, ensuring their successful journey through space [92]-[96]. This broad spectrum of applications highlights the DSN's central role in advancing our understanding of the universe and supporting ongoing space missions [97]. Table 4 below presents some of the application domains of DSNs,

Table 4 Applications of Deep Space Networks

Application	Description
Interplanetary Missions	Facilitates communication and data transmission with spacecraft exploring planets, moons, and other celestial bodies.
Scientific Data Collection	Receives and transmits scientific data from deep space missions, enabling the study of planetary atmospheres, surface conditions, and more.
Radio and Radar Astronomy	Supports observations of celestial phenomena through radio and radar signals, contributing to our understanding of the universe.
Space Telescope and Observatory Support	Assists in data transmission and command management for space telescopes and observatories, enhancing their scientific capabilities.
Spacecraft Navigation and Control	Provides tracking and command functions for spacecraft trajectory adjustments and mission operations.

4. Security, Privacy, and Performance Issues in DSN

The deep space network is the cornerstone of interplanetary communication, playing a pivotal role in the success of space exploration missions. However, its effectiveness is continually challenged by issues related to security, privacy, and performance. Security concerns are paramount, as any breach can compromise mission integrity and national security. Privacy issues also pose significant risks, given the sensitive nature of the data transmitted between Earth and spacecraft. Additionally, performance issues can severely impact mission outcomes, with delays or data loss potentially jeopardizing critical operations. Addressing these challenges is essential to maintaining the reliability and success of the DSN, ensuring that it continues to support the ambitious goals of space exploration.

4.1. Security Issues in Deep Space Networks

Deep Space Networks (DSNs) face a range of security issues [98] due to the critical nature of their operations and the challenges of space communication. Below is a detailed analysis of three major security issues, including how attacks occur, vulnerabilities exploited, their impacts, mitigation strategies, and identified gaps.

4.1.1. Data Interception

Data interception involves unauthorized parties capturing the sensitive information transmitted between spacecraft and ground stations [99], [100]. Given the vast distances and the weak nature of the signals, the data is vulnerable to interception by malicious actors who can exploit the lack of encryption or use sophisticated technology to eavesdrop [101].

The Deep Space Networks (DSNs) face significant vulnerabilities due to a lack of robust encryption for data in transit and insufficient data protection mechanisms [102]- [104]. These weaknesses can lead to the compromise of sensitive scientific data and mission-critical commands, posing a risk of unauthorized access to confidential information [105]. The resulting breaches can disrupt mission operations, potentially jeopardizing the success and safety of space missions by undermining the integrity and confidentiality of transmitted data.

Mitigation Strategies and Gaps

To address vulnerabilities in Deep Space Networks (DSNs), implementing end-to-end encryption is essential to ensure data confidentiality throughout transmission [106]-[110]. Exploring advanced methods like quantum cryptography, which promises theoretically unbreakable encryption, represents a forward-looking approach. However, current efforts reveal gaps such as the limited implementation of cutting-edge encryption technologies and the necessity for ongoing advancements [111], [112]. As threats evolve, the field must continuously update and enhance encryption techniques to maintain robust protection and address emerging security challenges effectively.

4.1.2. Signal Jamming

Signal jamming disrupts communication between spacecraft and ground stations by emitting interference signals [113], [114]. This can be intentional (malicious) or unintentional (due to environmental factors). Jamming can prevent the successful transmission and reception of critical data and commands. In Figure 5, it shows how jamming attack takes place in an wireless communication systems [115].

Deep Space Networks (DSNs) are particularly vulnerable due to the susceptibility of their communication channels to interference and the lack of resilience in communication protocols against jamming [116] - [119]. This susceptibility can lead to significant disruptions, potentially resulting in mission failures or loss of crucial data. The impact of such disruptions includes a reduced effectiveness in maintaining consistent contact and control over spacecraft, which can jeopardize mission success and compromise the integrity of scientific and operational data. These vulnerabilities highlight the critical need for robust anti-jamming measures and resilient communication protocols to ensure the continuous reliability and effectiveness of DSN operations [120].

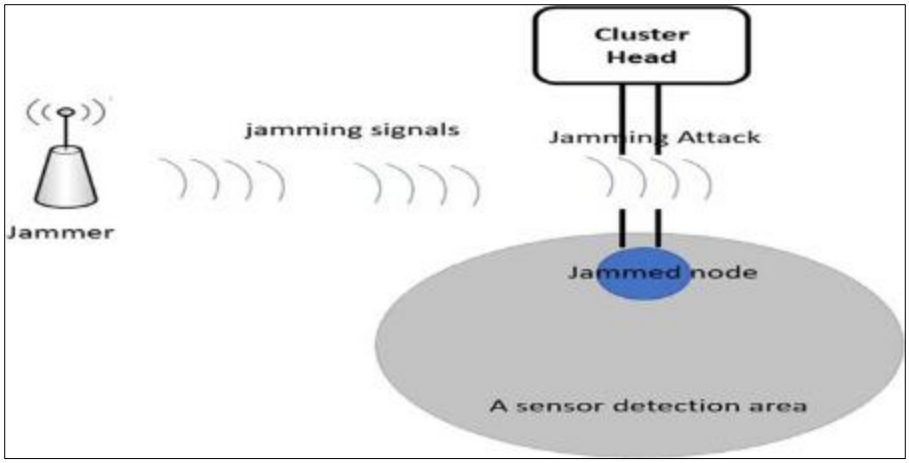

Figure 5 Jamming Attack on a Wireless Network

To counteract vulnerabilities in Deep Space Networks (DSNs), effective anti-jamming techniques such as Frequency Hopping Spread Spectrum (FHSS) and Direct Sequence Spread Spectrum (DSSS) are employed to reduce the impact of interference [121]. Additionally, implementing resilient communication protocols [122] and adaptive error-correction methods helps maintain reliable communication despite environmental disruptions [123], [124]. However, gaps persist, including the need for more advanced anti-jamming technologies to address increasingly sophisticated interference techniques and the ongoing development required for protocols that can dynamically adapt to new and evolving

jamming methods [125], [126]. Addressing these gaps is crucial for enhancing the robustness of DSN communications and ensuring uninterrupted mission success.

4.1.3. Unauthorized Access

Unauthorized access involves individuals gaining access to DSN systems without permission. This can result from compromised credentials, inadequate access controls, or vulnerabilities in authentication mechanisms [127]- [129]. Deep Space Networks (DSNs) face significant risks due to weak access controls and inadequate authentication mechanisms, including insufficient multi-factor authentication and role-based access controls [130] - [133]. These vulnerabilities can lead to data breaches, allowing unauthorized manipulation of mission data [134] and resulting in a loss of control over spacecraft. Such breaches pose serious threats to mission integrity, potentially leading to sabotage and compromising the overall success of space missions. Enhancing access controls and authentication measures is critical to protecting DSN operations from these severe impacts [135], [136].

To address vulnerabilities in Deep Space Networks (DSNs), implementing multi-factor authentication (MFA) and role-based access control (RBAC) is crucial for restricting access and protecting sensitive data [137] - [139]. Regular security audits and updates further enhance these access control mechanisms. However, gaps remain, including inadequate implementation of MFA across all systems and the ongoing need for continuous improvements in access control and authentication practices [140]-[143]. Addressing these gaps is essential to strengthening DSN security and ensuring comprehensive protection against unauthorized access and potential breaches. Table 5 gives a summary of DSN security issues.

Table 5 Security issues in deep space networks

Security Issue	How the Attack Takes Place	Vulnerabilities Exploited	Impact to DSN	Mitigation Strategies	Gaps Found
Data Interception	Unauthorized capture of data in transit	Lack of robust encryption	Compromised data confidentiality and integrity	Encryption, Quantum Cryptography	Need for advanced encryption techniques
Signal Jamming	Interference disrupting communication	Susceptibility to jamming	Communication disruption, potential mission failures	Anti-Jamming Techniques, Resilient Protocols	Advanced anti-jamming technologies required
Unauthorized Access	Gaining access without permission	Weak access controls and authentication	Data breaches, loss of spacecraft control	MFA, Role-Based Access Control (RBAC)	Need for improved access control practices

4.2. Privacy Issues in Deep State Networks

Deep Space Networks (DSNs) are vital for communication between spacecraft and Earth, transmitting sensitive data like scientific measurements and astronaut health information. Ensuring data privacy is crucial due to the complexity and volume of transmitted data. The unique challenges of DSNs, such as vast distances and the need for robust communications, make protecting this data difficult. Comprehensive measures are needed to safeguard sensitive information and ensure mission success. In this section the paper discusses three major privacy challenges in Deep State Networks

4.2.1. Man-in-the-Middle (MitM) Attacks

Man-in-the-Middle (MitM) attacks pose significant privacy threats to Deep Space Networks (DSNs) [144] - [146]. These attacks involve an adversary intercepting and relaying messages between two parties who believe they are directly communicating with each other, as shown in Figure 6 [147], [148]. Given the sensitivity of data transmitted in DSNs, such as mission-critical commands and scientific measurements, MitM attacks can have severe consequences.

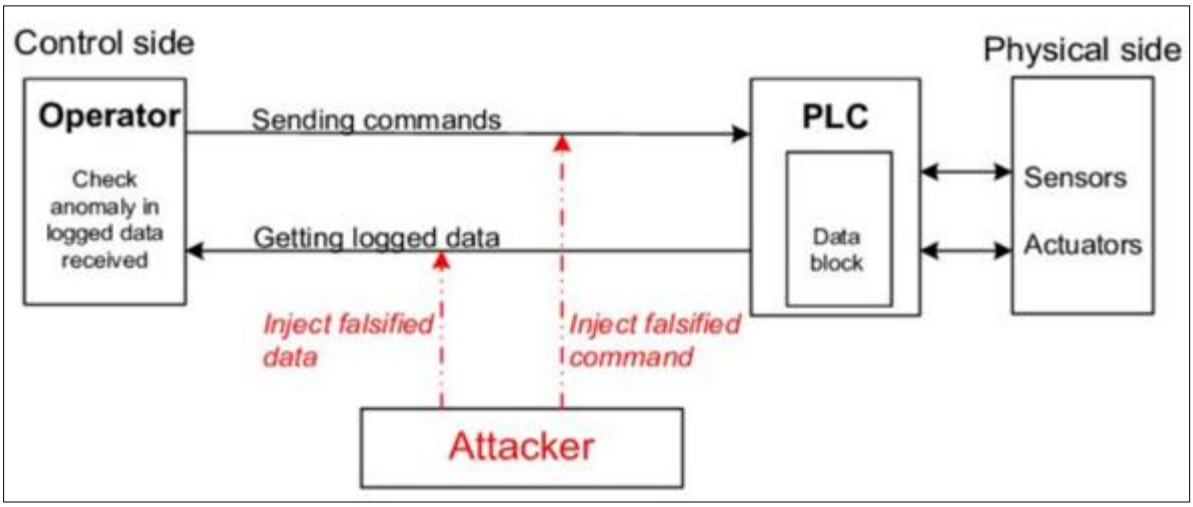

Figure 6 Man in the Middle Attack Model

MitM attacks occur when attackers exploit weaknesses in the communication protocols used by DSNs [149] - [152]. They insert themselves between the communicating parties, intercepting data without detection. Vulnerabilities include inadequate encryption and lack of authentication mechanisms [153]. The impact includes unauthorized data access, manipulation of transmitted data, and potential disruption of mission commands.

