Journal of *Cybersecurity and Privacy*

MDPI

Review

Cyber Attacks on Space Information Networks: Vulnerabilities, Threats, and Countermeasures for Satellite Security

Afsana Sharmin [1,*], Bahar Uddin Mahmud [1], Norun Nabi [2], Mujiba Shaima [3] and Md Jobair Hossain Faruk [4,*]

[1] Department of Computer Science, Western Michigan University, Kalamazoo, MI 49008, USA; baharuddin.mahmud@wmich.edu
[2] Department of Computer Science, Washington University of Science and Technology (WUST), Alexandria, VA 22314, USA; norunnabinishan@gmail.com
[3] Department of Computer Science, Monroe University, Bronx, NY 10468, USA; shaimacme@gmail.com
[4] Department of Computer Science, New York Institute of Technology, Broadway, NY 10023, USA
* Correspondence: afsana.sharmin@wmich.edu (A.S.); jobair.upsi16@gmail.com (M.J.H.F.)

Abstract

The growing reliance on satellite-based infrastructures for communication, navigation, defense, and environmental monitoring has magnified the urgency of securing Space Information Networks (SINs) against cyber threats. This paper presents a comprehensive review of the vulnerabilities, threat vectors, and advanced countermeasures impacting SINs. Key vulnerabilities, including system complexity, use of Commercial Off-the-Shelf (COTS) components, lack of standardized security frameworks, and emerging quantum threats, are critically analyzed. This paper classifies cyber threats into active and passive categories, highlighting real-world case studies such as Denial-of-Service attacks, message modification, eavesdropping, and satellite transponder hijacking. A detailed survey of countermeasures follows, focusing on AI-driven intrusion detection, federated learning approaches, deep learning techniques, random routing algorithms, and quantum-resistant encryption. This study emphasizes the pressing need for integrated, resilient, and proactive security architectures tailored to the unique constraints of space systems. It concludes by identifying research gaps and recommending future directions to enhance the resilience of SINs against evolving cyber threats in an increasingly contested space environment.

Keywords: space information networks; satellite cybersecurity; satellite communication; security; space security; space systems vulnerabilities

Received: 29 July 2025
Revised: 29 August 2025
Accepted: 15 September 2025
Published: 17 September 2025

Citation: Sharmin, A.; Mahmud, B.U.; Nabi, N.; Shaima, M.; Faruk, M.J.H. Cyber Attacks on Space Information Networks: Vulnerabilities, Threats, and Countermeasures for Satellite Security. *J. Cybersecur. Priv.* **2025**, *5*, 76. https://doi.org/10.3390/jcp5030076

1. Introduction

The expansion of space-based infrastructure has ushered in a new era of global interconnectivity, empowering sectors such as communication, navigation, environmental monitoring, military surveillance, and scientific research. At the core of this evolution lies the concept of Space Information Networks (SINs)—complex, heterogeneous architectures that integrate satellites, ground stations, inter-satellite links (ISLs), and terrestrial networks to form dynamic and data-driven communication ecosystems [1].

The interdisciplinary nature of CubeSat cybersecurity, combining elements of aerospace engineering, computer science, and multiphysics modeling, adds complexity and innovation to the design of resilient space systems. The growing use of CubeSats in modern space missions introduces additional cybersecurity challenges due to their reliance on Commercial Off-The-Shelf (COTS) components and open-source systems [2]. The convergence of Low Earth Orbit (LEO) satellite constellations with terrestrial broadband

services, the adoption of cloud-based ground infrastructure, and the integration of 5G for seamless interoperability illustrate how the satellite communication industry is evolving and aligning with next-generation technologies. These advancements enable global Internet coverage, low-latency data transmission, and support for emerging applications such as autonomous systems and Internet of Things (IoT) integration [3].

However, the rapid digitization and increasing reliance on Commercial Off-the-Shelf (COTS) components, software-defined networking, and the Internet of Space Things (IoST) have significantly expanded the attack surface of SINs [3,4]. Unlike terrestrial systems, space systems are constrained by long development lifecycles, limited computational resources, and physical inaccessibility once deployed—making them particularly vulnerable to persistent and evolving cyber threats.

High-profile incidents and test attacks have shown that a wide range of adversaries, including nation-states, cybercriminals, and insiders, can exploit weaknesses in space systems. They have been able to disrupt satellite telemetry, hijack control signals, spoof navigation, and steal sensitive data [5]. Threats like jamming, spoofing, DDoS, unauthorized access, eavesdropping, zero-day attacks, and supply chain breaches highlight the urgent need for strong, flexible, and scalable security solutions to protect Space Information Networks.

The rise of Low Earth Orbit (LEO) constellations, especially large commercial mega-constellations, has added new layers of complexity to SIN security. These networks depend on fast, automated link-switching and edge computing, making it even harder to detect intrusions and respond to incidents quickly [6]. At the same time, advances in quantum computing and increasingly sophisticated cyber attacks are putting traditional cryptographic protections at risk. To stay ahead, the space sector must shift toward a proactive, forward-looking approach to cybersecurity.

Although there is growing attention from governments and space agencies, cybersecurity for Space Information Networks (SINs) remains inconsistent, with little standardization and few real-world implementations. A clear understanding of vulnerabilities, threats, and defenses is essential to protect these critical systems.

Objectives and Contributions

This survey addresses the urgent need for a systematic study of cyber threats facing SINs. Our primary objectives are as follows:

- Identify and categorize the major vulnerabilities that render SINs susceptible to cyber attacks, including technical, organizational, and architectural weaknesses.
- Present a taxonomy of threat types within the SIN domain.
- Review and critically assess current countermeasures, including artificial intelligence (AI), federated learning, deep learning techniques, random-routing techniques, and quantum computing.
- Highlight key research challenges and propose future directions for securing SINs against advanced persistent threats.

2. Review Methodology and Literature Selection

To ensure a comprehensive and balanced perspective on the cybersecurity landscape of Space Information Networks, a systematic literature review methodology was adopted. The goal was to identify, categorize, and synthesize the most relevant and high-quality research addressing vulnerabilities, threats, and countermeasures related to satellite-based communication systems.

2.1. Search Strategy

The literature search was conducted using major academic databases including Google Scholar, IEEE Xplore, SpringerLink, ScienceDirect, and ACM Digital Library. Additional sources included policy reports, white papers, and standards documentation. To ensure comprehensive coverage, Boolean operators were applied to combine synonyms and acronyms. An example of the full Boolean search string is provided below:

("cybersecurity" OR "information security" OR "network security") AND ("space systems" OR "satellite communication" OR "space information networks" OR "SINs") AND ("cyber attack" OR "threat detection" OR "intrusion detection" OR "vulnerabilities") AND ("artificial intelligence" OR "AI" OR "machine learning" OR "deep learning" OR "federated learning").

2.2. Inclusion and Exclusion Criteria

To ensure the relevance and quality of the sources, the following criteria were used:

- Inclusion: Peer-reviewed articles, published conference proceedings, and preprints (from 2006 to 2025) that directly address cyber threats, vulnerabilities, defense mechanisms, or resilience strategies for space or satellite-based systems.
- Exclusion: Articles focused solely on non-space terrestrial cybersecurity, non-peer-reviewed blog posts or news, and publications without technical contributions.

2.3. Screening Process

An initial pool of over 220 publications was retrieved. After title and abstract screening, 92 papers were shortlisted for full-text review. Following a deeper evaluation of methodology relevance and data richness, 48 high-impact articles were selected for detailed analysis. As shown in Figure 1, the PRISMA flowchart demonstrates the systematic process of identifying, screening, and including studies for the review. These include foundational works such as [1,4,5,7,8], as well as recent innovations in AI-driven threat detection and federated learning [9,10].

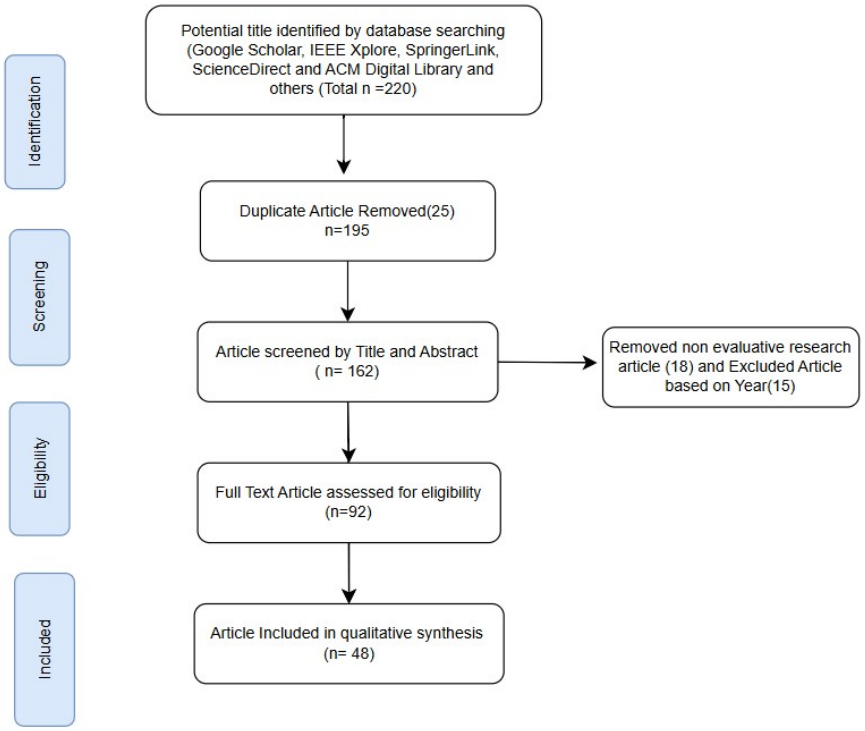

Figure 1. PRISMA flowchart depicting the article search process.

2.4. Categorization Framework

The selected literature was organized into three primary thematic categories:

1. Vulnerabilities: Systemic weaknesses and risks inherent in space systems and their interconnections.
2. Threats: Existing and emerging cyber attack types targeting satellite systems.
3. Countermeasures: Detection, prevention, and response strategies, including AI/ML, encryption, and quantum computing.

3. Background on Space Information Networks (SINs)

3.1. Definition and Architecture

Space Information Networks (SINs) refer to the integrated communication systems that link multiple satellites, ground control stations, and user terminals into a cohesive, information-centric network. Unlike traditional point-to-point satellite links, SINs leverage inter-satellite links (ISLs), onboard processing, and data relay mechanisms to enable autonomous data routing, in-network computation, and real-time situational awareness [1].

Figure 2 illustrates the three key segments of Space Information Networks, space, ground, and user segments, highlighting their roles in satellite communication and data processing.

- Space segment: Includes satellites in various orbits (LEO, MEO, GEO) equipped with communication payloads, sensors, and ISL capabilities.
- Ground segment: Consists of mission control centers, data processing stations, and antenna arrays responsible for uplink/downlink operations, tasking, and telemetry tracking.
- User segment: Encompasses terminals and receiving stations utilized by end-users in domains such as defense, navigation, environmental monitoring, and telecommunications.

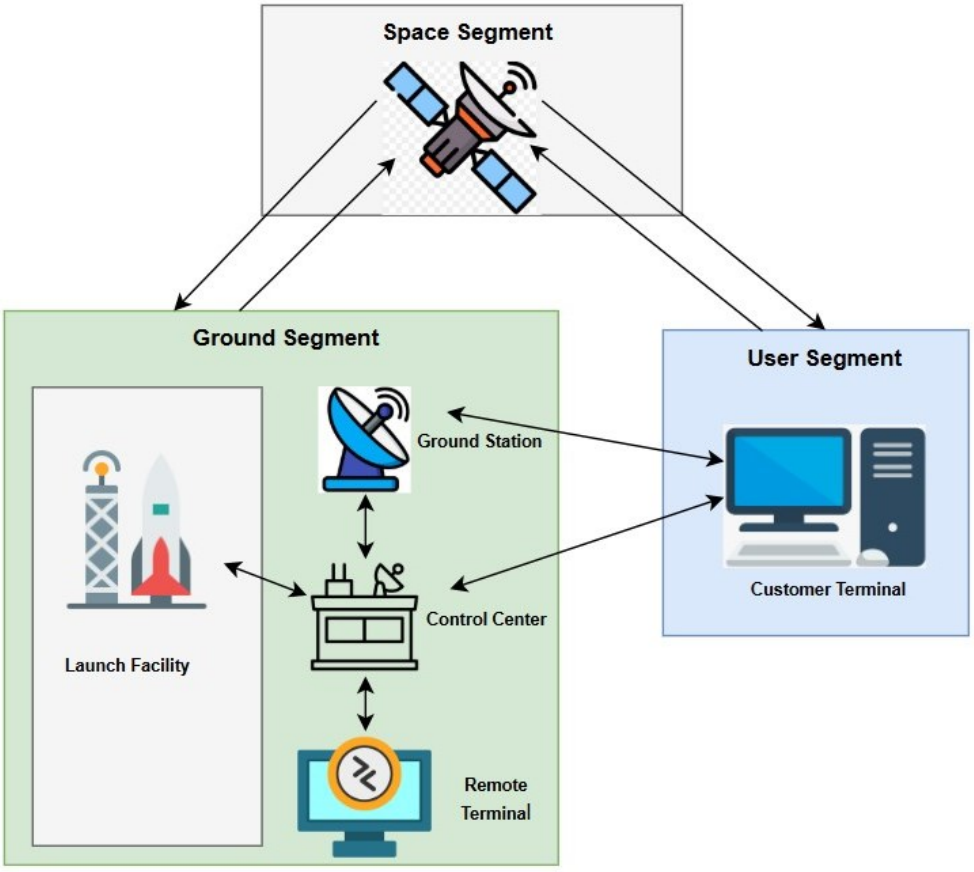

Figure 2. The architecture of Space Information Networks.

3.2. Key Enabling Technologies

Several technological advancements underpin the functionality of SINs:

1. Software-defined networking (SDN): Enables centralized control of data flow and dynamic reconfiguration of communication paths based on network conditions.
2. Edge computing: Allows satellites to preprocess data onboard, reducing latency and bandwidth usage for ground transmission.
3. Commercial Off-the-Shelf (COTS) components: Widely adopted to reduce cost and development time, though often at the expense of introducing vulnerabilities.
4. Internet of Space Things (IoST): Refers to a globally distributed network of interconnected space-based assets that share sensing, communication, and control data [4].

3.3. Unique Cybersecurity Challenges in SINs

The deployment and operation of SINs present several distinct cybersecurity challenges:

- Physical inaccessibility: Once in orbit, satellites cannot be physically patched or reconfigured, limiting the ability to respond to emerging threats.
- Latency and bandwidth constraints: These hinder the deployment of traditional intrusion detection and monitoring systems.
- Long lifecycle and legacy systems: Many satellite components are used for decades, often running outdated software stacks with unpatched vulnerabilities.
- Highly distributed and interdependent systems: Attackers can compromise one node and propagate threats across space and ground infrastructure.
- Lack of standardization: Varying design and security practices across space agencies and commercial operators create gaps in defense [5].

4. Significant Vulnerabilities in Space Information Networks Susceptible to Cyber Attacks

Space information networks, which are integral to modern communication, navigation, and surveillance, are increasingly vulnerable to cyber attacks due to their complexity, their interconnectedness, and the evolving nature of cyber threats. These vulnerabilities pose significant risks to critical infrastructure, global communication, and national security. This section explores the key vulnerabilities of Space Information Networks.

4.1. Complexity of Space Systems and Interconnectedness

Space systems today are incredibly complex and deeply interconnected, blending hardware, software, and communication networks into a single, tightly integrated structure. Because these systems operate across space, ground, and link segments, a weakness in one area, whether physical or digital, can quickly affect the entire network. The growing use of Commercial Off-the-Shelf (COTS) components and the rise of satellite mega-constellations have made these systems even more exposed to cyber threats. The old idea that space systems were protected by their complexity no longer holds true. With so many aspects of our daily lives, like GPS, weather forecasting, and global communications, relying on space infrastructure, even a single compromised satellite can lead to serious disruptions. That is why it is so important to build cybersecurity directly into these systems from the start, ensuring they can detect, resist, and recover from attacks [1].

4.2. Increased Attack Surface Due to New Technologies

The proliferation of small satellites, such as CubeSats, and the use of Commercial Off-The-Shelf (COTS) components have expanded the attack surface. These satellites, while cost-effective and efficient, rely on open-source operating systems and hardware, making them more accessible to attackers [4]. Additionally, the increasing use of software-defined

communications and the Internet of Space Things (IoST) has introduced new vulnerabilities, as these systems often lack robust security measures [4,6].

4.3. Lack of Standardized Security Measures

The lack of comprehensive security standards and the reliance on traditional security-through-obscurity approaches have left many space systems vulnerable to cyber threats. Unlike terrestrial systems, space systems often prioritize safety and availability over confidentiality and integrity, creating gaps that attackers can exploit [5,11]. Furthermore, the lack of ownership regarding security in SATCOM ecosystems and the difficulty in tracking the mitigation of vulnerabilities further complicate the problem.

4.4. Evolving Threat Landscape

The threat landscape for Space Information Networks is rapidly evolving, with attackers constantly devising new and inventive ways to breach digital systems. The increasing affordability of software-defined communications equipment has made it easier for attackers to gain communication capabilities with orbital assets [6]. Additionally, the growing number of cyber attacks, including zero-day attacks and supply chain attacks, poses a significant challenge to the security of space systems [7,8].

4.5. Physical and Cyber Interdependencies

Space systems are vulnerable not only to cyber threats but also to physical threats that can manifest in cyberspace and vice versa. For example, conventional electronic warfare measures can now have effects in cyberspace, and some cyber threats can have detrimental effects in the physical domain [1].

4.6. Insider Threats and Supply Chain Risks

Insider threats and supply chain risks are two major, yet often underestimated, challenges in keeping space systems secure. Insider threats are especially dangerous because they come from people who already have legitimate access to sensitive systems, making it easier for them to exploit weaknesses from within. Given how complex and interconnected space missions are, even a single insider action could lead to serious consequences. At the same time, the supply chains that support space projects are vast and global, often involving third-party vendors and Commercial Off-The-Shelf (COTS) components that may not be fully vetted for security. This opens the door to hidden vulnerabilities like malware or backdoors. The lack of comprehensive regulations covering the entire production lifecycle exacerbates these risks [5,11].

4.7. Limited Cyber Resilience Engineering Standards

The lack of comprehensive cyber resilience engineering standards for space systems is a significant challenge. Space systems often face unique challenges, such as the lack of physical access for repair, radiation-induced faults, and the need for long-term reliability, which are not adequately addressed by current standards [5].

4.8. Quantum Technology Threats

The advent of quantum technologies poses a future threat to the security of satellite communication networks. While quantum-resistant encryption solutions are being developed, the current lack of widespread implementation leaves many systems vulnerable to future attacks [8].

4.9. Tension Between Principles-Based and Compliance-Based Standards

The tension between principles-based and compliance-based standards is a challenge in securing Space Information Networks. Participants acknowledge that principles-based standards offer flexibility and allow organizations to tailor security practices to specific risks and system requirements. However, this flexibility can also lead to inconsistent implementation and gaps in protection if clear guidance is lacking. On the other hand, compliance-based standards provide well-defined checklists and measurable outcomes, which can be helpful for accountability but may become rigid and fail to adapt to evolving threats in the dynamic space domain. Experts expressed concern that strict compliance can give a false sense of security and delay engineering timelines. The consensus was that a balanced approach is needed—one that combines the adaptability of principles-based frameworks with the structure and clarity of compliance models, ensuring both agility and accountability in securing space systems [5].

4.10. Budget Constraints and Lack of Investment

Budget constraints and the lack of investment in cybersecurity are significant barriers to achieving cyber resilience in space systems. The high cost of developing and launching space systems often leaves little room for investing in advanced cybersecurity measures [5].

4.11. Challenges in Testing and Validation

The challenges in testing and validation of cybersecurity measures in space systems are significant. The complexity of space systems and the lack of comprehensive testing methodologies make it difficult to identify and mitigate vulnerabilities before deployment [5].

Table 1 highlights the major vulnerabilities in Space Information Networks, covering technical, operational, and emerging risks. These include system complexity, lack of standardized security, evolving threats, supply chain risks, and budget or testing challenges, all of which expand the attack surface and hinder resilience.

Table 1. Key vulnerabilities in Space Information Networks.

Vulnerability	Description	Citation(s)
Complexity of space systems	Interconnectedness and tight integration of components create a large attack surface.	[1]
Increased attack surface	Use of COTS components and small satellites expands the attack surface.	[4]
Lack of standardized security measures	Prioritization of safety over security leaves gaps for exploitation.	[5,11]
Evolving threat landscape	New attack methods and affordable communication equipment increase risks.	[6,7]
Insider threats and supply chain risks	Global supply chains and COTS components introduce vulnerabilities.	[5,11]
Limited cyber resilience standards	Unique challenges of space systems are not adequately addressed.	[5]
Quantum technology threats	Future threats to satellite communication networks require quantum-resistant solutions.	[8]
Tension between standards	Flexibility vs. compliance in standards complicates security implementation.	[5]
Budget constraints	High costs of space systems leave little room for cybersecurity investment.	[5]
Challenges in testing and validation	Complexity of space systems makes comprehensive testing difficult.	[5]

This table summarizes major vulnerabilities in Space Information Networks based on a review of the recent academic and technical literature.

5. Threats in Space Information Networks

Space Information Networks (SINs) are much more open and exposed than traditional terrestrial networks, making them more vulnerable to a wide range of threats. As space missions increasingly rely on interconnected satellite systems, ensuring the security and privacy of these networks has become a major concern. Figure 3 shows the taxonomy of security threats in Space Information Networks (SINs), classifying them into active and passive threats, with subcategories like jamming, node compromise, and eavesdropping. It also includes communication interference types: inter-system and intra-system. According to the Consultative Committee for Space Data Systems (CCSDS), threats to SINs can be grouped into three broad categories: natural threats, environmental threats, and mission threats [12]. Natural threats include unavoidable space phenomena like electromagnetic radiation or extreme weather, while environmental threats stem from system failures, such as power loss or technical malfunctions. Mission threats, however, are more deliberate, carried out by individuals or organizations with harmful intent. These include cyber attacks, signal interference, and data theft. Mission threats can lead to communication disruption, force-based destruction, and, more commonly, information theft and destruction, which accounts for over half of all attacks on SINs. These mission-related attacks can be either active, like jamming or injecting malicious code, or passive, such as eavesdropping or intercepting satellite transmissions [13]. With SINs playing such a critical role in defense, navigation, and global communications, protecting them from both internal and external threats is more important than ever.