Mitigation strategies include implementing secure communication protocols, end-to-end encryption, and mutual authentication mechanisms. Regular security audits and protocol updates are essential [154] - [158]. However, gaps remain in fully implementing these strategies across all systems, necessitating continuous monitoring and improvement of communication protocols to counter evolving threats [159], [160].

4.2.2. Replay Attacks

Replay attacks in DSNs involve attackers capturing and retransmitting valid data transmissions to deceive the receiving system into accepting them as legitimate [161] - [164]. As shown in Figure 6, this type of attack can significantly compromise the integrity of DSNs communications, leading to unauthorized command execution and operational confusion. Replay attacks occur when attackers record valid communications and replay them at a later time to gain unauthorized access or execute commands as in Figure 7 [165] - [168]. Vulnerabilities include the absence of time-stamping, nonces, or sequence numbers in data packets [169]. The impact includes unauthorized command execution, duplication of valid data, and potential confusion or malfunction in mission operations.

Mitigation strategies involve time-stamping data packets [170], using nonces and sequence numbers, and deploying anti-replay mechanisms. Regular security updates and audits are crucial [171] - [173]. Gaps identified include insufficient implementation of anti-replay measures across all systems and the need for continuous protocol updates to counter new attack methods.

4.2.3. Side-Channel Attacks

Side-channel attacks involve attackers extracting sensitive information from DSN systems by analyzing physical emissions, such as electromagnetic leaks, power consumption, or timing information [174], [175]. These attacks can compromise the confidentiality and security of sensitive DSN data, including encryption keys [176]. Side-channel attacks occur when attackers use specialized equipment to monitor and analyze side-channel emissions from DSN hardware and software; represented in Figure 8 [177] - [181]. Vulnerabilities include insufficient shielding and protection against side-channel emissions. The impact includes unauthorized access to sensitive information , potential disclosure of encryption keys, and compromise of system security [182].

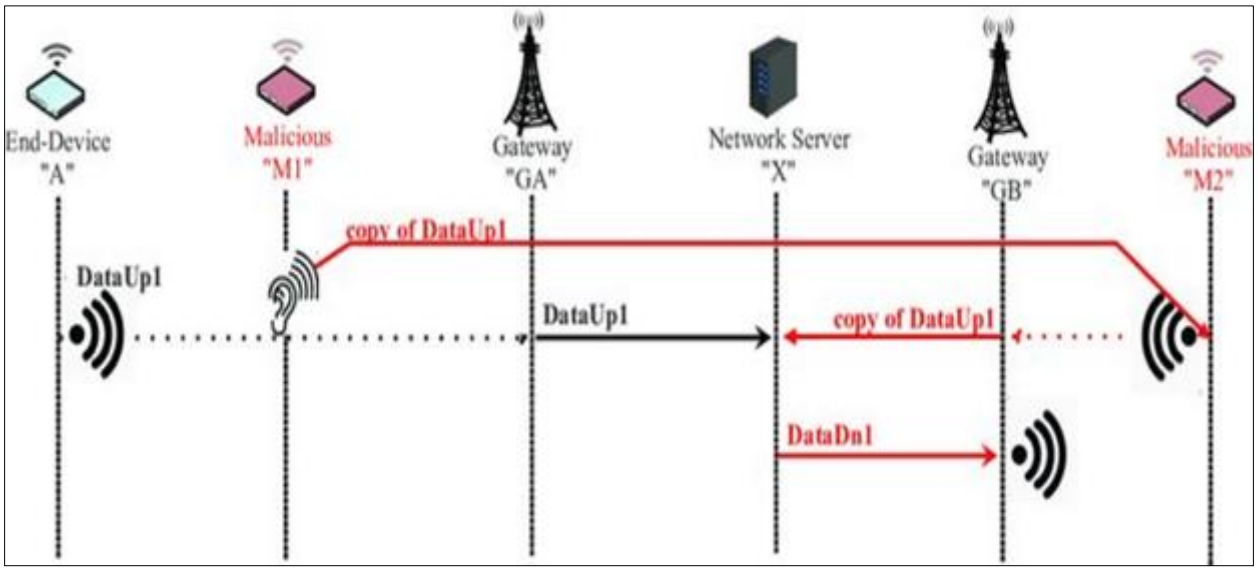

Figure 7 Replay Attack

Mitigation strategies include implementing shielding and noise generation techniques, using side-channel resistant algorithms, and continuous monitoring for side-channel emissions. Regular security assessments and updates to protection measures are essential [183] - [186]. Gaps identified include insufficient protection against side-channel emissions and the need for advanced mitigation techniques to counter evolving threats.

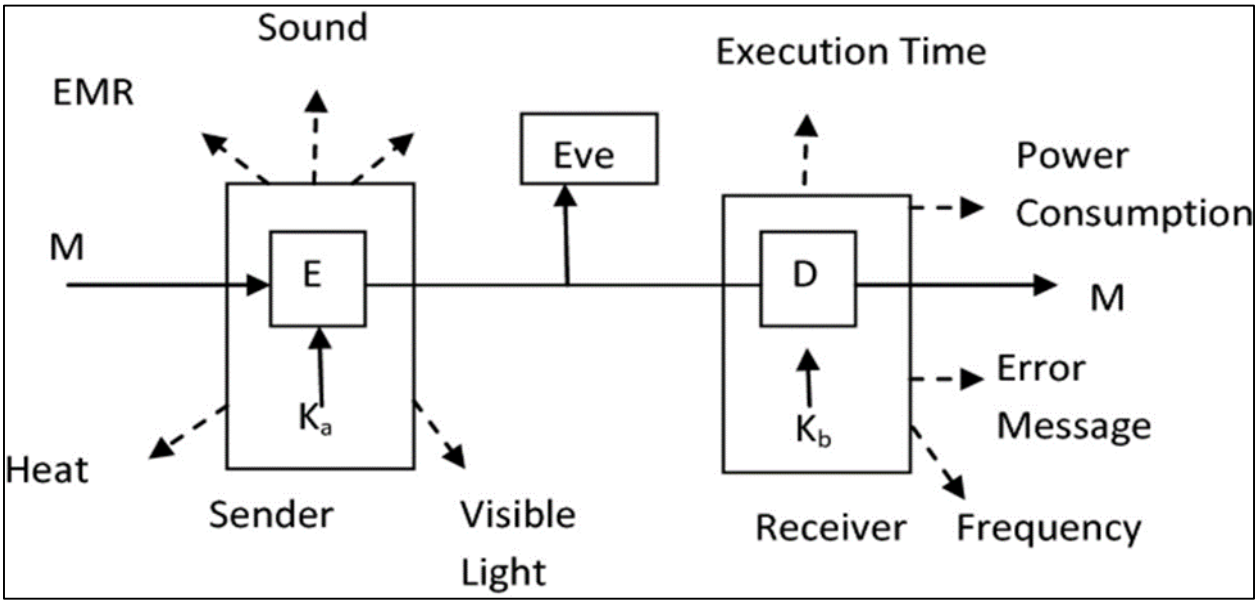

Figure 8 Side Channel Attack

Side-channel attacks are a significant threat to the security of cryptographic systems because they exploit indirect information leakage to bypass traditional security measures. Unlike conventional attacks that target weaknesses in algorithms or software, side-channel attacks take advantage of physical emanations such as power consumption, electromagnetic leaks, or even sound to extract sensitive information like cryptographic keys. These attacks can be particularly dangerous because they often require minimal access to the target system and can be performed without the need for extensive technical expertise. As technology advances and systems become more complex, the potential for side-channel vulnerabilities increases, underscoring the need for robust countermeasures and continual vigilance in security practices. Table 6 describes some of the privacy challenges in DSNs.

Table 6 Privacy Challenges

Privacy Attack	How it Occurs	Impact	Mitigation Strategies	Gaps Identified
Man-in-the-Middle (MitM)	Exploiting communication protocol weaknesses	Unauthorized data access, data manipulation, mission disruption	Secure communication protocols, end-to-end encryption, mutual authentication	Need for stronger communication protocols, ongoing monitoring
Replay Attacks	Recording and retransmitting valid communications	Unauthorized command execution, duplication of data, operational confusion	Time-stamping data packets, using nonces and sequence numbers, anti-replay mechanisms	Insufficient implementation of anti-replay measures, continuous protocol updates
Side-Channel Attacks	Analyzing physical emissions from DSN hardware/software	Unauthorized access to sensitive information, disclosure of encryption keys, system compromise	Shielding, noise generation, side-channel resistant algorithms, continuous monitoring	Insufficient protection against side-channel emissions, need for advanced mitigation techniques

4.3. Performance Issues in Deep Space Networks (DSN)

Performance issues in Deep Space Networks (DSNs) are critical as they directly impact the reliability and efficiency of communication between spacecraft and Earth-based stations. These issues can affect data transmission speed, latency, and overall network throughput [187], [188]. Key performance issues include signal attenuation, latency, bandwidth limitations, and data rate constraints.

4.3.1. Signal Attenuation

Signal attenuation is a major performance issue in DSNs due to the vast distances involved in space communications [189], [190]. As signals travel over millions of kilometers, they weaken, leading to potential loss of data integrity and communication reliability. Signal attenuation occurs as electromagnetic waves lose energy over long distances [191], [192]. The vacuum of space, interstellar dust, and the presence of other celestial bodies can further weaken signals. Vulnerabilities include inadequate amplification and signal boosting mechanisms. The impact includes reduced data quality, increased error rates, and potential communication blackouts.

Mitigation Strategies and Gaps:

Mitigation strategies involve using high-gain antennas, signal amplification, and error-correction techniques. Implementing adaptive modulation and coding can also help maintain signal integrity [193] - [195]. However, gaps remain in fully compensating for extreme distances and ensuring consistent signal strength.

4.3.2. Latency

Latency is a significant performance challenge in DSNs due to the time it takes for signals to travel between Earth and distant spacecraft [196] - [200]. This delay affects real-time communication and mission control operations. Latency [201] occurs due to the finite speed of light, which limits how quickly signals can travel. For instance, communication with Mars can experience a delay of up to 24 minutes round trip. Vulnerabilities include delayed response times and difficulty in executing time-sensitive commands [202] - [204]. The impact includes slower data exchange, delayed mission responses, and challenges in real-time monitoring.

Mitigation strategies involve developing autonomous systems onboard spacecraft to reduce reliance on Earth-based instructions, and using predictive algorithms to anticipate and preemptively address issues [205], [206]. Gaps identified include the need for more advanced autonomy and predictive models to fully mitigate latency effects.

4.3.3. Bandwidth Limitations

Bandwidth limitations in DSNs restrict the amount of data that can be transmitted within a given time frame, affecting the volume and speed of data exchange [207] between spacecraft and ground stations. Bandwidth limitations occur due

to the restricted frequency spectrum available for space communications and the need to share this spectrum among multiple missions [208]-[210]. Vulnerabilities include congestion and limited data transmission capabilities [211], [212]. The impact includes slower data rates, reduced data quality, and potential loss of critical information.

Mitigation strategies involve optimizing data compression, utilizing higher frequency bands, and developing more efficient communication protocols [213]-[215]. Regular upgrades to ground station equipment and spectrum management are also necessary. Gaps include the challenge of continually increasing bandwidth to meet growing data demands. Table 7 discusses some of the performance challenges in the DSN environment.