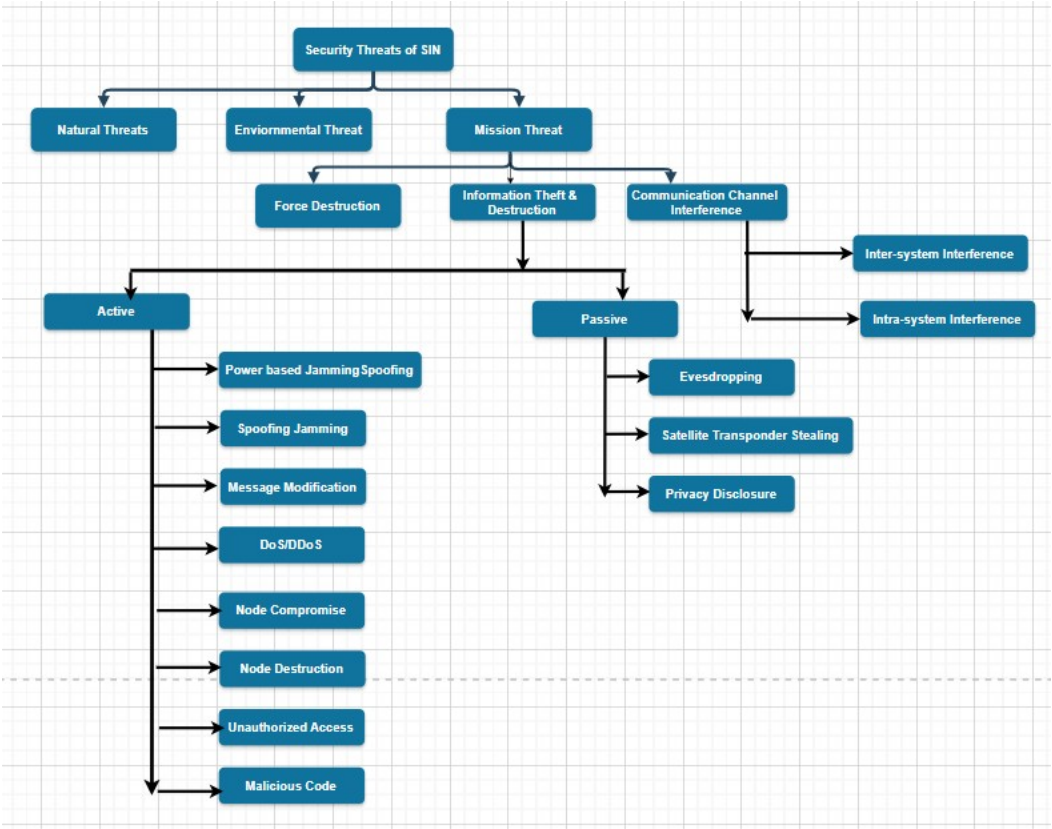

Figure 3. Classification of security threats in Space Information Networks (SINs).

5.1. Case Examples of Cyber Threats

5.1.1. Active Security Attacks

Active security attacks involve deliberate actions aimed at disrupting or damaging the normal operation of a system. Unlike passive attacks, these are noticeable to the victim

because they interfere directly with communications or services. They pose a major threat to both the integrity and availability of the network. Some of the most common types of active attacks include power-based jamming, spoofing jamming, message modification, Denial-of-Service (DoS) attacks, node compromise, and node destruction.

Denial-of-Service (DoS) Attacks

In a Denial-of-Service (DoS) attack, the attacker overwhelms the information system with excessive traffic, making it unavailable to legitimate users. Typically, this type of attack is launched from a single computer or device. A Distributed Denial-of-Service (DDoS) attack, on the other hand, involves multiple devices working together to flood the system. These devices are usually compromised bots that the attacker controls to generate massive amounts of malicious traffic [14].

Message Modification

Message modification occurs when a hacker intercepts communication and alters its content. This can involve changing, inserting, or deleting parts of a message. Such attacks are more likely to happen in the ground segment, where an attacker may illegally gain access to the system and modify operational data. These altered messages can lead to incorrect decisions or system malfunctions. To defend against message modification, modern satellite communication systems (SCSs) often use Intrusion Detection Systems (IDSs) and encryption techniques to detect and prevent unauthorized changes [13].

5.1.2. Passive Security Attacks

Passive attacks are especially dangerous because they happen silently, and victims often do not realize they have been targeted. These attacks do not interfere with the system's normal operations but aim to steal information, leading to a serious loss of confidentiality.

Eavesdropping

Eavesdropping occurs when unauthorized parties listen in on satellite communications. Due to the open and wireless nature of space transmissions, it is relatively easy for attackers, whether individuals or rival organizations, to intercept signals. In LEO satellite systems, the frequent switching of access links and the large number of satellites create more opportunities for such interception. Eavesdroppers can gather data over time and use it to plan future attacks. Techniques like Direct Sequence Spread Spectrum (DSSS) and Physical Layer Security (PLS) are commonly used to make interception more difficult and protect communication privacy [13].

Satellite Transponder Stealing

Satellite Transponder Stealing occurs when attackers illegally use a satellite's transponder, the device that receives and retransmits signals, to send their own data without authorization. This type of attack is common in satellites that use transparent forwarding, where the satellite simply relays any incoming signal without verifying its source. By carefully studying the satellite's transmission frequency and orbit, attackers can inject their signals using techniques like Direct Sequence Spread Spectrum (DSSS) with low power density, making their transmissions blend in with legitimate traffic. Because the satellite forwards signals indiscriminately, unauthorized data gets transmitted without detection. A common way to defend against this threat is to regularly change the satellite's operating parameters, such as its frequency, making it harder for attackers to maintain unauthorized access.

6. Effective Countermeasures for Preventing and Responding to Cyber Attacks on Satellite-Based Information Networks

Satellite-based information networks are critical components of modern communication and navigation systems, but they are increasingly vulnerable to cyber attacks. These attacks can disrupt critical services, compromise sensitive data, and pose significant risks to national security and global infrastructure. To address these challenges, this section outlines the most effective countermeasures for preventing and responding to cyber attacks on satellite-based information networks, drawing insights from recent research papers.

6.1. Artificial Intelligence and Machine Learning for Threat Detection

The integration of artificial intelligence (AI) and machine learning (ML) into satellite network security has emerged as a powerful tool for detecting and mitigating cyber threats. AI can analyze vast amounts of data in real-time, identifying anomalies and distinguishing between benign and malicious activities [15]. Federated learning (FL) has been successfully applied in Satellite–Terrestrial Integrated Networks to detect DDoS attacks while preserving data privacy [9,10]. AI also enhances space situational awareness and enables predictive maintenance for proactive threat management [15].

In [16], the authors proposed a privacy-preserving intrusion detection framework called a federated deep learning framework for IoT-integrated smart satellite networks, where bidirectional LSTMs are trained locally at different nodes and then aggregated through the FedAvg algorithm. This design enables cross-operator collaboration without sharing raw telemetry, preserving data privacy while still leveraging distributed intelligence. On benchmark datasets such as ToN-IoT and UNSW-NB15, the proposed approach achieved near-centralized accuracy (99.7%), clearly outperforming local models and CNN baselines, thereby demonstrating that temporal sequence modeling combined with federated learning is particularly effective for satellite–IoT threat detection [16].

The paper [17] explores using Temporal Convolutional Networks (TCNs) to spot anomalies in spacecraft telemetry streams (e.g., voltages, currents, temperatures). The model learns normal time series behavior by predicting the next readings; when actual values deviate too much from the forecast, it flags potential faults. Compared with recurrent models like LSTMs, the TCN approach offers similar detection quality but with faster, more efficient inference, making it well-suited for real-time, on-orbit health monitoring and early warning of system issues.

A practical IDS for satellites, CANSat-IDS splits detection between the spacecraft and the ground. A tiny on-board module watches CAN-bus timing patterns in real time (fast, low-power) to catch obvious disruptions, while a richer ground-side analyzer inspects packet contents to uncover replay and subtler payload tampering. Models are trained and updated on Earth, then pushed back as firmware, so the satellite stays lightweight but current. In tests with common CAN-bus attack scenarios (DoS, fuzzing, replay), the system reports consistently high detection, showing that this split design fits on-orbit constraints without sacrificing coverage [18].

Cuéllar et al. present an explainable, supervised anomaly detection pipeline for spacecraft telemetry. It models common anomaly modes—point spikes, magnitude shifts, waveform changes, frequency shifts, and abrupt contextual deviations—by building a compact three-feature signature per time window: a moving-average prediction error to capture magnitude deviations, STFT dispersion to capture frequency irregularities, and an LSTM prediction error to capture waveform mismatch. A lightweight classifier (with Random Forest performing best) labels windows, and LIME explanations highlight which feature drove each alert [19].

Global Navigation Satellite Systems (GNSS) play a critical role in positioning, navigation, and timing applications; however, their susceptibility to spoofing attacks—where counterfeit signals mislead the receiver—poses a significant security risk. An integrated detection approach that combines the discrete wavelet transform (DWT) and machine learning (ML) classifiers was proposed in [20]. Specifically, Daubechies wavelets (db4 and db8) are employed for effective time–frequency localization, enabling the identification of anomalies induced by spoofing attacks. Experimental evaluations on GPS and Galileo datasets (OAKBAT) demonstrate high classification accuracy, with Support Vector Machines (SVMs) utilizing the radial basis function kernel outperforming other models. Furthermore, the approach reduces computational complexity by using pre-extracted statistical and spectral features as classifier inputs, making it suitable for real-time GNSS spoofing detection. In [21], it explores the use of machine learning algorithms, including ARIMA, MLP, RNN, LSTM, and GRU, to predict spacecraft parameters such as battery temperature and power bus voltage using Egyptsat-1 telemetry data. We discussed two papers in detail and gave our own critical observations.

6.1.1. Distributed Network Intrusion Detection System in Satellite–Terrestrial Integrated Networks Using Federated Learning

Satellite–Terrestrial Integrated Networks (STINs) combine the coverage of satellite communication with the flexibility of terrestrial infrastructure. However, STINs are inherently vulnerable due to their limited computational resources, high latency, and strong privacy constraints. Traditional centralized Network Intrusion Detection Systems (NIDSs) are ineffective in such environments due to impracticalities in data aggregation and real-time analysis. The paper [9] addresses the security and privacy issues in STINs by proposing a distributed NIDS architecture based on federated learning (FL), allowing localized learning without compromising data privacy. This approach is particularly tailored to detecting Distributed Denial-of-Service (DDoS) attacks across both satellite and terrestrial domains.

The flowchart in Figure 4 illustrates the development pipeline of a federated learning-based NIDS for Satellite–Terrestrial Integrated Networks (STINs). It begins with constructing the STIN architecture and generating specialized datasets. Federated learning is then integrated with an adapted algorithm to balance training across diverse nodes. Finally, optimized network topology ensures stable deployment and real-time threat monitoring.

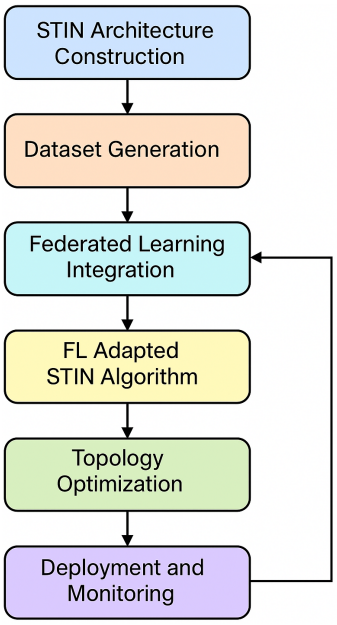

Figure 4. Federated learning-based STIN-NIDS framework workflow.

STIN Architecture Construction

A realistic prototype was developed using OpenStack and KVM virtualization to simulate a Satellite–Terrestrial Integrated Network (STIN) consisting of satellite, terrestrial, and attack networks. They implemented a Delay-Tolerant Network (DTN) for satellite communication, integrating the ION stack and creating realistic inter-node delays. The system comprises a satellite network with three LEO satellites utilizing DTN via the ION protocol, a terrestrial network featuring two satellite gateways, two routers, and three clients, and an attack network comprising four hosts simulating DDoS and other cyber attacks.

The STIN dataset, built from 3 h of simulated traffic with benign flows and 11 attack types, was reduced via 1:500 sampling into TER20 and SAT20. After feature selection, 15 flow-level attributes were retained for efficient training on resource-constrained nodes.

Federated Learning Adapted Algorithm

Traditional methods like centralized cloud processing or distributed machine learning (DML) require transmitting raw data to central or edge servers, which poses serious privacy risks, especially when dealing with sensitive security data like that used for DDoS detection. This can lead to privacy violations and reduced participation from data owners. In contrast, federated learning eliminates the need to share raw data, allowing models to be trained locally and only sharing encrypted updates. This ensures data privacy, legal compliance, and broader participation, making it ideal for secure, large-scale, real-world applications. Federated learning (FL) was integrated using a horizontal scheme in which each node independently trains a CNN model and shares only encrypted gradients (via Paillier encryption) with an aggregation server for secure model updates. To accommodate the disparities in resource availability between satellite and terrestrial nodes, a custom FL-adapted STIN algorithm dynamically adjusts model complexity and synchronizes training times, ensuring efficiency and responsiveness. The FL-adapted STIN algorithm is designed with two critical goals in mind:

- Synchronization of processing time across heterogeneous nodes.
- Efficient and accurate traffic identification in both satellite and terrestrial domains.

Due to the limited computational resources available on satellite nodes, the model complexity, Cmodel, has a significant impact on the overall training time, Ttrain (terrestrial network training time). To ensure resource-efficient training, the model complexity is estimated as

$$C_{model} \sim \mathcal{O}\left(\sum_{j=1}^{N} A_j^2 \cdot B_j^2 \cdot Q_{j-1} \cdot Q_j\right) \quad (1)$$

where N is the number of convolutional layers in the neural network, A is the side length of each convolution kernel output feature map, B is the side length of each convolution kernel, j denotes the j-th convolutional layer of the neural network, and Q is the number of convolution kernels in the j-th convolutional layer. Therefore, the purpose of the algorithm is to output a suitable C_{out_model} to achieve time synchronization in the FL process.

The flowchart below (Figure 5) illustrates the core workflow of the FL-Adapted STIN Algorithm, which is designed to maintain synchronization and efficiency in a federated learning environment involving both satellite and terrestrial nodes.

The process begins by initializing key variables: the satellite training time (T_{strain}), terrestrial training time (T_{ttrain}), and initial model complexity (C_{init_model}). Once these parameters are set, the aggregation server collects the gradient updates from both the satellite and terrestrial nodes after their local training.

Next, the server computes the actual training times for both domains. These values are then compared to assess synchronization, specifically by checking whether the satellite training time falls within 80% to 100% of the terrestrial training time.

If the satellite training time lies within this acceptable range, it indicates that the current model complexity is well-balanced for both types of nodes, and the output model (C_{out_model}) is retained as the initial one (C_{init_model}). However, if the satellite training time is either significantly faster or slower, the system adjusts the model complexity accordingly—either simplifying or enriching the model—so that future training rounds maintain better timing synchronization across the network.

This adaptive mechanism ensures efficient training in resource-constrained satellite environments while maintaining the integrity of the federated learning process.

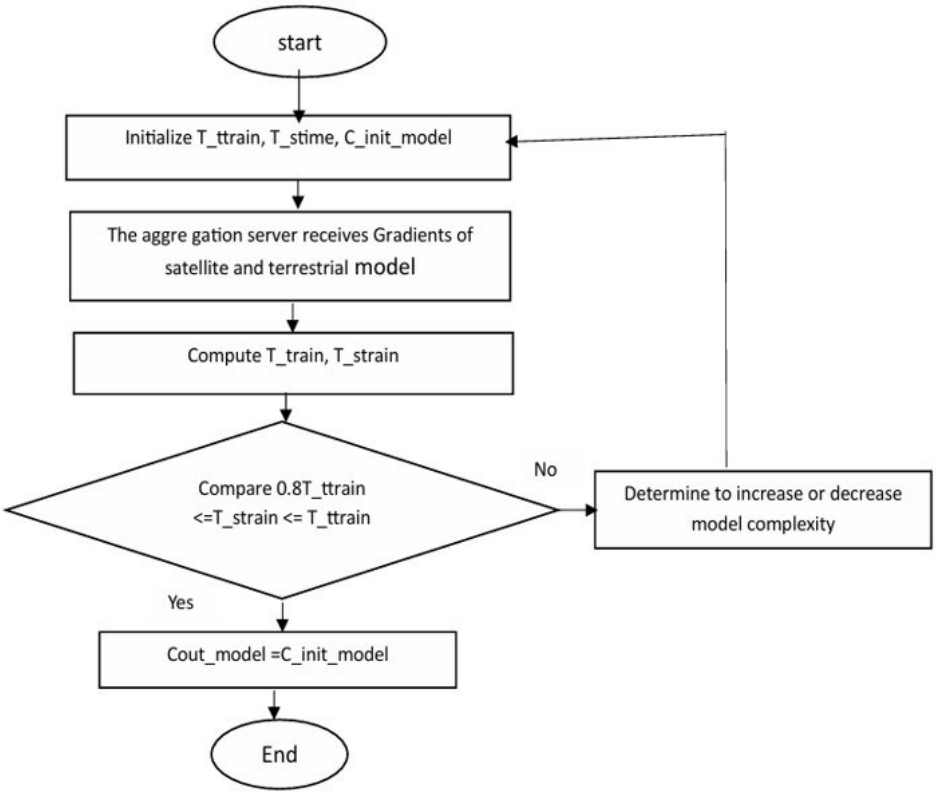

Figure 5. Workflow of the FL-Adapted STIN Algorithm.

Topology Optimization

In Satellite–Terrestrial Integrated Networks (STINs), the satellite topology is highly dynamic due to frequent orbital changes, which leads to instability in routing, data transmission delays, and challenges in detecting and mitigating attacks such as DDoS. Since federated learning (FL) depends on synchronous model exchanges between satellites and ground nodes, these frequent topology variations can disrupt communication and degrade training performance. To address this, topology optimization focuses on calculating link stability weights and weighted distances between satellite nodes to form a low-switching, stable communication graph. This optimized topology reduces packet loss, minimizes retraining delays, and ensures consistent data flow, thereby enhancing the accuracy and reliability of the NIDS while enabling efficient FL operation with minimal overhead.

Evaluation and Performance Metrics

The distributed NIDS was evaluated using multiple metrics: accuracy, false-positive rate (FPR), mean squared error (MSE), CPU utilization, packet loss, and malicious traffic recognition rate. Three CNN variants were considered in this study. CNN1 served as the

baseline model used in federated learning (FL). CNN2 introduced added complexity to enhance representational capacity, while CNN3 was designed with roughly double the complexity of CNN1 to assess the impact of scaling on performance.

Results showed that FL-CNN1 outperformed traditional NIDSs (Snort, Bro IDS) in terms of CPU efficiency, accuracy (90%), low FPR, and robustness to unseen attack types like Slowloris and file-transfer DDoS. More complex models (CNN2, CNN3) caused performance degradation due to resource limits on satellites.

Critical Observations and Reflections

The paper offers a well-conceived solution for intrusion detection in hybrid satellite–terrestrial networks through the use of federated learning (FL). The approach effectively addresses critical challenges like privacy, limited resources, and attack detection in distributed environments. However, our observation is that the real-world applicability of the proposed framework is constrained by the relatively small-scale testbed and simulated conditions. The prototype, while realistic in design, does not fully reflect the complexity and dynamics of operational STIN environments such as LEO constellations with thousands of moving nodes and varying topologies. Furthermore, while the FL-adapted training algorithm is designed with resource awareness in mind, key practical challenges like communication disruptions, heterogeneous latency, adversarial model poisoning, and model drift in evolving threat landscapes are either simplified or not fully explored. There is also limited discussion on the cost of implementing secure gradient aggregation or encrypted model sharing under real-time constraints. Despite these limitations, the paper presents a strong foundation and opens up important directions for future research including hierarchical FL architectures, adaptive model tuning, and robust deployment in 5G/6G-integrated STINs.

6.1.2. Deep Learning Approach for Interruption Attacks Detection in LEO Satellite Networks

Low Earth Orbit (LEO) satellite networks have become a fundamental part of next-generation global communications, providing essential services for both civilian and governmental sectors. However, their wide-area broadcasting capabilities, reliance on open communication protocols, and constrained on-board resources make them highly vulnerable to cyber threats, especially interruption attacks such as Distributed Denial of Service (DDoS) and network jamming. Traditional intrusion detection solutions, primarily designed for terrestrial networks, are insufficient in the dynamic and resource-limited environment of LEO constellations. Recognizing these unique challenges, this study introduces a deep learning-based interruption detection strategy specifically tailored for LEO satellite networks. By harnessing artificial intelligence, the goal is to proactively detect and classify different types of interruptions, thereby enhancing the resilience and security of space-based communication systems.

To address the cybersecurity challenges faced by LEO satellite networks, the authors developed a deep learning-driven intrusion detection framework [22]. This framework utilizes simulated traffic datasets generated via satellite network simulators to train and evaluate various deep learning models, including MLP, CNN, RNN, GRU, and LSTM architectures. By leveraging these models, the system achieves high accuracy in detecting benign traffic as well as multiple categories of interruptions such as DDoS attacks, meteorological disturbances, and jamming events. The approach emphasizes not only offline full-network detection but also realistic online flow-based detection at the satellite level, making it practical for deployment in real-world LEO networks.