Table 7 Performances Challenges

Performance Issue	How it Occurs	Impact	Mitigation Strategies	Gaps Identified
Signal Attenuation	Weakening of signals over long distances	Reduced data quality, increased error rates, communication blackouts	High-gain antennas, signal amplification, error-correction	Compensating for extreme distances, ensuring consistent signal strength
Latency	Time delay due to finite speed of light	Slower data exchange, delayed mission responses, challenges in real-time monitoring	Autonomous systems, predictive algorithms	Advanced autonomy, predictive models to mitigate latency
Bandwidth Limitations	Restricted frequency spectrum, shared among missions	Slower data rates, reduced data quality, potential loss of information	Data compression, higher frequency bands, efficient protocols	Increasing bandwidth to meet data demands
Data Rate Constraints	Balancing data volume with transmission power and bandwidth	Prolonged data transmission times, potential data loss, delays in critical information	Adaptive data rate techniques, improved transmitter efficiency, data prioritization	Innovation in data rate optimization, efficient power management systems

4.4. Gaps Analysis

The analysis of security, privacy, and performance gaps in Deep Space Networks (DSNs) highlights critical vulnerabilities and areas requiring improvement to ensure reliable and secure communication for space missions [216] - [218]. Security gaps such as weak encryption, insufficient access controls, and susceptibility to interference need addressing through advanced encryption technologies, comprehensive multi-factor authentication, and robust anti-jamming techniques [219] - [224].

Privacy concerns, including data transmission security and unauthorized access, necessitate implementing end-to-end encryption, stringent access controls, and secure data management practices [225] -[230]. Performance issues like signal attenuation, latency, bandwidth limitations, and data rate constraints demand solutions like high-gain antennas, autonomous systems, spectrum optimization, and adaptive data rate techniques [231] - [234]. Table 8 presents some of the gap analysis and recommendations.

Table 8 Gap Analysis and Recommendation

Category	Gaps Analysis	Future Recommendations
Security	- Weak encryption protocols	- Develop advanced encryption technologies (e.g., quantum cryptography)
	- Insufficient multi-factor authentication and role-based access controls	- Implement comprehensive MFA and RBAC across all systems
	- Lack of robust communication protocols against jamming	- Invest in advanced anti-jamming techniques

	- Inadequate cybersecurity defenses with terrestrial network integration	- Enhance IDPS, firewalls, and conduct continuous vulnerability assessments
Privacy	- Inadequate encryption for data in transit	- Implement end-to-end encryption and explore quantum cryptography
	- Vulnerability to interference and jamming	- Develop resilient protocols that detect and mitigate interference
	- Weak access controls and authentication mechanisms	- Adopt comprehensive MFA and RBAC, coupled with regular security audits
	- Insufficient secure storage solutions and data management practices	- Establish secure storage solutions and enforce strict data management practices
Performance	- Signal attenuation over long distances	- Utilize high-gain antennas and signal amplification techniques
	- Significant communication delays (latency) due to vast distances	- Develop autonomous systems onboard spacecraft to reduce latency reliance
	- Bandwidth limitations due to restricted frequency spectrum	- Optimize spectrum usage and develop efficient communication protocols
	- Data rate constraints balancing data volume with available transmission power and bandwidth	- Implement adaptive data rate techniques and improve transmitter efficiency

According to [235], DSNs are crucial for communication between Earth and spacecraft operating beyond Earth's orbit. These networks enable data transmission for various space missions, including robotic and human exploration. Despite advancements in technology, there are significant gaps in privacy, security, and performance issues that need to be addressed to ensure the effectiveness and safety of these missions.

4.4.1. Privacy Issues

Privacy issues in the DSN are a serious concern due to the sensitivity and critical nature of the data it handles. The DSN, responsible for communicating with interplanetary spacecraft, relays vast amounts of scientific data, mission-critical information, and potentially sensitive communications between Earth and space missions. Unauthorized access or interception of this data could compromise mission integrity, lead to the loss of invaluable scientific information, and even pose national security risks.

The complexity of the DSN infrastructure and the long transmission distances involved also increase the vulnerability to cyber threats and potential data breaches. Therefore, ensuring the privacy and security of the DSN is paramount to maintaining the safety, reliability, and success of space exploration missions. Some of the privacy issues that are yet to be addressed in DNSs are presented in Table 9.

Table 9 Privacy gaps in DSN

Privacy issue	**Explanation**
Mission data exposure	Data transmitted through DSNs can include sensitive mission details, scientific data, and potentially classified information. Unauthorized access or interception can compromise mission integrity [236], [237].
Astronauts' privacy	Communication involving human space missions may contain personal information about astronauts, including medical data, which needs to be protected from unauthorized access [238].
Ground station security	Ground stations are critical nodes in DSNs. Weak security measures at these stations can lead to unauthorized access to sensitive data [239].
Data relay security	Data relayed through multiple points, including satellites and ground stations, is vulnerable to interception and unauthorized access at various stages [241]-[243].

Cross-border data transmission	DSNs often involve transmitting data across multiple countries' airspace and jurisdictions, complicating the enforcement of privacy regulations [244].
International collaboration	Collaborations between different space agencies require harmonized privacy standards [245], which can be difficult to achieve due to varying national laws.
Long-term Storage	Data from space missions is often stored long-term for future analysis [246]. Ensuring the privacy of this data over extended periods is challenging.
Secondary Use of Data	Clear policies are needed to govern the secondary use of mission data to prevent misuse or unauthorized analysis [247].

4.4.2. Security Issues

Security issues in the DSN are of critical importance due to the essential role the DSN plays in interplanetary communications and mission control. Any breach in DSN security could have severe consequences, including the disruption of communication with spacecraft, loss of scientific data, and interference with mission operations. Such breaches could be the result of cyberattacks, signal jamming, or unauthorized access, potentially leading to mission failures, loss of billions of dollars in investments, and compromised national security.

Given the complexity and sophistication of space missions, the DSN must implement stringent security measures to protect against evolving threats and ensure the continuous and secure transmission of data between Earth and space. The security issues in Table 10 are yet to be addressed in DNSs.

Table 10 Security gaps in DSN

Security issue	**Details**
Long distance communication	Encrypting data for long-distance space communication presents unique challenges, including the need for robust encryption algorithms that can withstand the harsh space environment [248].
Key management	Managing encryption keys over vast distances and ensuring their secure exchange is a significant challenge [249].
Hacking and cyber attacks	DSNs are vulnerable to cyber attacks [250], including hacking attempts aimed at disrupting communication or gaining unauthorized access to sensitive data.
Denial of Service (DoS) attacks	DoS attacks can target ground stations or satellites, leading to communication blackouts that can jeopardize mission success [251].
Tampering and physical attacks	Satellites and other space-based assets are vulnerable to tampering or physical attacks [252], including those from adversarial nations.
Space debris and collisions	The increasing amount of space debris poses a threat to the physical security of communication satellites [253], potentially leading to data loss or communication disruption.
Physical intrusion	Ground stations must be protected from physical intrusions [254] that could lead to sabotage or unauthorized data access.
Environmental threats	Ground stations are also vulnerable to natural disasters, which can disrupt operations and compromise data security [255].

4.4.3. Performance Issues

Performance issues in the deep space networks can critically impact the success of space missions, as the DSN is responsible for maintaining reliable communication with spacecraft across vast distances in the solar system. Any degradation in performance, such as delays, data loss, or signal interference, can hinder the timely transmission of essential scientific data and commands, potentially jeopardizing mission objectives and the safety of spacecraft. Given the complexity of space missions and the precision required in operations, even minor performance issues can result in significant setbacks, financial losses, and missed opportunities for scientific discovery. Therefore, ensuring optimal performance of the DSN is crucial for the success and advancement of space exploration. Some of the performance issues that are yet to be addressed in DNSs are described in Table 11 below.

Table 11 DNS performance gaps

Performance issue	Particulars
Long distances	The vast distances involved in deep space communication lead to significant signal delays [256], which can affect the real-time control of spacecraft and data transmission efficiency.
Light speed limitations	Communication is constrained by the speed of light, leading to unavoidable latency that must be accounted for in mission planning [257].
Weak signals	Signals weaken over long distances [258], requiring highly sensitive receivers and powerful transmitters to ensure reliable communication.
Interference	Space weather, cosmic radiation, and other sources of interference can disrupt signals [259], affecting communication quality and reliability.
Spectrum allocation	The available bandwidth for deep space communication is limited [260], leading to potential congestion and competition for frequencies.
Data compression	Effective data compression techniques [261] are necessary to maximize the use of available bandwidth without compromising data integrity.
Slow data rates	The data rates achievable over vast distances are relatively slow [262], limiting the amount of data that can be transmitted in a given time frame.
Adaptive techniques	Implementing adaptive communication techniques that can dynamically adjust data rates based on signal quality and other factors is challenging [263].
Component failures	The harsh space environment can lead to component failures in both spacecraft and ground-based systems [264], affecting communication reliability.
Fault tolerance	Designing fault-tolerant systems [265] that can continue to operate despite failures is critical for ensuring continuous communication.
Backup systems	Effective backup systems and redundancy are necessary to maintain communication in case of primary system failures [266].
Cross-agency coordination	International collaboration and coordination are required to implement and manage redundant communication systems effectively [267].

It is therefore essential to counter the above privacy, security, and performance gaps in Deep Space for the success of space missions. This requires continuous advancements in encryption and cybersecurity measures, robust regulatory frameworks, innovative communication technologies, and international cooperation. Ensuring the reliability, security, and efficiency of DSNs will be crucial as space exploration continues to expand and evolve.

4.5. Future Research scopes

Future research in Deep Space Networks (DSNs) aims to address the critical gaps in privacy, security, and performance, ensuring more robust and reliable communication systems for space missions. Table 12 discusses some promising research areas.

Table 12 Probable research scopes

Research scopes	Details
	Quantum cryptography: Research into quantum key distribution (QKD) [268] can provide theoretically unbreakable encryption methods, making data transmission more secure against future quantum computing threats. Implementing QKD in space-based communication systems to secure long-distance transmissions.
	Homomorphic encryption: Developing efficient homomorphic encryption algorithms [269] that allow computations on encrypted data without needing decryption, preserving privacy [270] even

Privacy	during data processing. Application of homomorphic encryption in on-board data processing units to ensure end-to-end data privacy.
	Differential privacy: Implementing differential privacy techniques [271] to ensure that individual data points in large datasets are protected, reducing the risk of sensitive information exposure. Applying differential privacy in the analysis of mission data to balance data utility and privacy.
	Secure Multi-Party Computation (SMPC): Researching SMPC methods [272] for securely sharing and processing data between multiple parties without revealing individual data inputs. Utilizing SMPC in collaborative space missions involving multiple agencies to ensure data privacy.
	Advanced anonymization techniques: Developing new algorithms for anonymizing data collected from space missions to prevent re-identification of sensitive information [273]. Ensuring that anonymized data retains its utility for scientific analysis while protecting privacy.
	Privacy-preserving data mining: Researching methods to mine data from deep space missions while preserving the privacy of sensitive information [274]. Implementing privacy-preserving data mining techniques in space data analytics platforms.
Security	Artificial Intelligence (AI) for threat detection: Using AI and machine learning to develop advanced threat detection systems that can identify and mitigate cyber attacks on DSNs in real-time [275], [275]. Researching adaptive AI models that can evolve with emerging cyber threats.
	Blockchain for secure communication: Exploring the use of blockchain technology [277] to secure communication channels and ensure data integrity and authenticity. Implementing decentralized blockchain networks for secure and tamper-proof space communications.
	Resilient Network Architectures: Developing resilient and adaptive network architectures [278] that can withstand cyber attacks and physical disruptions. Researching self-healing networks that can automatically reconfigure to maintain communication during failures.
	Post-quantum cryptography: Investigating cryptographic algorithms that are resistant to quantum attacks, ensuring the long-term security of DSNs. Implementing post-quantum cryptographic solutions in space communication systems [279]-[281].
	Satellite hardening: Researching techniques to harden satellites against physical tampering [282], space weather, and cosmic radiation. Developing materials and designs that enhance the durability and security of space-based communication assets.
	Secure ground stations: Enhancing the physical security of ground stations through advanced surveillance, access control, and intrusion detection systems [283]. Researching methods to secure the environmental resilience of ground stations against natural disasters.
Performance	Advanced modulation and coding techniques: Developing new modulation and coding techniques [284] to improve data rates and signal quality over long distances. Researching adaptive modulation schemes that can dynamically adjust based on signal conditions.
	Interference mitigation: Investigating methods to mitigate interference from space weather, cosmic radiation, and other sources [285]. Developing robust algorithms for real-time interference detection and correction.
	High-efficiency data compression: Researching innovative data compression algorithms that maximize bandwidth usage without compromising data quality [286], [287]. Implementing lossless and lossy compression techniques tailored for space communication.
	Dynamic spectrum management: Exploring dynamic spectrum management techniques [288] to optimize the allocation and usage of available frequencies. Developing algorithms for real-time spectrum allocation and interference avoidance.
	Fault-tolerant systems: Designing fault-tolerant communication systems [289] that can maintain operation despite hardware or software failures. Researching redundancy protocols that ensure continuous communication in the event of primary system failures.
	Predictive maintenance: Using AI and machine learning for predictive maintenance of both space-based and ground-based communication assets [290]. Developing models that can predict and preemptively address potential failures, ensuring higher reliability.

	Edge computing in space: Investigating the implementation of edge computing in space to process data closer to its source, reducing latency [291]. Developing lightweight, efficient edge computing nodes for spacecraft.
	Optimized data routing: Researching optimized data routing algorithms [292] that minimize latency and maximize throughput. Implementing real-time routing adjustments based on network conditions.

It is evident that future research in DNSs should focus on advancing encryption techniques, developing robust cyber-security measures, enhancing signal transmission and processing, and optimizing network performance. Collaborative efforts between space agencies, academic institutions, and industry partners are essential to address these challenges and ensure the successful communication for future space missions.

5. Conclusion

The research on DSNs highlights critical security, privacy, and performance challenges. Key security gaps include weak encryption, insufficient access controls, and vulnerability to cyber-attacks and interference. Privacy issues revolve around inadequate data transmission security, weak access controls, and poor data management. Performance challenges encompass signal attenuation, latency, bandwidth limitations, and data rate constraints. To address these, advanced encryption, comprehensive multi-factor authentication (MFA), role-based access controls (RBAC), anti-jamming techniques, and enhanced cybersecurity measures are recommended. Additionally, employing high-gain antennas, autonomous onboard systems, and adaptive data rate techniques will improve performance. Implementing these strategies ensures DSNs remain secure, private, and efficient, supporting future space missions effectively.

Compliance with ethical standards

Disclosure of conflict of interest

The author declares that he holds no conflict of interest.

References

[1] Asmar SW. Radio science techniques for deep space exploration. John Wiley & Sons, 2022 Mar 29.

[2] Arzo ST, Sikeridis D, Devetsikiotis M, Granelli F, Fierro R, Esmaeili M, Akhavan Z. Essential technologies and concepts for massive space exploration: Challenges and opportunities. IEEE Transactions on Aerospace and Electronic Systems. 2022 Apr 21, 59(1):3-29.

[3] Casanovas Ventura M. Study: An Assessment on the Requirements for Deep Space Optical Communications (Master's thesis, Universitat Politècnica de Catalunya).

[4] Tortora P, Modenini D, Zannoni M, Gramigna E, Strollo E, Togni A, Paolini E, Valentini L, Cocciolillo O, Simone L. Ground and Space Hardware for Interplanetary Communication Networks. InA Roadmap to Future Space Connectivity: Satellite and Interplanetary Networks 2023 Apr 6 (pp. 107-138). Cham: Springer International Publishing.

[5] Nasr M. Innovation Challenges in NASA's Planetary Program and a Policy Framework for Sustainable and Equitable Space Resource Utilization (Doctoral dissertation, Massachusetts Institute of Technology).

[6] Huff JD. Performance Characteristics of the Interplanetary Overlay Network in 10 Gbps Networks (Master's thesis, Ohio University).

[7] Zhang J, Li J. Laser Inter-Satellite Links Technology. John Wiley & Sons, 2023 Jan 5.

[8] 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.

[9] Alhilal AY, Braud T, Hui P. A roadmap toward a unified space communication architecture. IEEE Access. 2021 Jul 5, 9:99633-50.

[10] Betriu P, M. Sòria, Javier Franch Gutiérrez, Llopis M, Antoni Barlabé. An assessment of different relay network topologies to improve Earth–Mars communications. Acta Astronautica. 2023 May 1, 206:72–88.

[11] Farkasvölgyi A, László Csurgai-Horváth, Petr Boháček. The evolution of lunar communication—From the beginning to the present. International Journal of Satellite Communications and Networking. 2023 Nov 22,

[12] Janson S. The concept and history of small satellites. Elsevier eBooks. 2023 Jan 1, 9–55.

[13] Bhatta B. Global Navigation Satellite Systems: New Technologies and Applications. CRC Press, 2021 May 9.

[14] Bille MA, Ferguson M, Ingraham R, Khan M, Russell C. NASA's Explorer Program: An Overlooked Success. 2024 Jan 4,

[15] Kinnison J, Schlei W, Rogers G, Copeland D, Reza Ashtari, Rose C, et al. Interstellar Probe: A Practical Mission to Escape the Heliosphere. 2021 Mar 6,

[16] Evans B. NASA's voyager missions: exploring the outer solar system and beyond. Springer Nature, 2022 Aug 23.

[17] 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).

[18] Debnath S, Arif W, Roy S, Srimanta Baishya, Sen D. A Comprehensive Survey of Emergency Communication Network and Management. Wireless Personal Communications. 2021 Dec 1, 124(2):1375–421.

[19] Elewaily DI, Ali HA, Saleh AI, Abdelsalam MM. Delay/Disruption-Tolerant Networking-based the Integrated Deep-Space Relay Network: State-of-the-Art. Ad hoc networks. 2024 Jan 1, 152:103307–7.

[20] Vaezi M, Azari A, Khosravirad SR, Shirvanimoghaddam M, Azari MM, Chasaki D, Popovski P. Cellular, wide-area, and non-terrestrial IoT: A survey on 5G advances and the road toward 6G. IEEE Communications Surveys & Tutorials. 2022 Feb 11, 24(2):1117-74.

[21] Spyridon Daousis, Nikolaos Peladarinos, Vasileios Cheimaras, Panagiotis Papageorgas, Piromalis DD, Radu Adrian Munteanu. Overview of Protocols and Standards for Wireless Sensor Networks in Critical Infrastructures. Future Internet. 2024 Jan 21, 16(1):33–3.

[22] Xu D, Xu Y, Zhang X, Yu X, Song S, Schober R. Interference Mitigation for Network-Level ISAC: An Optimization Perspective. arXiv preprint arXiv:2402.09974. 2024 Feb 15.

[23] 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.

[24] Eliza M.-R. Kempton, Knutson HA. Transiting Exoplanet Atmospheres in the Era of JWST. Reviews in Mineralogy and Geochemistry. 2024 Jul 1, 90(1):411–64.

[25] Stewart E, Zelinskie A, Masetti M. Unfolding the Universe with the James Webb Space Telescope: Combining Art, Science, and Technology for Public Outreach. 2023 International Conference on Environmental Systems.

[26] 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.

[27] Vanacore C. Spacecraft Systems & Navigation. Spacecraft Systems & Navigation [Internet]. 2022 Nov 21 [cited 2024 Jul 29], i–194. Available from: https://commons.erau.edu/student-works/182/

[28] Kozorez DA, Krasilshchikov MN, Kruzhkov DM, Sypalo KI. Autonomous navigation during the final ascent of a spacecraft into the geostationary orbit. Autonomous integrated navigation system concept. Journal of Computer and Systems Sciences International. 2015 Sep, 54:798-807.

[29] 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.

[30] Dhamani N, Johnston MD, Lucena G. A demand access paradigm for nasa's deep space network.

[31] Sisay Tadesse Arzo, Riccardo Bassoli, Devetsikiotis M, Granelli F, Frank. Softwarization in Satellite and Interplanetary Networks. Signals and communication technology. 2023 Jan 1, 203–26.

[32] Priyadarshini I, Bhola B, Kumar R, So-In C. A novel cloud architecture for internet of space things (IoST). Ieee Access. 2022 Jan 18, 10:15118-34.

[33] Aslan Ö, Aktuğ SS, Ozkan-Okay M, Yilmaz AA, Akin E. A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. Electronics. 2023 Mar 11, 12(6):1333.

[34] Pavur J. Securing new space: on satellite cyber-security (Doctoral dissertation, University of Oxford).

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

[36] Jap JT. Validating Successful Data Transmission and Data Integrity.

[37] Abosata N, Al-Rubaye S, Inalhan G, Emmanouilidis C. Internet of things for system integrity: A comprehensive survey on security, attacks and countermeasures for industrial applications. Sensors. 2021 May 24, 21(11):3654.

[38] 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.

[39] Babuscia A. Telecommunication Systems for Small Satellites Operating at High Frequencies: A Review. Information. 2020 May 8, 11(5):258.

[40] 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).

[41] Marc Sanchez Net, Wyatt J, Castano R, Townes SA, Lazio JW, Malphrus BK, et al. Enabling a Larger Deep Space Mission Suite: A Deep Space Network Queuing Antenna for Demand Access. 2022 IEEE Aerospace Conference (AERO). 2022 Mar 5,

[42] Davarian F, Babuscia A, Baker J, Hodges R, Landau D, Lau CW, Lay N, Angert M, Kuroda V. Improving small satellite communications in deep space—a review of the existing systems and technologies with recommendations for improvement. part I: Direct to earth links and smallsat telecommunications equipment. IEEE Aerospace and Electronic Systems Magazine. 2020 Jul 1, 35(7):8-25.

[43] Goh E, Hamsa Shwetha Venkataram, Hoffmann M, Johnston MD, Wilson B. Scheduling the NASA Deep Space Network with Deep Reinforcement Learning. arXiv (Cornell University). 2021 Mar 6,

[44] Karmous S, Adem N, Atiquzzaman M, Sumudu Samarakoon. How Can Optical Communications Shape the Future of Deep Space Communications? A Survey. IEEE Communications Surveys & Tutorials. 2024 Jan 1, 1–1.

[45] Ledesma O, Lamo P, Fraire JA, Ruiz M, Sánchez MA. Architectural framework and feasibility of internet of things-driven mars exploration via satellite constellations. Electronics. 2024 Mar 30, 13(7):1289.