To design an effective interruption detection system for Low Earth Orbit (LEO) satellite networks, the authors first developed a comprehensive simulation environment using Om-

net++ coupled with the INET library. The simulated network topology consisted of 20 Earth terminals and three satellites interconnected via inter-satellite links and satellite-to-ground links. To create a robust dataset reflective of real-world conditions, four distinct traffic scenarios were generated: (1) benign normal communication traffic, (2) UDP flood attacks simulating Distributed Denial-of-Service (DDoS) incidents, (3) meteorological disturbances such as rain and thunderstorms, and (4) network jamming attacks emulated by airborne interference sources.

From the simulation outputs, two specialized datasets were constructed. The first dataset, designated as SATCOM.LEO.NDBPO.#1, captured exhaustive network traffic at each node, providing a full network view suitable for offline intrusion detection. The second dataset, SATCOM.LEO.NDBPO.#2, was developed for realistic operational settings, recording flow-level information only at the satellite nodes to simulate the constraints of limited visibility and real-time detection. As shown below (Figure 6), Common features in both datasets cover packet timing, sender/receiver details, packet size, frequency channel, signal quality (SNIR), and throughput. Dataset-1 includes detailed node-level features like received/sent packets and queue statistics, while Dataset-2 focuses more on flow-level metrics such as flow bytes per second and time between packets, enabling real-time detection scenarios. Feature extraction from these datasets incorporated key metrics such as packet size, frequency, throughput, signal-to-noise ratio (SNIR), and flow statistics. All features were normalized using the min-max scaling technique to optimize them for deep learning classifiers.

TABLE : Description of «SATCOM.LEO.NDBPO.#1» and «SATCOM.LEO.NDBPO.#2» features

No.	Feature	Description	Dataset#1	Dataset#2
-	sendTime	Sending time according to the sniffed packet	yes	yes
-	sender	Packet sender	yes	yes
-	reciever	Packet receiver	yes	yes
-	IP_src	Ip Address of the source	yes	yes
-	port_src	Port of the source	yes	yes
-	IP_dest	Ip Addres of the destination	yes	yes
-	port_dest	Port of the destination	yes	yes
-	Frequency	Transmission frequency	yes	no
1	Next_Current_diff	Global time difference between current and next	yes	yes
2	Next_Pre_diff	Global time difference between previous and next	yes	yes
3	SNext_Current_diff	Local time difference between current and next	yes	yes
4	SNext_Pre_diff	Local time difference between previous and next	yes	yes
5	size	Packet size	yes	yes
6	channel	Frequency channel	yes	yes
7	duration	Transmission duration	yes	no
8	packet_type	Packet type (Udp,Icmp)	yes	yes
9	rcvdPK	Recieved packets	yes	no
10	sentPK	Sent packets	yes	no
11	droppedPKWrongPort	Dropped packets, wrong ports	yes	no
12	DataQueueLen	Data queue length	yes	no
13	passedUpPk	Passed up packets	yes	no
14	rcvdPKFromHL	Received from higher layer	yes	no
15	rcvdPKFromLL	Received from lower layer	yes	no
16	sentDownPK	Sent down packets	yes	no
17	DropPKByQueue	dropped packets from queue	yes	no
18	snir	Signal-to-interference-plus-noise ratio	yes	yes
19	throughput	Transmission throughput	yes	yes
20	Flow Bytes_s	Flow's bytes per second	no	yes
21	Flow Packets_s	Flow's packets per second	no	yes
22	meanT_b_2P	Mean time between two packets	no	yes
23	maxT_b_2P	Maximum time between two packets	no	yes
24	minT_b_2P	Minimum time between two packets	no	yes

Figure 6. Features of datasets.

Following dataset preparation, multiple deep learning models were implemented and rigorously tested. The models included Multi-Layer Perceptron (MLP), Convolutional Neural Network (CNN), Recurrent Neural Network (RNN), Gated Recurrent Unit (GRU), and Long Short-Term Memory (LSTM) networks. Each model was trained and validated on 70% of the data, with the remaining 30% reserved for independent testing. Training focused on two main tasks: binary classification to distinguish between normal and attack traffic, and multi-class classification to identify specific types of interruptions.

To further evaluate real-world applicability, a real-time Intrusion Detection System (IDS) was developed using the best-performing deep learning models. This IDS captures live packet flows, processes features in real time, and classifies traffic into benign or attack categories. Two operating modes were introduced: "Normal Mode," emphasizing high precision with minimal false positives, and "Safe Mode," favoring sensitivity to capture as many attack events as possible even at the cost of increased false positives. Through a combination of simulation-based dataset generation, deep learning classification, and real-time IDS deployment, this study establishes a practical and scalable framework for securing LEO satellite networks against interruption threats.

In this study, several deep learning models, MLP, CNN, RNN, GRU, and LSTM, were evaluated for detecting interruption attacks in Low Earth Orbit (LEO) satellite networks. Two datasets were used: SAT-COM.LEO.NDBPO.#1, which assumes full network surveillance, and SAT-COM.LEO.NDBPO.#2, which simulates a more realistic environment with limited monitoring at satellite nodes.

For binary classification (distinguishing normal and attack traffic), the LSTM model achieved the highest performance on the SAT-COM.LEO.NDBPO.#1 dataset, reaching 99.98% accuracy with a very low false-positive rate of 0.014%. On the more challenging SAT-COM.LEO.NDBPO.#2 dataset, the GRU model performed the best, achieving 96.12% accuracy. The CNN, although initially promising, showed higher false positives and longer training times and was therefore not preferred for practical deployment.

For multi-class classification (identifying specific types of attacks such as UDP flood, natural interference, and jamming), the MLP model achieved the best results on SAT-COM.LEO.NDBPO.#1 with an accuracy of 99.33%. On the SAT-COM.LEO.NDBPO.#2 dataset, the MLP, GRU, and LSTM models achieved similar performance, around 94.35% accuracy. Among them, the MLP showed relatively better control over false-positive rates, which is important for minimizing unnecessary alarms in real-world applications.

In addition, the authors developed a real-time Intrusion Detection System (IDS) using the trained models. Two operational modes were introduced: a Normal Mode, prioritizing low false alarms, and a Safe Mode, aiming to detect every possible threat even at the cost of higher false positives. In testing, the IDS successfully detected UDP flooding attacks, meteorological disturbances, and network jamming events with strong reliability, especially in Normal Mode where false alarms were minimal.

Critical Observations and Reflections

The research revealed that deep learning models like MLP, GRU, and LSTM achieved impressive detection accuracy for both binary and multi-class interruption detection in LEO satellite networks. Notably, LSTM excelled in binary classification, while the MLP demonstrated strong consistency with low false-positive rates in multi-class classification. However, despite high performance in controlled simulations, some limitations emerged. Models like the CNN, which are effective in other domains, struggled to adapt to the unique traffic characteristics of satellite communication. This suggests that not all deep learning architectures are equally suited for every network environment.

Additionally, while offline detection yielded near-perfect results, real-time detection presented new challenges, particularly in balancing sensitivity and false-positive rates. This highlights an important reality: models that perform well under ideal conditions may struggle in real-world scenarios with constraints like limited data, computing power, and communication delays.

Ultimately, it became clear that future systems must be designed with a focus on both accuracy and operational robustness, addressing these real-world limitations. This study also opens up opportunities for integrating federated learning and lightweight models, which could enhance performance while maintaining scalability and security in satellite networks. Future research should focus on integrating deep learning-based interruption detection into Delay/Disruption-Tolerant Networking (DTN) protocols to improve robustness under satellite communication disruptions. Additionally, developing hybrid models that combine Bi-LSTM with attention mechanisms can better capture temporal dependencies and enhance detection performance.

6.2. Network Segmentation and Traffic Filtering

Network segmentation involves dividing a network into smaller, isolated segments, each with its own security controls. This approach limits the spread of malicious activities in case of a breach [23]. Traffic filtering monitors and blocks suspicious or malicious packets. Optimized satellite network topologies further enhance this by reducing traceability of malicious packets due to frequent link switching [9].

A K-Bottleneck Minimize routing algorithm avoids bottleneck paths in LEO satellite networks, improving robustness and attack resistance. By statistically modeling high-risk links under the ICARUS framework, the scheme forces adversaries to generate significantly larger attack volumes, thereby raising their operational cost and enabling earlier anomaly detection [24].

The paper [25] presents a comprehensive threat modeling and security assessment framework for satellite networks, based on the Threat Vector–Hierarchical Attack Representation Model (TV-HARM). It analyzes the vulnerabilities in satellite communication protocols, operating systems, and network segments, proposing a structured approach for evaluating network security. The study identifies attack paths, assesses the risks using security metrics, and demonstrates the effectiveness of mitigation strategies, including protocol and OS patches. Experimental results highlight the remaining vulnerabilities in satellite networks and emphasize the need for robust defense mechanisms.

In [26], the authors develop a machine learning-based trust model with Ant Colony Optimization (ACO) for secure routing and DDoS filtering in integrated satellite–terrestrial networks. The system integrates AdaBoost with SVM classifiers and dynamically updates routing paths, reinforcing trustworthy nodes while filtering malicious traffic, thus offering a scalable defense for resource-constrained satellite environments.

Time-varying bottleneck links in Low Earth Orbit (LEO) satellite networks have a unique vulnerability caused by frequent handovers and uneven traffic distribution. In [27], the authors proposed SKYFALL, a comprehensive analyzer that uses real constellation data, routing, and traffic distributions to model risks from compromised user terminals. Findings show that LFAs targeting bottleneck links can reduce legal traffic throughput by a factor of 3.4×, with a wide regional impact. In [28], the authors presented the SLT secure routing algorithm, which leverages Dempster–Shafer evidence theory for trust evaluation and improves packet delivery while isolating malicious nodes. Together, these approaches demonstrate how routing diversity, trust-based filtering, and dynamic analysis enhance segmentation and traffic control in satellite networks. We now discuss one of the routing techniques and give our own observations.

6.2.1. Random Routing Algorithm for Enhancing the Cybersecurity of LEO Satellite Networks

Low Earth Orbit (LEO) satellite networks have emerged as a cornerstone of next-generation communication infrastructures due to their low latency, global coverage, and potential to support broadband services. With the deployment of large satellite constellations such as Starlink and OneWeb, the role of LEO networks in both civilian and governmental operations has significantly expanded. However, this evolution has also exposed such networks to new security vulnerabilities, particularly Distributed Denial-of-Service (DDoS) attacks. Unlike terrestrial systems, LEO networks feature dynamic topologies, limited computational capabilities, and predictable routing behavior—all of which make traditional cybersecurity solutions insufficient. Attackers can exploit deterministic routing patterns to congest specific inter-satellite links, leading to service disruption. Hence, the need for a more adaptable, uncertainty-driven routing strategy forms the core motivation of this study.

To enhance cybersecurity in Low Earth Orbit (LEO) satellite networks, the authors proposed a randomized routing algorithm [14], referred to as k-RAND. To mitigate DDoS attacks in LEO satellite networks, the proposed random routing algorithm (k-RAND) introduces controlled randomness into the packet forwarding process by selecting among multiple routing strategies with a weighted probability distribution. This approach significantly increases the uncertainty for attackers, making it much harder to predict and congest specific communication links. As a result, attackers must expend more resources, compromise a larger number of bots, and spread attack traffic across many satellites, thereby raising the overall cost and complexity of executing a successful DDoS attack. By making attacks less efficient and more expensive, k-RAND offers a practical and scalable defense mechanism for safeguarding future dense LEO satellite constellations against evolving cyber threats.

Instead of relying on a fixed routing scheme, k-RAND selects one of four classical routing strategies—k-Shortest Paths (k-SP), Ground-to-Ground Disjoint Paths (k-DG), Satellite-to-Satellite Disjoint Paths (k-DS), and Limited-Overlap Shortest Paths (k-LO)—based on a weighted probability distribution, shown in Figure 7. This randomness increases the attacker's uncertainty and the cost of mounting a successful Distributed Denial-of-Service (DDoS) attack.

The k-RAND selection process is driven by a random variable and thresholds a_1, a_2, and a_3, each corresponding to one of the four routing algorithms. To determine the optimal distribution values, the authors formulate a Bayesian optimization problem that maximizes the average cost of attack, defined as the traffic resources an adversary must expend.

Simulations were conducted using the ICARUS framework over a realistic Starlink-like satellite constellation comprising 1584 nodes. The optimization process was executed over 50 iterations, yielding the final probability mass function as follows: k-LO (58.8%), k-SP (37.7%), k-DG (2.6%), and k-DS (0.9%).

Simulation outcomes show that the k-RAND algorithm increases both the median and average costs required for a successful DDoS attack, outperforming all four baseline algorithms. Specifically, compared to the deterministic k-SP routing, k-RAND improved the average cost by 1.71% and the median cost by 2.05%. This increase implies that attackers would need to deploy more distributed bots or higher bandwidth per node, making the attack less feasible. The cumulative distribution function (CDF) further confirms that k-RAND achieves a higher probability of attack cost exceeding critical thresholds across the cost range of 0.82–0.96. Although the detectability metric (MaxUp) slightly degraded—indicating a marginally reduced ability to detect attacks via traffic spikes—the trade-off is considered acceptable given the significant gain in network robustness. Overall, the k-

RAND algorithm introduces a novel layer of randomness to routing logic, which effectively deters targeted DDoS attempts and enhances the resiliency of LEO satellite networks without compromising basic communication functionality.

Critical Observations and Reflections

The paper tackles an important and growing problem by proposing a random routing algorithm (k-RAND) to make LEO satellite networks more resilient against DDoS attacks. A major strength is how it increases uncertainty for attackers without needing heavy hardware changes, making it practical for real-world satellite systems. The use of simulations on a Starlink-like constellation and the application of Bayesian optimization show solid technical design. Overall, the idea of using randomness at the network layer is clever and addresses a real cybersecurity gap as satellite networks expand. While the paper presents a strong solution, there are a few important gaps. Although it shows that k-RAND raises the attacker's cost, it does not deeply explore how the slight drop in detectability (MaxUp) could impact real-world detection, where speed is crucial. The randomness is limited to just four routing strategies, and the assumption that attackers will not adapt over time might not hold, especially against more advanced adversaries. Also, the focus is mainly on inter-satellite links, without considering ground station attacks, beam-hopping, or link failures that could change routing behaviors. Lastly, while satellite hardware limitations are mentioned, they are not tested experimentally. Overall, the approach is promising, but future work should test it in more dynamic, realistic settings and against smarter attacks.

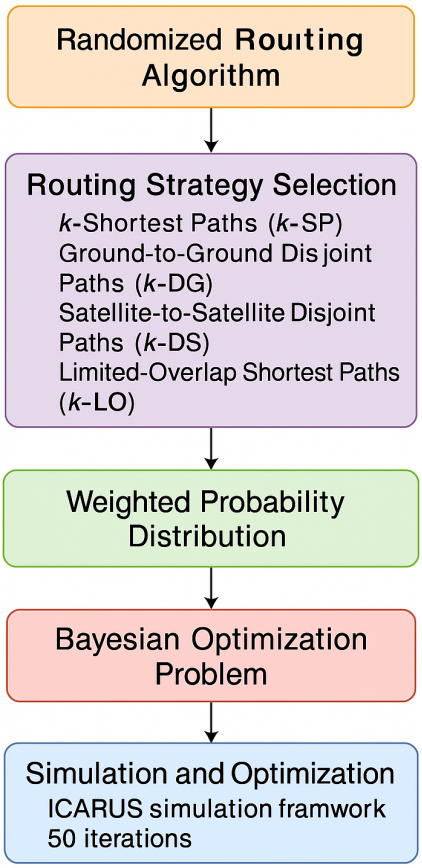

Figure 7. The diagram outlines the methodology of the k-RAND algorithm, beginning with the selection of randomized routing strategies among four classical algorithms. It proceeds through assigning weighted probabilities, formulating a Bayesian optimization problem, and executing simulations via the ICARUS framework over 50 iterations to maximize the average cost of DDoS attacks and enhance network robustness.

6.3. Encryption and Authentication Mechanisms

Encryption is a fundamental countermeasure for securing satellite communications. Traditional cryptographic methods, such as AES, provide confidentiality at the MAC layer, but legacy SATCOM deployments often rely on outdated schemes, making them vulnerable to modern attacks. Advanced encryption techniques and emerging quantum-safe solutions are essential to protect data from interception and ensure long-term security in satellite networks [29]. Additionally, robust authentication mechanisms ensure that only authorized entities can access the network, reducing the risk of malicious actors gaining entry [30]. For instance, the use of physically unclonable functions (PUFs) and dynamic seed frequency hopping (DSFH) can enhance mutual authentication and mitigate spoofing attacks [30].

In recent years, the integration of blockchain technology into satellite network security has gained significant attention due to its potential to enhance data integrity, privacy, and authentication. A decentralized system was proposed for space situational awareness using blockchain technology, which could significantly improve satellite safety operations by providing a more efficient way to track and prevent satellite collisions in Low Earth Orbit (LEO) [31]. This decentralized approach is crucial for mitigating the growing concerns over space debris and collisions, a critical issue for satellite security.

Similarly, in [32], they introduced a blockchain-based authentication scheme designed for Low Earth Orbit (LEO) satellite-assisted Internet of Things (IoT) systems. This scheme addresses several challenges inherent in LEO satellite communication, such as dynamic topology and frequent link switching, by leveraging blockchain's decentralized nature to provide secure and efficient authentication [32]. Their approach reduces the complexity of centralized systems, making it more suitable for resource-constrained satellite networks.

Moreover, the effectiveness of blockchain in securing satellite communication networks is discussed, particularly in terms of access control, confidentiality, and authentication. They proposed a blockchain-based architecture that ensures secure communication channels and protects satellite networks from external threats by using distributed ledger technology [33]. Their work emphasizes the importance of combining traditional security strategies with emerging technologies like blockchain to safeguard satellite systems from cyber attacks.

A Zero Trust-based authentication protocol was proposed for inter-satellite links (ISLs) in Next-Generation Low Earth Orbit (LEO) networks, addressing the growing security challenges in dynamic, high-speed satellite environments. Unlike traditional static methods, the proposed approach employs the principle of "never trust, always verify," enabling continuous authentication across satellite nodes. It leverages orbital parameters for dynamic identity verification combined with lightweight Hyperelliptic Curve Cryptography (HECC) to enhance security without overburdening limited satellite resources. The protocol ensures resilience against threats such as spoofing, replay, and man-in-the-middle attacks while maintaining low latency [34].

Space–air–ground integrated networks (SAGINs) present unique security challenges due to their heterogeneous architecture and dynamic connectivity. To address these issues, ref. [35] introduces an AI-oriented Two-Phase Multifactor Authentication Scheme (ATMAS) that combines conventional cryptographic one-shot authentication (Phase I) with AI-driven continuous authentication (Phase II). By leveraging spatial–temporal features such as location, traffic volume, and mobility patterns, the proposed approach enhances resilience against spoofing, replay, and man-in-the-middle attacks while maintaining real-time protection and low latency. Security analysis validates mutual authentication and forward secrecy.

Recent advancements in quantum communication have addressed key challenges in achieving secure, large-scale implementations. Collins et al. [36] experimentally demonstrated quantum digital signatures (QDSs) over a record channel loss of 42.8 dB, corre-

sponding to an equivalent fiber length of 134 km. This implementation, based on differential phase-shift QKD, represents the longest reported distance for QDS and ensures non-repudiation and message integrity in realistic conditions.

In parallel, Roger et al. [37] developed a real-time gigahertz free-space QKD system capable of completing the entire protocol within a single emulated satellite overpass. The system achieved a secure key length of 4.58 Mbit, leveraging laser-based classical communication and high-speed polarization encoding, marking a major step toward practical intercontinental quantum-secure communication.

Complementing these efforts, Sidhu et al. [38] analyzed the finite-key effects in satellite QKD, revealing that short overpass durations in Low Earth Orbit (LEO) impose stringent limitations on key generation. By employing optimized decoy-state BB84 protocols and tight finite-key security bounds, the study provides essential design guidelines for future satellite-based quantum networks.

Post-quantum authentication is a critical requirement for securing satellite communications. Traditional schemes relying on number-theoretic assumptions are vulnerable to quantum attacks, making them unsuitable for future space networks. Lattice-based protocols, such as those built on the Ring Learning with Errors (RLWE) problem, provide quantum-resistant authentication and key agreement mechanisms for satellite systems [39].

Satellite-based quantum key distribution (QKD) faces practical constraints such as limited transmission time, high optical link loss, and finite-size statistical effects that impact secure key generation. To address these challenges, ref. [40] evaluates the finite-resource performance of three representative Low Earth Orbit (LEO) missions: CQT-Sat, implementing entanglement-based BBM92; QUARC-ROKS, using decoy-state BB84; and QEYSSat, operating in both uplink and downlink configurations. Leveraging recent advances in finite-key analysis, the study demonstrates improved key extraction efficiency under high-loss conditions, enabling nonzero secure key generation from a single satellite pass.

The first large-scale space-to-ground quantum communication network is demonstrated in [41], integrating four metropolitan quantum key distribution (QKD) networks, a 2000 km fiber backbone, and two satellite–ground links to achieve end-to-end secure communication over 4600 km. The network incorporates optimized optical coupling, higher system clock rates, and an efficient decoy-state BB84 protocol, resulting in a satellite–ground key rate of 47.8 kbps—approximately 40 times higher than previous implementations. The architecture supports more than 150 users, provides resilience against known quantum attacks, and demonstrates long-term operational stability, representing a significant milestone toward global-scale quantum networks and future quantum Internet applications. Now we discuss one of the quantum techniques and give our own observations.

6.3.1. QCrypt: Advanced Quantum-Based Image Encryption for Secure Satellite Data Transmission

Insights

Advanced encryption techniques, like quantum-based encryption, enhance satellite communication security by leveraging quantum mechanics principles, which provide superior protection against cyber threats. The proposed QCrypt technique [42] utilizes quantum chaotic maps, classic chaotic maps, and DNA encoding to secure satellite and remote sensing images during transmission. This approach significantly improves resistance to attacks such as histogram analysis, differential attacks, and chosen-plaintext attacks, addressing the critical need for secure data transmission in the face of evolving cyber threats. The paper highlights the limitations of existing classical cryptography methods in securing satellite and remote sensing images, emphasizing their inadequacy in addressing the advanced security demands posed by increased cyber attack threats and the sensitive nature of the images being transmitted. It discusses recent advancements in quantum computing and

research, indicating that leveraging quantum mechanics and principles can significantly enhance security, thereby justifying the need for a novel quantum-based image encryption technique, QCrypt, which incorporates quantum chaotic maps, classic chaotic maps, and DNA encoding techniques.