[46] Carter P, Cheung KM, Jun W, Kimmel E. An Expanded Deep Space Relay Architecture for Improved Communication and Navigation. 2024 Mar 2,

[47] 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.

[48] Bar-Sever Y, Burt E, Cheung KM, Ely T, Hamkins J, Lichten SM, Net MS, Ogbe D, Tjoelker R, Towfic Z, Yu N. Architectures and Technology Investment Priorities for Positioning, Navigation, and Timing at the Moon and Mars.

[49] Enes Koktas, Basar E. Communications for the Planet Mars: Past, Present, and Future. IEEE aerospace and electronic systems magazine. 2024 Jan 1, 1–35.

[50] Togni A. Deep and near space tracking stations in support of lunar and planetary exploration missions.

[51] Matthias Aichinger-Rosenberger, Wolf A, Senn C, Hohensinn R, Marcus Franz Glaner, Moeller G, et al. MPG-NET: A low-cost, multi-purpose GNSS co-location station network for environmental monitoring. Measurement. 2023 Jul 1, 216:112981–1.

[52] Xu Y, Larsson EG, Jorswieck EA, Li X, Jin S, Chang TH. Distributed Signal Processing for Extremely Large-Scale Antenna Array Systems: State-of-the-Art and Future Directions. arXiv preprint arXiv:2407.16121. 2024 Jul 23.

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

[54] Murray J, Arnold JA, Manis A, Matney M. Optimizing Altitude Sampling and Sensitivity with the Goldstone Orbital Debris Radar. In2nd International Orbital Debris Conference (IOC II) 2023 Dec 4.

[55] Majumdar AK. Technology Developments, Research Challenges, and Advances for FSO Communication for Space/Aerial/Terrestrial/Underwater (SATU) Links. Springer eBooks. 2022 Jan 1, 129–58.

[56] Fraire JA, Gasparini EL. Centralized and Decentralized Routing Solutions for Present and Future Space Information Networks. IEEE Network. 2021 Jul, 35(4):110–7.

[57] 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.

[58] Hirata A, Hirokawa J. High-Gain Antennas. Springer series in optical sciences/SPringer series in optical sciences. 2021 Dec 8, 155–60.

[59] Meor A, Mohamad Harris Misran, Mohd, Redzuan Abdul Manap, bin S, Shadia Suhaimi, et al. Innovation Design of High Gain Array Antenna for 5G Communication. International journal emerging technology and advanced engineering. 2023 Jul 16, 13(7):11–20.

[60] Ji X, Chen Y, Li J, Wang D, Zhao Y, Wu Q, Li M. Design of High-Gain Antenna Arrays for Terahertz Applications. Micromachines. 2024 Mar 18, 15(3):407.

[61] Nabil El Hassainate, Ahmed Oulad Said, Zouhair Guennoun. Circularly Polarized Square Patch Array Antenna with Circular Slot for Deep Space CubeSat Communication. 2024 Apr 24,

[62] Li C, Liu Y. Gain and bandwidth enhancement of low-profile unidirectional radiation spiral slot antenna. Microwave and Optical Technology Letters. 2023 Apr 19, 65(8):2436–42.

[63] Tran LT, Khuat CD, Phi LV. A Wideband, High Gain and Low Sidelobe Array Antenna for Modern ETC Systems. Applied Computational Electromagnetics Society journal. 2023 Sep 18,

[64] 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.

[65] E. Mazarico, Buccino D, Weiss BP, Dombard AJ, Genova A, Hussmann H, et al. The Europa Clipper Gravity and Radio Science Investigation. Space Science Reviews. 2023 May 8, 219(4).

[66] Wang C, Zhang Z, Wu J, Chen C, Gao F. An overview of protected satellite communications in intelligent age. Science China Information Sciences. 2021 May 10, 64(6).

[67] Raghunandan K. Satellite Communication. Textbooks in telecommunication engineering. 2022 Jan 1, 247–75.

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

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

[70] Stojče Dimov Ilčev. Ground Communication Segment. Springer eBooks. 2019 Dec 11, 227–313.

[71] 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.

[72] Li H, Li M. Analysis of the pattern recognition algorithm of broadband satellite modulation signal under deformable convolutional neural networks. Lv Z, editor. PLOS ONE. 2020 Jul 13, 15(7):e0234068.

[73] Athur Mugumya, Akankunda J, Matsiko E, Mohammed Dahiru Buhari. A review in advanced digital signal processing systems. Deleted Journal. 2024 May 19, 3(1):135–44.

[74] Dewa Made Wiharta, Nyoman Putra Sastra, Rama AAB. GPS-Based Rocket Payload Position Tracking System. Jurnal Sains dan Teknologi. 2023 Mar 29, 12(1):48–55.

[75] Zhan Y, Wan P, Jiang C, Pan X, Chen X, Guo S. Challenges and Solutions for the Satellite Tracking, Telemetry, and Command System. IEEE Wireless Communications. 2020 Dec, 27(6):12–8.

[76] 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.

[77] Mikhailik DA, Kozlov YV, Malygin IV. Design and Study of an Antenna System for Receiving Telemetry Information from Spacecraft Cubesat. 2022 Systems of Signals Generating and Processing in the Field of on Board Communications. 2022 Mar 15,

[78] You R, Gao W, Wu C, Li H. Technologies for spacecraft antenna engineering design. Springer, 2021.

[79] Sarieddeen H, Alouini MS, Al-Naffouri TY. An Overview of Signal Processing Techniques for Terahertz Communications. Proceedings of the IEEE. 2021 Oct, 109(10):1628–65.

[80] Farid Agayev, Almaz Mehdiyeva, Sevinj Bakhshaliyeva. Algorithm for Simplifying Procedures for Digital Measurement of Signal Parameters and Reducing Signal Errors. Algorithms for intelligent systems. 2024 Jan 1, 689–713.

[81] Modenini A, Ripani B. A Tutorial on the Tracking, Telemetry, and Command (TT&C) for Space Missions. IEEE Communications surveys and tutorials/IEEE communications surveys and tutorials. 2023 Jan 1, 25(3):1510–42.

[82] Alsalmani A. Design modular command and data handling subsystem hardware architectures.

[83] Zhang Qingjun, Jie L. Spacecraft System Design. CRC Press eBooks. Informa, 2023.

[84] 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.

[85] Song YJ, Hong S, Kim DG, Bang J, Bae J. Lessons learned from Korea Pathfinder Lunar Orbiter flight dynamics operations: NASA Deep Space Network interfaces and support levels. Journal of Astronomy and Space Sciences. 2023, 40(2):79-88.

[86] Yang L, Wang R, Liu X, Zhou Y, Liang J, Zhao K. An Experimental Analysis of Checkpoint Timer of Licklider Transmission Protocol for Deep-Space Communications. 2021 Jul 1,

[87] 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.

[88] Haldorai A. Deep Space Communications Current Trends, Technologies and Opportunities. Advances in Intelligent Systems and Technologies. 2022 Jul 30, 87–96.

[89] Virkler K, Soriano M, Pineda JL, Kocz J, Horiuchi S, McNichols T, et al. DSN Radio Astronomy Spectrometer. 2021 Aug 28,

[90] Pearlman AB, Majid WA, Prince TA. Observations of radio magnetars with the Deep Space Network. Advances in Astronomy. 2019, 2019(1):6325183.

[91] 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

[92] Wu W, Wang C, Liu Y, Qin L, Lin W, Ye S, et al. Frontier scientific questions in deep space exploration. Chinese Science Bulletin (Chinese Version). 2022 Nov 3, 68(6):606–27.

[93] Turan E, Speretta S, Gill E. Autonomous navigation for deep space small satellites: Scientific and technological advances. Acta Astronautica. 2022 Apr, 193:56–74.

[94] Zhou Y, Wang R, Yang L, Liang J, Burleigh SC, Zhao K. A Study of Transmission Overhead of a Hybrid Bundle Retransmission Approach for Deep-Space Communications. IEEE transactions on aerospace and electronic systems. 2022 Oct 1, 58(5):3824–39.

[95] Zhu X, Jiang C. Integrated Satellite-Terrestrial Networks Towards 6G: Architectures, Applications, and Challenges. IEEE Internet of Things Journal. 2021, 1–1.

[96] Niu Z, Shen XS, Zhang Q, Tang Y. Space-air-ground integrated vehicular network for connected and automated vehicles: Challenges and solutions. Intelligent and Converged Networks. 2020 Sep, 1(2):142–69.

[97] Sidhu JS, Joshi SK, Gündoğan M, Brougham T, Lowndes D, Mazzarella L, et al. Advances in space quantum communications. IET Quantum Communication. 2021 Jul 19, 2(4):182–217.

[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] Pavur J, Martinovic I. Building a launchpad for satellite cyber-security research: lessons from 60 years of spaceflight. Journal of Cybersecurity. 2022 Jan 1, 8(1):tyac008.

[100] Yue P, An J, Zhang J, Jia Y, Pan G, Wang Shuai, et al. Low Earth Orbit Satellite Security and Reliability: Issues, Solutions, and the Road Ahead. IEEE Communications Surveys and Tutorials. 2023 Jan 1, 1–1.

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

[102] Omolara AE, Alabdulatif A, Abiodun OI, Alawida M, Alabdulatif A, Arshad H. The internet of things security: A survey encompassing unexplored areas and new insights. Computers & Security. 2022 Jan 1, 112:102494.

[103] Bharati S, Podder P. Machine and Deep Learning for IoT Security and Privacy: Applications, Challenges, and Future Directions. Xiong J, editor. Security and Communication Networks. 2022 Aug 27, 2022:1–41.

[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] Vollmer B. NATOs Mission-Critical space capabilities under threat: cybersecurity gaps in the military space asset supply chain. arXiv preprint arXiv:2102.09674. 2021 Feb 18.

[106] Volini AG. A Deep Dive into Technical Encryption Concepts to Better Understand Cybersecurity & Data Privacy Legal & Policy Issues. J. Intell. Prop. L.. 2020, 28:291.

[107] Uher J, Harper J, Mennecke III RG, Patton P, Farroha B. Investigating end-to-end security in the fifth generation wireless capabilities and IoT extensions. InCyber Sensing 2016 2016 May 12 (Vol. 9826, pp. 51-66). SPIE.

[108] Adalier M, Burleigh S. Cross-domain Autonomous Communication Protocol for Delay Tolerant Networks. InNAECON 2018-IEEE National Aerospace and Electronics Conference 2018 Jul 23 (pp. 124-131). IEEE.

[109] Srivastava A, Gupta S, Quamara M, Chaudhary P, Aski VJ. Future IoT-enabled threats and vulnerabilities: State of the art, challenges, and future prospects. International Journal of Communication Systems. 2020 Aug, 33(12):e4443.

[110] 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.

[111] Ahilan A, Jeyam A. Breaking Barriers in Conventional Cryptography by Integrating with Quantum Key Distribution. Wireless Personal Communications. 2022 Nov 15,

[112] Lindsay JR. Demystifying the Quantum Threat: Infrastructure, Institutions, and Intelligence Advantage. Security Studies. 2020 Feb 7, 29(2):1–27.

[113] Marchese M, Morosi S, Patrone F. Intelligent Space Communication Networks. Signals and communication technology. 2023 Jan 1, 171–83.

[114] Yu J, Gong Y, Fang J, Zhang R, An J. Let us work together: Cooperative beamforming for UAV anti-jamming in space–air–ground networks. IEEE Internet of Things Journal. 2022 Feb 18, 9(17):15607-17.

[115] Mbarek B, Ge M, Pitner T. An adaptive anti-jamming system in HyperLedger-based wireless sensor networks. Wireless Networks. 2022 Jan 20, 28(2):691–703.

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

[118] Cetinkaya A, Kikuchi K, Hayakawa T, Ishii H. Randomized Transmission Protocols for Protection against Jamming Attacks in Multi-Agent Consensus. Automatica. 2020 Jul, 117:108960.

[119] Alipour-Fanid A, Dabaghchian M, Zeng K. Impact of Jamming Attacks on Vehicular Cooperative Adaptive Cruise Control Systems. IEEE Transactions on Vehicular Technology. 2020 Nov, 69(11):12679–93.

[120] Cherifi F, Omar M, Chenache T, Radji S. Efficient and lightweight protocol for anti-jamming communications in wireless body area networks. Computers & Electrical Engineering. 2022 Mar, 98:107698.

[121] M.N. Cankara, M.E. Cek. Covert Digital Communication Using Random Frequency Hopped Spread-Spectrum. 2021 13th International Conference on Electrical and Electronics Engineering (ELECO). 2021 Nov 25,

[122] 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.

[123] Wang H, Guo D, Zhang B. Compressive sampling for recognition of frequency-hopping spread spectrum signals. In2020 International Conference on Wireless Communications and Signal Processing (WCSP) 2020 Oct 21 (pp. 691-696). IEEE.

[124] Wang J, Liang Y, Xu X, Wang J, Zhong Y. A High Dynamic Velocity Locked Loop for the Carrier Tracking of a Wide-Band Hybrid Direct Sequence/Frequency Hopping Spread-Spectrum Signal. Electronics [Internet]. 2024 Jan 1 [cited 2024 Jul 30], 13(9):1794. Available from: https://www.mdpi.com/2079-9292/13/9/1794

[125] Chirov DS, Chertova OG, Lobov EM, Bazylev MV. Construction of a Communication Channel with UAVs Based on Direct Sequence Spread Spectrum Signals. 2024 Mar 12,

[126] Solouki MA, Angizi S, Violante M. Dependability in Embedded Systems: A Survey of Fault Tolerance Methods and Software-Based Mitigation Techniques. arXiv preprint arXiv:2404.10509. 2024 Apr 16.

[127] Khalaf M, Ayad A, Hossain M, Kassouf M, Deepa Kundur. A Survey on Cyber-Physical Security of Active Distribution Networks in Smart Grids. IEEE access. 2024 Jan 1, 1–1.

[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] Yu K, Tan L, Mumtaz S, Al-Rubaye S, Al-Dulaimi A, Bashir AK, Khan FA. Securing critical infrastructures: deep-learning-based threat detection in IIoT. IEEE Communications Magazine. 2021 Oct, 59(10):76-82.

[130] Almarri S, Frikha M. Authentication and Access Control Mechanisms to Secure IoT Environments: A comprehensive SLR.

[131] Obaidat MA, Obeidat S, Holst J, Al Hayajneh A, Brown J. A Comprehensive and Systematic Survey on the Internet of Things: Security and Privacy Challenges, Security Frameworks, Enabling Technologies, Threats, Vulnerabilities and Countermeasures. Computers. 2020 May 30, 9(2):44.

[132] Mogadem MM, Li Y, Meheretie DL. A survey on internet of energy security: related fields, challenges, threats and emerging technologies. Cluster Computing. 2021 Nov 2,

[133] Amachaghi EN, Shojafar M, Chuan Heng Foh, Moessner K. A Survey for Intrusion Detection Systems in Open RAN. IEEE access. 2024 Jan 1, 1–1.

[134] 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.

[135] Jangjou M, Sohrabi MK. A Comprehensive Survey on Security Challenges in Different Network Layers in Cloud Computing. Archives of Computational Methods in Engineering. 2022 Jan 24,

[136] Bhat S. Analysis of Cybersecurity for the Enterprise.

[137] Aboukadri S, Ouaddah A, Mezrioui A. Machine learning in identity and access management systems: Survey and deep dive. Computers & Security. 2024 Jan 23:103729.

[138] Abubakar MA. Blockchain-based Authentication and Access Control Mechanism for Internet of Things (IoT) (Doctoral dissertation).

[139] Kopra T. Increasing resilience in privileged access management.

[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] Singh SP, Afzal N. The MESA Security Model 2.0: A Dynamic Framework for Mitigating Stealth Data Exfiltration. arXiv preprint arXiv:2405.10880. 2024 May 17.

[142] Dammak M. Authentication and authorization security solution for the internet of thing (Doctoral dissertation, Université Bourgogne Franche-Comté, Université de la Manouba (Tunisie)).

[143] Kaushik K, Ouaissa M, Chaudhary A, editors. Advanced Techniques and Applications of Cybersecurity and Forensics. CRC Press, 2024 Jul 22.

[144] Bhushan B, Sahoo G, Rai AK. Man-in-the-middle attack in wireless and computer networking—A review. In2017 3rd International Conference on Advances in Computing, Communication & Automation (ICACCA)(Fall) 2017 Sep 15 (pp. 1-6). IEEE.

[145] Narang M, Aman Jatain, Nirmal Punetha. A Survey on Detection of Man-In-The-Middle Attack in IoMT Using Machine Learning Techniques. Algorithms for intelligent systems. 2024 Jan 1, 117–32.

[146] Zaman S, Alhazmi K, Aseeri MA, Ahmed MR, Khan RT, Kaiser MS, Mahmud M. Security threats and artificial intelligence based countermeasures for internet of things networks: a comprehensive survey. Ieee Access. 2021 Jun 16, 9:94668-90.

[147] 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.

[148] Le A, Roedig U, Rashid A. Lasarus: Lightweight attack surface reduction for legacy industrial control systems. InEngineering Secure Software and Systems: 9th International Symposium, ESSoS 2017, Bonn, Germany, July 3-5, 2017, Proceedings 9 2017 (pp. 36-52). Springer International Publishing.

[149] Wu Y, Ru Y, Lin Z, Liu C, Xue T, Zhao X, Chen J. Research on Cyber Attacks and Defensive Measures of Power Communication Network. IEEE Internet of Things Journal. 2022 Jun 9, 10(9):7613-35.

[150] Swain KP, Sharma A, Amey Karkare, Chakrabarti S, Gryazina E, Vladimir Terzija. Network-Level Vulnerability Assessment of Synchrophasor Measurement Devices. IEEE Access. 2024 Jan 1, 1–1.

[151] Batoul Achaal, Mehdi Adda, Berger M, Ibrahim H, Awde A. Study of smart grid cyber-security, examining architectures, communication networks, cyber-attacks, countermeasure techniques, and challenges. Cybersecurity. 2024 May 2, 7(1).

[152] Shinde O, Kulkarni V, Harsh Patani, Rajput A, Jaiswal RC. A Survey: Network Attack Detection and Mitigation Techniques. Lecture notes in networks and systems. 2024 Jan 1, 263–75.

[153] 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.

[154] Khalid H, Shaiful Jahari Hashim, Hashim F, Ameen W, Muhammad Akmal Chaudhary, Hamza. RAVEN: Robust Anonymous Vehicular End-to-End Encryption and Efficient Mutual Authentication for Post-Quantum Intelligent Transportation Systems. IEEE Transactions on Intelligent Transportation Systems. 2024 Jan 1, 1–13.

[155] Ullah S, Bazai SU, Imran M, Ilyas QM, Mehmood A, Saleem MA, Rafique MA, Haider A, Khan I, Iqbal S, Gulzar Y. Recent Developments in Authentication Schemes Used in Machine-Type Communication Devices in Machine-to-Machine Communication: Issues and Challenges. Computers, Materials & Continua. 2024 Apr 1, 79(1).

[156] Fatma Foad Ashrif, Sundararajan EA, Mohammad Kamrul Hasan, Ahmad R, Aisha-Hassan Abdalla Hashim, Azhar Abu Talib. Provably secured and lightweight authenticated encryption protocol in machine-to-machine communication in industry 4.0. Computer Communications. 2024 Mar 1, 218:263–75.

[157] Thankaraja Raja Sree, Harish R, T. Veni. FogSec: A secure and effective mutual authentication scheme for fog computing. Concurrency and computation. 2024 Feb 29, 36(12).

[158] Ahmed CA, Mohammad M, Mohammed A. An Effective Mechanism to Mitigate Packet Dropping Attack from MANETs using Chaotic Map based Authentication Technique. Recent Patents on Engineering. 2024 Apr 1, 18(3):66-76.

[159] 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.

[160] Sunil Prajapat, Kumar P, Kumar S. A privacy preserving quantum authentication scheme for secure data sharing in wireless body area networks. Cluster Computing. 2024 Apr 14,

[161] Sandeep Y, Venugopal P. In-depth evaluation of security requirements and attacks for secure data communication in ITS. InAIP Conference Proceedings 2024 Mar 26 (Vol. 2966, No. 1). AIP Publishing.

[162] Fatima Tu Zahra, Yavuz Selim Bostanci, Mujdat Soyturk. Security of Wireless IoT in Smart Manufacturing: Vulnerabilities and Countermeasures. Studies in computational intelligence. 2024 Jan 1, 419–41.

[163] Lee H, Lee H, Jun S, Kim HK. Expanding the Attack Scenarios of SAE J1939: A Comprehensive Analysis of Established and Novel Vulnerabilities in Transport Protocol. arXiv preprint arXiv:2406.00810. 2024 Jun 2.

[164] Ahmad U, Han M, Alireza Jolfaei, Jabbar S, Muhammad Ibrar, Aiman Erbad, et al. A Comprehensive Survey and Tutorial on Smart Vehicles: Emerging Technologies, Security Issues, and Solutions Using Machine Learning. IEEE Transactions on Intelligent Transportation Systems. 2024 Jan 1, 1–28.

[165] 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.

[166] Loukil S, Fourati LC, Nayyar A, So-In C. Investigation on security risk of LoRaWAN: Compatibility scenarios. IEEE Access. 2022 Sep 20, 10:101825-43.

[167] Gargoum S, Negar Yassaie, Al-Dabbagh AW, Feng C. A Data-Driven Framework for Verified Detection of Replay Attacks on Industrial Control Systems. IEEE Transactions on Automation Science and Engineering. 2024 Jan 1.

[168] Gao D, Ou L, Liu Y, Yang Q, Wang H. DeepSpoof: Deep Reinforcement Learning-Based Spoofing Attack in Cross-Technology Multimedia Communication. IEEE Transactions on Multimedia. 2024 Jan 1, 1–13.

[169] Slavica Tomović, Bogdan Krivokapić, Đula Nađ, Igor Radusinović. BEKMP: A Blockchain-Enabled Key Management Protocol for Underwater Acoustic Sensor Networks. IEEE Access. 2024 Jan 1, 1–1.

[170] Mutlaq KA, Nyangaresi VO, Omar MA, Abduljabbar ZA. Symmetric Key Based Scheme for Verification Token Generation in Internet of Things Communication Environment. InApplied Cryptography in Computer and Communications: Second EAI International Conference, AC3 2022, Virtual Event, May 14-15, 2022, Proceedings 2022 Oct 6 (pp. 46-64). Cham: Springer Nature Switzerland.