In Figure 8, QCrypt employs quantum chaotic maps and classic chaotic maps as part of its encryption process, leveraging the principles of quantum mechanics to enhance the security of satellite and remote sensing images during transmission. The technique also incorporates DNA encoding methods, which contribute to the overall security framework, ensuring that the encrypted images are resistant to various types of attacks, including histogram analysis, differential attacks, and chosen-plaintext attacks.

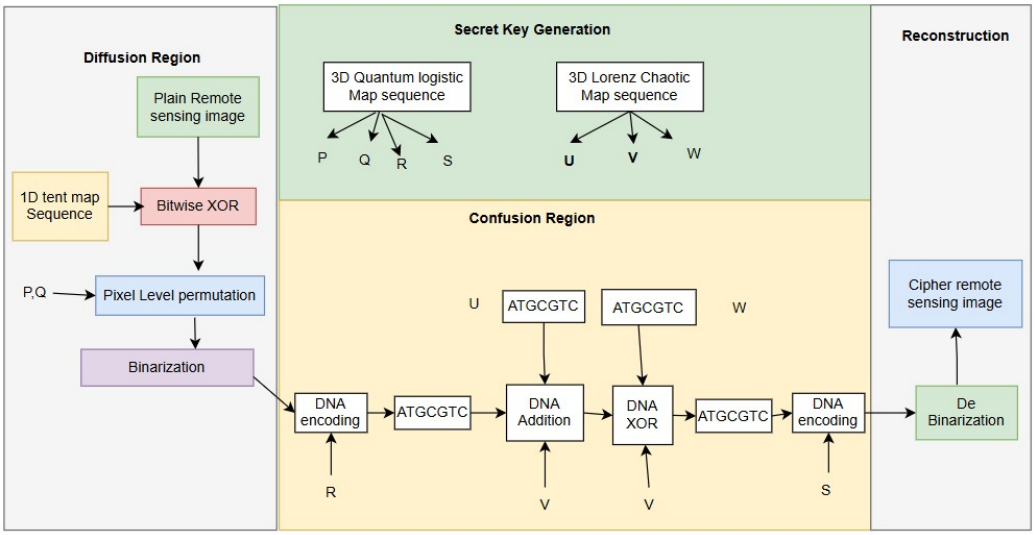

Figure 8. This diagram illustrates the step-by-step process of the QCrypt encryption model, including key generation using classical (Lorenz) and quantum chaotic maps, diffusion via pixel mixing and XOR operations, DNA-based confusion operations (encoding, addition, XOR, decoding), and final reconstruction into the encrypted cipher image.

The QCrypt encryption scheme demonstrated strong security and performance in encrypting satellite images from the MLRSNet dataset. It showed high key sensitivity, where even minor changes in the initialization values led to completely different encrypted outputs. The model effectively resisted chosen-plaintext attacks by disrupting predictable patterns using XOR operations and pixel permutations. Histogram analysis of the encrypted images revealed a uniform distribution, indicating strong resistance to statistical attacks. Chi-square test values for all sample images were below the critical threshold, confirming statistical uniformity. Entropy analysis yielded values close to the ideal value of 8, reflecting high unpredictability in the encrypted data. The scheme also showed excellent resistance to differential attacks, with NPCR values around 99.6% and UACI near 33%, indicating significant pixel-level changes with minor input modifications. Error metrics such as RMSE and PSNR confirmed strong encryption, showing low similarity between the original and encrypted images. Pixel correlation in encrypted images dropped to near-zero, highlighting the model's effectiveness in eliminating spatial redundancy. Compared to other existing models, QCrypt outperformed in reducing pixel correlation and improving UACI, establishing itself as a robust and efficient quantum-based encryption method suitable for secure satellite data transmission.

Critical Observations and Reflections on QCrypt

QCrypt introduces a hybrid image encryption method combining quantum chaotic maps, classical chaos, and DNA encoding, greatly enhancing security and randomness. It

achieves high resistance to attacks with NPCR (∼99.6%) and entropy (∼7.64), validated using realistic MLRSNet satellite images.

Despite its strong design, QCrypt's use of quantum principles remains at a simulation level through Qiskit, not leveraging real quantum hardware. The dependence on a centralized Key Management Center (KMC) introduces a potential single point of failure. Additionally, scalability to extremely large satellite images and performance under real-time constraints were not thoroughly evaluated. The study also lacks analysis of vulnerabilities to side-channel attacks, an important consideration for critical infrastructure.

QCrypt marks a significant step forward in advancing secure satellite image transmission by blending quantum-inspired chaos with DNA-based encryption. However, to achieve true deployment readiness, further work is needed on actual quantum implementation, decentralized key management, scalability optimization, and comprehensive security against hardware-level attacks.

6.4. Key Cybersecurity Mechanisms for Satellite Networks

Table 2 outlines essential countermeasures for securing satellite-based information networks. In addition to conventional methods like encryption, AI-driven anomaly detection, blockchain, and quantum communication, other mechanisms such as Intrusion Detection Systems (IDSs), secure multiparty computation, and satellite swarm resilience strategies are crucial. These measures collectively enhance threat detection, secure data transmission, and maintain operational integrity even under adversarial conditions, ensuring robust and future-proof satellite cybersecurity.

Table 2. Key countermeasures for securing satellite-based information networks.

Countermeasure	Mechanism	Citation(s)
Encryption and authentication	Protects data from interception and ensures authorized access.	[30,43]
AI and machine learning	Detects anomalies and predicts system failures in real time.	[9,15,16]
Federated learning-based IDS (AI/ML; privacy-preserving)	BiLSTM detectors train on-board/ground and aggregate via FedAvg to detect Sat–IoT threats without sharing raw telemetry.	[16]
Temporal CNN-based telemetry monitoring (AI/ML; real-time)	TCN forecasts next readings and flags anomalies from residuals, enabling fast on-orbit health monitoring.	[17]
Edge–ground distributed IDS for CAN bus (architecture + ML)	Lightweight on-board timing analysis pairs with ground-side payload inspection; models updated as firmware.	[18]
Explainable anomaly detection (XAI)	Compact magnitude/frequency/waveform features + lightweight classifier, with LIME explanations for each alert.	[19]
Network segmentation and filtering	Limits the spread of malicious activities and blocks suspicious traffic.	[9,23]
Blockchain technology	Ensures secure communication, authentication, and data integrity.	[32,33]
Active defense	Neutralizes attackers without harming legitimate users.	[44]
Quantum communication	Future-proofs networks against quantum attacks.	[8,37–42]
Cross-Layer Security Frameworks	Integrates multiple layers of defense against various types of attacks.	[30]
Best practices for SATCOM	Includes information sharing, risk management, and responses to threats.	[45]
Runtime verification	Monitors and simulates systems in real time to identify vulnerabilities.	[46]
Vulnerability assessment	Identifies and mitigates potential security risks through simulations.	[23]
Insider threat mitigation	Preserves data privacy during learning processes.	[9,10]
Redundant ground stations	Ensures service availability even if some stations are compromised.	[47]
Space cybersecurity policies	Addresses challenges posed by COTS hardware and software.	[1]
GNSS spoofing detection using wavelets and ML	Combines discrete wavelet transform with ML classifiers for accurate spoofing detection in GNSS signals.	[20]
Zero Trust-based authentication for ISLs	Applies continuous verification and lightweight HECC encryption to secure inter-satellite links against spoofing and replay attacks.	[34]
AI-oriented Two-Phase Multifactor Authentication in SAGINs	Cryptographic one-shot authentication with AI-based continuous verification using spatial–temporal features.	[35]
Finite-resource QKD for small satellites	Evaluates finite-key performance for CubeSat-based QKD missions, enabling secure keys under high-loss conditions.	[40]

Table 2. *Cont.*

Countermeasure	Mechanism	Citation(s)
Space-to-ground quantum communication network	Demonstrates a 4600 km quantum-secure communication network integrating fiber and satellite QKD links.	[41]
Quantum digital signatures over fiber	Implements QDS over 134 km equivalent fiber loss using DPS-QKD protocol for non-repudiation.	[36]
Gigahertz free-space QKD	Achieves real-time gigahertz QKD over an emulated satellite pass, full key distillation within one overpass.	[37]
Finite-key effects in satellite QKD	Analyzes finite-block statistics to optimize secret key length in short-duration satellite QKD links.	[38]
Network segmentation and filtering	K-Bottleneck Minimize routing avoids high-risk links, raising attacker cost and improving robustness.	[24]
Trust + ML-based filtering	Ensemble trust model with ACO routing achieves 98% accuracy in detecting and isolating DDoS traces.	[26]
Bottleneck Risk Analyzer (SKYFALL)	Identifies time-varying LEO bottleneck links; shows link flooding can cut throughput by 3.4×.	[27]
Trust-based secure routing (SLT)	D-S evidence trust evaluation integrated with OPSPF increases delivery rate and isolates malicious nodes.	[28]

This table consolidates the most effective cyber defense mechanisms for securing space-based information infrastructure.

7. Discussion and Future Direction

The cybersecurity of Space Information Networks (SINs) must evolve to meet the dynamic and increasingly sophisticated threat landscape. Based on the vulnerabilities, threat models, and emerging countermeasures identified in this survey, several key future research directions are recommended. Future work should focus on designing lightweight artificial intelligence (AI) and federated learning (FL) models [9,16] that operate efficiently within the constrained computational resources of satellites. These models must support real-time anomaly detection, resist adversarial inputs, and minimize communication overhead during federated training. Special attention must be given to adaptive learning techniques that can handle evolving threat landscapes and varying satellite network topologies without requiring frequent centralized updates.

Although current approaches show promise in strengthening segmentation and filtering for satellite networks, several challenges remain open. In [24], the authors suggest that future research should extend bottleneck-aware routing into multi-constellation and inter-operator environments, where traffic diversity could further raise attacker costs. In [26], the authors emphasize integrating real-time machine learning models that adapt to evolving attack patterns while minimizing the computational load on satellite nodes. The need is identified for federated and distributed IDS frameworks, which could share anomaly insights across satellites without exposing raw data. This could include proactive mitigation strategies that combine traffic scheduling and policy-based throttling with predictive analytics to anticipate time-varying bottleneck exploitation [27]. In [28], the authors recommend refining trust-based routing by incorporating cross-layer trust metrics (e.g., energy, mobility, QoS) to ensure more resilient detection and isolation of malicious nodes in dynamic LEO environments.

To mitigate Distributed Denial-of-Service (DDoS) attacks and predictable routing paths in large Low Earth Orbit (LEO) constellations, advanced randomized and context-aware routing algorithms [14] such as k-RAND must be further developed. Future algorithms should incorporate real-time topology changes, orbital dynamics, and multi-path diversity to improve uncertainty for attackers while maintaining low latency and efficient resource usage in dynamic satellite networks.