[171] Md. Ataullah, Chauhan N. Exploring security and privacy enhancement technologies in the Internet of Things: A comprehensive review. Security and Privacy. 2024 Jul 12,

[172] P. Kanaga Priya, R. Sivaranjani, Kumarasamy Thangaraj, Naif Alsharabi. Various Attacks on the Implementation of Cryptographic Algorithms. Springer eBooks. 2023 Jan 1, 221–58.

[173] Gómez-Marín E, Parrilla L, Tejero López JL, Morales DP, Castillo E. Toward Sensor Measurement Reliability in Blockchains. Sensors. 2023 Dec 6, 23(24):9659.

[174] Picek S, Perin G, Mariot L, Wu L, Batina L. SoK: Deep Learning-based Physical Side-channel Analysis. ACM Computing Surveys. 2023 Feb 9, 55(11):1–35.

[175] Adomas Baliuka, Stöcker M, Auer M, Freiwang P, Weinfurter H, Knips L. Deep-learning-based radio-frequency side-channel attack on quantum key distribution. Physical review applied. 2023 Nov 20, 20(5).

[176] 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.

[177] Aljuffri AA. Securing Power Side Channels by Design.

[178] Glamocanin O. Evaluating, Exploiting, and Hiding Power Side-Channel Leakage of Remote FPGAs. EPFL, 2023.

[179] Arsalan Javeed, Yilmaz C, Savas E. Microarchitectural Side-Channel Threats, Weaknesses and Mitigations: A Systematic Mapping Study. IEEE Access. 2023 Jan 1, 11:48945–76.

[180] Devi M, Majumder A. Side-Channel Attack in Internet of Things: A Survey. Lecture notes in networks and systems. 2020 Aug 4, 213–22.

[181] Tosun T, Savas E. Zero-Value Filtering for Accelerating Non-Profiled Side-Channel Attack on Incomplete NTT based Implementations of Lattice-based Cryptography. IEEE Transactions on Information Forensics and Security. 2024 Jan 29.

[182] 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.

[183] Zunaidi MR, Sayakkara A, Scanlon M. Revealing IoT Cryptographic Settings through Electromagnetic Side-Channel Analysis. Electronics. 2024 Apr 20, 13(8):1579.

[184] Zajić A, Prvulovic M. Understanding Analog Side Channels Using Cryptography Algorithms. Springer, 2023 Sep 30.

[185] Zunaidi MR, Sayakkara A, Scanlon M. Systematic Literature Review of EM-SCA Attacks on Encryption. arXiv preprint arXiv:2402.10030. 2024 Feb 15.

[186] Monfared SK, Forte D, Tajik S. RandOhm: Mitigating Impedance Side-channel Attacks using Randomized Circuit Configurations. arXiv preprint arXiv:2401.08925. 2024 Jan 17.

[187] Xie Y, Jiang X, Gong G, Jiang Z, Jin G, Chen H. Yinker: A flexible BBR to achieve the high-throughput and low-latency data transmission over Wi-Fi and 5G networks. Computer Networks. 2023 Feb 1, 222:109530.

[188] 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.

[189] Bassel Al Homssi, Kosta Dakic, Wang K, Tansu Alpcan, Allen B, Boyce R, et al. Artificial Intelligence Techniques for Next-Generation Massive Satellite Networks. IEEE Communications Magazine. 2023 Jan 1, 1–7.

[190] Mohsan SAH, Khan MA, Amjad H. Hybrid FSO/RF networks: A review of practical constraints, applications and challenges. Optical Switching and Networking. 2023 Feb, 47:100697.

[191] Guo Y, Ruan K, Wang GS, Gu J. Advances and mechanisms in polymer composites toward thermal conduction and electromagnetic wave absorption. Science Bulletin. 2023 Jun 1, 68(11):1195–212.

[192] Qin M, Zhang L, Wu H. Dielectric Loss Mechanism in Electromagnetic Wave Absorbing Materials. Advanced Science. 2022 Feb 7, 9(10):2105553.

[193] Wang C, Zhang Z, Wu J, Chen C, Gao F. An overview of protected satellite communications in intelligent age. Science China Information Sciences. 2021 May 10, 64(6).

[194] Kulkarni J, Sim CYD, Jawad Yaseen Siddiqui, Apte AM, Ajay Kumar Poddar, Rohde UL. Multifunctional and Multiband Planar Antennas for Emerging Wireless Applications. CRC Press, 2023.

[195] Honi DG, Ali AH, Abduljabbar ZA, Ma J, Nyangaresi VO, Mutlaq KA, Umran SM. Towards Fast Edge Detection Approach for Industrial Products. In2022 IEEE 21st International Conference on Ubiquitous Computing and Communications (IUCC/CIT/DSCI/SmartCNS) 2022 Dec 19 (pp. 239-244). IEEE.

[196] Priyadarshani R, Park KH, Ata Y, Alouini MS. Jamming Intrusions in Extreme Bandwidth Communication: A Comprehensive Overview. arXiv preprint arXiv:2403.19868. 2024 Mar 28.

[197] Davarian F, Asmar S, Angert M, Baker J, Gao J, Hodges R, Israel D, Landau D, Lay N, Torgerson L, Walsh W. Improving small satellite communications and tracking in deep space—a review of the existing systems and technologies with recommendations for improvement. Part II: small satellite navigation, proximity links, and communications link science. IEEE Aerospace and Electronic Systems Magazine. 2020 Jul 1, 35(7):26-40.

[198] Chaine PJ. Suitability of Time Sensitive Networking for spacecraft industry requirement (Doctoral dissertation, Institut Supérieur de l'Aéronautique et de l'Espace (ISAE)).

[199] Feldmann M, Fraire JA, Walter F, Burleigh S. Ring Road Networks: Access for Anyone. IEEE Communications Magazine. 2022 Apr 1, 60(4):38–44.

[200] Alhilal A, Braud T, Hui P. The sky is NOT the limit anymore: Future architecture of the interplanetary Internet. IEEE Aerospace and Electronic Systems Magazine. 2019 Aug 1, 34(8):22-32.

[201] 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.

[202] Ji Hyun Nam, Brandt E, Bauer S, Liu X, Renna M, Tosi A, et al. Low-latency time-of-flight non-line-of-sight imaging at 5 frames per second. Nature Communications. 2021 Nov 11, 12(1).

[203] Claudia de Rham, Tolley AJ. Causality in curved spacetimes: The speed of light and gravity. 2020 Oct 20, 102(8).

[204] Chaccour C, Soorki MN, Saad W, Bennis M, Popovski P. Can Terahertz Provide High-Rate Reliable Low Latency Communications for Wireless VR? IEEE Internet of Things Journal. 2022, 1–1.

[205] Karetsi F, Papapetrou E. Lightweight network-coded ARQ: An approach for Ultra-Reliable Low Latency Communication. Computer Communications. 2022 Mar, 185:118–29.

[206] Goddard RH. Goddard Space Flight Center.

[207] 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.

[208] Buitrago-Leiva JN, Camps A, Moncada Niño A. Considerations for Eco-LeanSat Satellite Manufacturing and Recycling. Sustainability. 2024 Jun 8, 16(12):4933.

[209] Sun Y, Peng M, Zhang S, Lin G, Zhang P. Integrated Satellite-Terrestrial Networks: Architectures, Key Techniques, and Experimental Progress. IEEE Network. 2022 Nov 1, 36(6):191–8.

[210] 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, 2:1505–25.

[211] Wang Y, Su Z, Ni J, Zhang N, Shen X. Blockchain-Empowered Space-Air-Ground Integrated Networks: Opportunities, Challenges, and Solutions. IEEE Communications Surveys & Tutorials. 2021, 1–1.

[212] Polese M, Cantos-Roman X, Singh A, Marcus MJ, Maccarone TJ, Melodia T, Jornet JM. Coexistence and spectrum sharing above 100 GHz. Proceedings of the IEEE. 2023 Jul 3.

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

[214] Kufakunesu R, Hancke GP, Abu-Mahfouz AM. A survey on adaptive data rate optimization in lorawan: Recent solutions and major challenges. Sensors. 2020 Sep 5, 20(18):5044.

[215] Rathore RS, Sangwan S, Kaiwartya O, Aggarwal G. Green Communication for Next-Generation Wireless Systems: Optimization Strategies, Challenges, Solutions, and Future Aspects. Cano JC, editor. Wireless Communications and Mobile Computing. 2021 May 25, 2021:1–38.

[216] Srivastava V, Tripathi S, Singh K, Son LH. Energy efficient optimized rate based congestion control routing in wireless sensor network. Journal of Ambient Intelligence and Humanized Computing. 2019 Sep 19, 11(3):1325–38.

[217] 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.

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

[219] Racionero-Garcia J, Siraj Ahmed Shaikh. Space and Cybersecurity: Challenges and Opportunities Emerging from National Strategy Narratives. 2024 Jan 1,

[220] Singh K, Yadav M, Singh Y, Barak D. Finding Security Gaps and Vulnerabilities in IoT Devices. Advances in environmental engineering and green technologies book series. 2024 Jun 14, 379–95.

[221] P. Swathika, J. Raja Sekar. Role-based Access and Advanced Encryption Techniques Ensure Cloud Data Security in Data Deduplication Schemes. 2023 Oct 11,

[222] Kumar Y, Kumar V. A Systematic Review on Intrusion Detection System in Wireless Networks: Variants, Attacks, and Applications. Wireless Personal Communications. 2023 Nov, 133(1):395-452.

[223] Rai N, Badrinath AR, Kamath A, Kumar VA, Gatti RR. Security Challenges of IoT-Enabled Vehicular Communications and Their Countermeasures. InCommunication Technologies and Security Challenges in IoT: Present and Future 2024 Mar 26 (pp. 351-368). Singapore: Springer Nature Singapore.

[224] 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.

[225] Schraml MG, Knopp A. Precoding for Security Gap Physical Layer Security in Multiuser MIMO Satellite Systems. MILCOM 2022 - 2022 IEEE Military Communications Conference (MILCOM). 2022 Nov 28,

[226] Bartusiak A, Lassig J, Nicolai S, Bretschneider P. Extended Gap Analysis: an Approach for Security Assessment of Critical Infrastructures. 2022 International Conference on Smart Energy Systems and Technologies (SEST). 2022 Sep 5,

[227] None Oluwatoyin Ajoke Fayayola, None Oluwabukunmi Latifat Olorunfemi, Olaseni P. DATA PRIVACY AND SECURITY IN IT: A REVIEW OF TECHNIQUES AND CHALLENGES. Computer science & IT research journal. 2024 Mar 18, 5(3):606–15.

[228] Taduri Suneetha, Dr Jai Bhagwan. A Secure Framework For Enhancing Data Privacy And Access Control In Healthcare Cloud Management Systems. 2024 May 4,

[229] Srikanth GU, Geetha R, Prabhu S. An efficient Key Agreement and Authentication Scheme (KAAS) with enhanced security control for IIoT systems. International Journal of Information Technology. 2023 Mar, 15(3):1221-30.

[230] 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.

[231] Yogeshwar Dutt Sharma, Bancha Luadang, Karthik Rudramuni, Abhishek Kandwal. High Gain Metamaterial Antenna for High Data Rate Mm-Wave Communication Systems. 2024 Feb 29

[232] Karim R, Iftikhar A, Ramzan R. Performance-Issues-Mitigation-Techniques for On-Chip-Antennas – Recent Developments in RF, MM-Wave, and Thz Bands With Future Directions. IEEE Access. 2020, 8:219577–610.

[233] Morais DH. Performance Optimization Techniques. Springer eBooks. 2021 Jan 1, 117–65.

[234] Viswanadha K, S. N. Design of High Gain, Bandwidth and Efficient Double Split Ring Slotted Antenna with Swastika Shape EBG Structures at 21.29GHz for High Data Rate Communications. International Journal of Computer Applications. 2018 Jan 17, 180(11):35–8.

[235] Fang X, Feng W, Chen Y, Ge N, Zheng G. Control-Oriented Deep Space Communications For Unmanned Space Exploration. IEEE Transactions on Wireless Communications. 2024 Jun 24.

[236] Ficco M, Granata D, Palmieri F, Rak M. A systematic approach for threat and vulnerability analysis of unmanned aerial vehicles. Internet of Things. 2024 Jul 1, 26:101180.

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

[238] Housen-Couriel D. IAC-21-E-9 (Paper ID: 67116) Information sharing for the mitigation of outer space–related cybersecurity threats. Acta Astronautica. 2023 Feb 1, 203:546-50.

[239] Bhushan B, Sahoo G. Recent advances in attacks, technical challenges, vulnerabilities and their countermeasures in wireless sensor networks. Wireless Personal Communications. 2018 Jan, 98:2037-77.

[240] 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.

[241] Li C, Sun X, Zhang Z. Effective methods and performance analysis of a satellite network security mechanism based on blockchain technology. IEEE Access. 2021 Aug 16, 9:113558-65.

[242] 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.

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

[244] Liu H, Tronchetti F. The Exclusive Utilization Space: A New Approach to the Management and Utilization of the Near Space. U. Pa. J. Int'l L.. 2018, 40:537.

[245] Kush RD, Warzel D, Kush MA, Sherman A, Navarro EA, Fitzmartin R, Pétavy F, Galvez J, Becnel LB, Zhou FL, Harmon N. FAIR data sharing: the roles of common data elements and harmonization. Journal of biomedical informatics. 2020 Jul 1, 107:103421.

[246] Guzman M, Hein AM, Welch C. Extremely long-duration storage concepts for space. Acta Astronautica. 2017 Jan 1, 130:128-36.

[247] Danezis G, Domingo-Ferrer J, Hansen M, Hoepman JH, Metayer DL, Tirtea R, Schiffner S. Privacy and data protection by design-from policy to engineering. arXiv preprint arXiv:1501.03726. 2015 Jan 12.

[248] Zhuo M, Liu L, Zhou S, Tian Z. Survey on security issues of routing and anomaly detection for space information networks. Scientific Reports. 2021 Nov 15, 11(1):22261.

[249] Sfar AR, Natalizio E, Challal Y, Chtourou Z. A roadmap for security challenges in the Internet of Things. Digital Communications and Networks. 2018 Apr 1, 4(2):118-37.

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

[251] 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.

[252] Falco G. The vacuum of space cyber security. In2018 AIAA SPACE and Astronautics Forum and Exposition 2018 (p. 5275).

[253] Murtaza A, Pirzada SJ, Xu T, Jianwei L. Orbital debris threat for space sustainability and way forward. IEEE access. 2020 Mar 9, 8:61000-19.

[254] Davis A, Chang H. Airport protection using wireless sensor networks. In2012 IEEE Conference on Technologies for Homeland Security (HST) 2012 Nov 13 (pp. 36-42). IEEE.

[255] Yaacoub JP, Noura H, Salman O, Chehab A. Security analysis of drones systems: Attacks, limitations, and recommendations. Internet of Things. 2020 Sep 1, 11:100218.

[256] Abraham DS, MacNeal BE, Heckman DP, Chen Y, Wu JP, Tran K, Kwok A, Lee CA. Recommendations emerging from an analysis of NASA's deep space communications capacity. Space Operations: Inspiring Humankind's Future. 2019:475-511.

[257] Ma Z, Xiao M, Xiao Y, Pang Z, Poor HV, Vucetic B. High-reliability and low-latency wireless communication for internet of things: Challenges, fundamentals, and enabling technologies. IEEE Internet of Things Journal. 2019 Mar 25, 6(5):7946-70.

[258] Guo AY, Tran MC, Childs AM, Gorshkov AV, Gong ZX. Signaling and scrambling with strongly long-range interactions. Physical Review A. 2020 Jul, 102(1):010401.

[259] Hapgood M. Linking Space Weather Science to Impacts—The View From the Earth. InExtreme events in Geospace 2018 Jan 1 (pp. 3-34). Elsevier.

[260] Jahid A, Alsharif MH, Hall TJ. A contemporary survey on free space optical communication: Potentials, technical challenges, recent advances and research direction. Journal of network and computer applications. 2022 Apr 1, 200:103311.

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

[262] Chen S, Liang YC, Sun S, Kang S, Cheng W, Peng M. Vision, requirements, and technology trend of 6G: How to tackle the challenges of system coverage, capacity, user data-rate and movement speed. IEEE Wireless Communications. 2020 Feb 19, 27(2):218-28.

[263] Sani Y, Mauthe A, Edwards C. Adaptive bitrate selection: A survey. IEEE Communications Surveys & Tutorials. 2017 Jul 12, 19(4):2985-3014.

[264] Lu Y, Shao Q, Yue H, Yang F. A review of the space environment effects on spacecraft in different orbits. IEEE access. 2019 Jul 10, 7:93473-88.

[265] Koren I, Krishna CM. Fault-tolerant systems. Morgan Kaufmann, 2020 Sep 1.

[266] Nowell B, Bodkin CP, Bayoumi D. Redundancy as a strategy in disaster response systems: A pathway to resilience or a recipe for disaster?. Journal of Contingencies and Crisis Management. 2017 Sep, 25(3):123-35.

[267] Senescu RR, Haymaker JR, Meža S, Fischer MA. Design process communication methodology: Improving the effectiveness and efficiency of collaboration, sharing, and understanding. Journal of Architectural Engineering. 2014 Mar 1, 20(1):05013001.

[268] Cao Y, Zhao Y, Wang Q, Zhang J, Ng SX, Hanzo L. The evolution of quantum key distribution networks: On the road to the qinternet. IEEE Communications Surveys & Tutorials. 2022 Jan 18, 24(2):839-94.

[269] Goyal HR, Shnain AH, Dixit KK, Kumar M, Khurana P, Harikrishna M. Secure and Efficient Data Fusion in IoT Systems Using Homomorphic Encryption and Machine Learning. In2024 International Conference on Communication, Computer Sciences and Engineering (IC3SE) 2024 May 9 (pp. 1634-1639). IEEE.

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

[271] Hassan MU, Rehmani MH, Chen J. Differential privacy techniques for cyber physical systems: A survey. IEEE Communications Surveys & Tutorials. 2019 Oct 1, 22(1):746-89.

[272] Zhao C, Zhao S, Zhao M, Chen Z, Gao CZ, Li H, Tan YA. Secure multi-party computation: theory, practice and applications. Information Sciences. 2019 Feb 1, 476:357-72.

[273] Sampaio S, Sousa PR, Martins C, Ferreira A, Antunes L, Cruz-Correia R. Collecting, processing and secondary using personal and (pseudo) anonymized data in smart cities. Applied Sciences. 2023 Mar 16, 13(6):3830.

[274] Zhang J, Chen B, Zhao Y, Cheng X, Hu F. Data security and privacy-preserving in edge computing paradigm: Survey and open issues. IEEE access. 2018 Mar 28, 6:18209-37.

[275] Maddireddy BR, Maddireddy BR. Proactive Cyber Defense: Utilizing AI for Early Threat Detection and Risk Assessment. International Journal of Advanced Engineering Technologies and Innovations. 2020 Dec 12, 1(2):64-83.

[276] Ghrabat MJ, Hussien ZA, Khalefa MS, Abduljabba ZA, Nyangaresi VO, Al Sibahee MA, Abood EW. Fully automated model on breast cancer classification using deep learning classifiers. Indonesian Journal of Electrical Engineering and Computer Science. 2022 Oct, 28(1):183-91.

[277] Li X, Wei L, Wang L, Ma Y, Zhang C, Sohail M. A blockchain-based privacy-preserving authentication system for ensuring multimedia content integrity. International Journal of Intelligent Systems. 2022 May, 37(5):3050-71.

[278] Shahab E, Taleb M, Gholian-Jouybari F, Hajiaghaei-Keshteli M. Designing a resilient cloud network fulfilled by reinforcement learning. Expert Systems with Applications. 2024 Dec 1, 255:124606.

[279] Halak B, Gibson T, Henley M, Botea CB, Heath B, Khan S. Evaluation of performance, energy, and computation costs of quantum-attack resilient encryption algorithms for embedded devices. IEEE Access. 2024 Jan 8.

[280] 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.

[281] Joseph D, Misoczki R, Manzano M, Tricot J, Pinuaga FD, Lacombe O, Leichenauer S, Hidary J, Venables P, Hansen R. Transitioning organizations to post-quantum cryptography. Nature. 2022 May 12, 605(7909):237-43.

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

[283] Radoglou-Grammatikis PI, Sarigiannidis PG. Securing the smart grid: A comprehensive compilation of intrusion detection and prevention systems. Ieee Access. 2019 Apr 9, 7:46595-620.

[284] Shen P, Wu Y, Luo Z, Wu Z, Jing J, Zhang H. Advanced Orthogonal Frequency and Phase Modulated Waveform for Ultrasonic Phased Array TFM Detection in CFRP Composites. IEEE Transactions on Instrumentation and Measurement. 2024 Mar 18, 73:1-0.

[285] Zheng Y, Ganushkina NY, Jiggens P, Jun I, Meier M, Minow JI, O'Brien TP, Pitchford D, Shprits Y, Tobiska WK, Xapsos MA. Space radiation and plasma effects on satellites and aviation: Quantities and metrics for tracking performance of space weather environment models. Space Weather. 2019 Oct, 17(10):1384-403.

[286] Song L, Ma W, Liu Z, Shi Z. Application of optimized sparse encoding algorithm in data compression. Digital Signal Processing. 2024 Aug 1, 151:104549.

[287] 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).

[288] Kakar J, Marojevic V. Waveform and spectrum management for unmanned aerial systems beyond 2025. In2017 IEEE 28th Annual international symposium on personal, indoor, and mobile radio communications (PIMRC) 2017 Oct 8 (pp. 1-5). IEEE.

[289] Ferreira FH, Nakagawa EY, Bertolino A, Lonetti F, de Oliveira Neves V, dos Santos RP. A framework for the design of fault-tolerant systems-of-systems. Journal of Systems and Software. 2024 May 1, 211:112010.

[290] Feruglio L, Benetton A, Varile M, Vittori D, Bloise I, Maderna R, Cardenio C, Madonia P, Rossi F, Azza FP, De Marchi P. Future-ready space missions enabled by end-to-end AI adoption. InArtificial Intelligence for Space: AI4SPACE 2023 Dec 18 (pp. 303-360). CRC Press.

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

[292] Suresh SS, Prabhu V, Parthasarathy V, Senthilkumar G, Gundu V. Intelligent data routing strategy based on federated deep reinforcement learning for IOT-enabled wireless sensor networks. Measurement: Sensors. 2024 Feb 1, 31:101012.