The development of standardized, scalable, and realistic space-specific simulation environments [12,13] is essential for evaluating and validating cybersecurity solutions

before real-world deployment. These testbeds should simulate diverse orbital environments (LEO, MEO, GEO), account for inter-satellite link variability and ground station interactions, and enable comprehensive modeling of cyber attack scenarios, including jamming, spoofing, and supply chain attacks.

As quantum computing progresses, the threat to traditional encryption methods grows. Research should prioritize the deployment of quantum-resistant encryption mechanisms [42] and quantum key distribution (QKD) for satellite communication systems..Future strategies must prioritize the integration of deepfake detection systems with quantum computing to create a resilient defense mechanism against AI-driven threats targeting satellite communications and smart city infrastructures. By combining AI-powered threat detection with quantum-resistant cryptography, these systems can proactively address the emerging challenges of cyberattacks in space and urban environments [48].

Blockchain-based solutions offer secure, decentralized authentication and data integrity for SINs [33]. Lightweight and scalable blockchain architectures adapted to high-latency, intermittent connectivity environments need further exploration. Building cybersecurity into the full system development lifecycle including supply chain assurance, secure software development, and in-orbit updates is essential. Security by design principles must become standard practice across space systems engineering.

Digital twins capable of simulating real-time operations and predicting cyber threats [46] would greatly enhance proactive threat identification, system introspection, and in-mission resilience.

Future strategies must promote collaboration between governments, space agencies, private industries, and academia. Establishing shared threat intelligence frameworks and common cybersecurity standards [10,45] will be key to enhancing global space infrastructure resilience.

8. Conclusions

This survey provided an in-depth analysis of the cyber vulnerabilities, threats, and countermeasures related to Space Information Networks. As satellites become increasingly critical to global communication, navigation, and defense, they have also become prime targets for sophisticated cyber attacks. Our review highlights that traditional cybersecurity methods are not enough to protect the complex and resource-limited environment of space systems.

We found that major vulnerabilities stem from system complexity, heavy reliance on Commercial Off-The-Shelf (COTS) components, weak encryption practices, and fragmented governance. The fast-evolving threat landscape ranging from DDoS attacks and spoofing to insider threats and emerging quantum-era risks calls for defense strategies that are advanced, flexible, and scalable.

New technologies like AI, federated learning, deep learning, blockchain, and quantum-resistant encryption offer promising ways to strengthen space system resilience. However, simply adopting new tools is not enough; their success depends on integrating secure-by-design principles, real-time verification, and rapid threat response into system development.

International collaboration, standardized cybersecurity frameworks, and better sharing of threat intelligence across sectors are also essential. Protecting Space Information Networks will require not just technical innovation but a coordinated effort among academia, industry, and government. Going forward, satellite missions must treat cybersecurity as a core part of their design and operations, from the earliest planning stages through the end of their lifecycle.

Author Contributions: Conceptualization, A.S. and B.U.M.; methodology, A.S.; validation, N.N., M.S. and M.J.H.F.; formal analysis, N.N. and M.S.; investigation, A.S. and B.U.M.; resources, M.S.; data curation, M.S. and N.N.; writing—original draft preparation, A.S. and B.U.M.; writing—review and editing, All Authors; visualization N.N. and M.S.; supervision, B.U.M. and M.J.H.F.; project administration, M.J.H.F. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding

Conflicts of Interest: The authors affirm that they have no conflicts of interest related to the publication of this manuscript. Furthermore, all ethical standards have been strictly upheld, including those concerning plagiarism, informed consent, research misconduct, data fabrication or falsification, duplicate publication or submission, and redundancy.

References

1. Thangavel, K.; Plotnek, J.J.; Gardi, A.; Sabbatini, R. Understanding and Investigating Adversary Threats and Countermeasures in the Context of Space Cybersecurity. In Proceedings of the 2022 IEEE/AIAA 41st Digital Avionics Systems Conference (DASC), Portsmouth, VA, USA, 18–22 September 2022; pp. 1–10. [CrossRef]
2. Borgia, S.; Topputo, F.; Zanero, S. HACK: A Holistic Modeling Approach for CubeSat Cyberattacks. *Mater. Res. Proc.* **2023**, *33*, 281–287. [CrossRef]
3. Yue, G.; Zhang, J.; Zhao, M.; Li, S.; Han, C.; Lin, X. LEO Satellite Constellation for 5G and Beyond: How to Address the Challenges? *Comput. Netw.* **2022**, *214*, 109144. [CrossRef]
4. Calabrese, M.; Kavallieratos, G.; Falco, G. A Hosted Payload Cyber Attack Against Satellites. In Proceedings of the AIAA SciTech 2024 Forum, Orlando, FL, USA, 8–12 January 2024; p. 0270. [CrossRef]
5. Shahzad, S.S.; Joiner, K.; Qiao, L.; Deane, F.; Plested, J. Cyber Resilience Limitations in Space Systems Design Process: Insights from Space Designers. *Systems* **2024**, *12*, 434. [CrossRef]
6. Willbold, J.; Sciberras, F.; Strohmeier, M.; Lenders, V. Satellite Cybersecurity Reconnaissance: Strategies and Their Real-World Evaluation. In Proceedings of the 2024 IEEE Aerospace Conference, Big Sky, MT, USA, 2–9 March 2024; pp. 1–13. [CrossRef]
7. Salim, S.; Moustafa, N.; Hassanian, M.; Ormod, D.; Slay, J. Deep-Federated-Learning-Based Threat Detection Model for Extreme Satellite Communications. *IEEE Internet Things J.* **2024**, *11*, 3853–3867. [CrossRef]
8. Kang, M.; Park, S.; Lee, Y. A Survey on Satellite Communication System Security. *Sensors* **2024**, *24*, 2897. [CrossRef]
9. Li, K.; Zhou, H.; Tu, Z.; Wang, W.; Zhang, H. Distributed Network Intrusion Detection System in Satellite-Terrestrial Integrated Networks Using Federated Learning. *IEEE Access* **2020**, *8*, 214852–214865. [CrossRef]
10. Akande, A.J.; Foo, E.; Hou, Z.; Li, Q. *Cybersecurity for Satellite Smart Critical Infrastructure*; Springer: Berlin/Heidelberg, Germany, 2023; pp. 1–22. [CrossRef]
11. Jero, S.; Furgala, J.; Heller, M.; Nahill, B.; Mergendahl, S.; Skowyra, R. Securing the Satellite Software Stack. In Proceedings of the Workshop on Security of Space and Satellite Systems (SpaceSec) 2024, San Diego, CA, USA, 1 March 2024; pp. 1–9. [CrossRef]
12. Zhuo, M.; Liu, L.; Zhou, S.; Tian, Z. Survey on security issues of routing and anomaly detection for space information networks. *Sci. Rep.* **2021**, *11*, 22261. [CrossRef]
13. Yue, P.; An J.; Zhang, J.; Ye, J.; Pan, G.; Wang, S.; Xiao, P.; Hanzo, L. Low Earth Orbit satellite security and reliability: Issues, solutions, and the road ahead. *IEEE Commun. Surv. Tutor.* **2023**, *25*, 1604–1652. [CrossRef]
14. Fratty, R.; Saar, Y.; Kumar, R.; Arnon, S. Random Routing Algorithm for Enhancing the Cybersecurity of LEO Satellite Networks. *Electronics* **2023**, *12*, 518. [CrossRef]
15. Singh, S.; Verma, S.; Pali, P.; Tiwari, H.; Kanojiya, S. Application of Artificial Intelligence (AI) to Enhance Satellite Security. *Int. J. Innov. Res. Comput. Commun. Eng.* **2023**, *12*, 3237–3240. [CrossRef]
16. Moustafa, N.; Khan, I.A.; Hassanin, M.; Ormrod, D.; Pi, D.; Razzak, I.; Slay, J. DFSat: Deep Federated Learning for Identifying Cyber Threats in IoT-based Satellite Networks. *IEEE Trans. Ind. Inform.* **2022**. [CrossRef]
17. Wang, Y.; Wu, Y.; Yang, Q.; Zhang, J. Anomaly Detection of Spacecraft Telemetry Data Using Temporal Convolution Networks. In Proceedings of the IEEE International Instrumentation and Measurement Technology Conference (I2MTC), Glasgow, UK, 17–20 May 2021. [CrossRef]
18. Almohri, H.M.J.; Nguyen, N.; Rana, M.M.; Matrawy, A.; Debbabi, M. CANSat-IDS: A Distributed Intrusion Detection System for Controller Area Networks in Satellites. *Comput. Secur.* **2024**, 138, 103617. [CrossRef]
19. Cuéllar, S.; Santos, M.; Alonso, F.; Fabregas, E.; Farias, G. Explainable anomaly detection in spacecraft telemetry. *Eng. Appl. Artif. Intell.* **2024**, *133*, 108083. [CrossRef]
20. Babic, K.; Balic, M.; Begusic, D. GNSS Spoofing Detection Based on Wavelets and Machine Learning. *Electronics* **2025**, *14*, 2391. [CrossRef]

21. Shahzad, S.S.; Joiner, K.; Qiao, L.; Deane, F.; Plested, J. Machine Learning Methods for Spacecraft Telemetry Mining. *IEEE Access* **2019**, *7*, 1–10. [CrossRef]
22. Azar, A.T.; Shehab, E.; Mattar, A.M.; Hameed, I.A.; Elsaid, S.A. Deep Learning-Based Hybrid Intrusion Detection Systems to Protect Satellite Networks. *J. Netw. Syst. Manag.* **2023**, *31*, 82. [CrossRef]
23. Toubi, A.; Hajami, A. Vulnerability Assessment and Mitigation Strategies for Satellite Communication Systems Under DDoS Attacks. In Proceedings of the International Conference on Global Aeronautical Engineering and Satellite Technology 2024 (GAST'24), Marrakesh, Morocco, 24–26 April 2024; pp. 1–8. [CrossRef]
24. Meng, F.; Yan, X.; Zhang, Y.; Yang, J.; Cao, A.; Liu, R.; Zhao, Y. Mitigating DDoS Attacks in LEO Satellite Networks Through Bottleneck Minimize Routing. *Electronics* **2025**, *14*, 2376. [CrossRef]
25. Park, J.; Eom, T.; Kim, H.; Park, H.; Yoon, Z.; Park, J. Threat Vector–Hierarchical Attack Representation Model-Based Threat Modeling and Security Assessment for Satellite Networks. *Appl. Sci.* **2025**, *15*, 2751. [CrossRef]
26. Panigrahi, L.; Pattanayak, B.K.; Mohanty, B.; Pattnaik, S.; Habboush, A.K. A Smart Secure Model for Detection of DDoS Malicious Traces in Integrated LEO Satellite–Terrestrial Communications. *Int. J. Electr. Electron. Res.* **2024**, *12*, 503–511. [CrossRef]
27. Deng, Y.; Wu, Q.; Lai, Z.; Gu, C.; Li, H.; Li, Y.; Liu, J. Time-varying Bottleneck Links in LEO Satellite Networks: Identification, Exploits, and Countermeasures. In Proceedings of the Network and Distributed System Security Symposium (NDSS), San Diego, CA, USA, 24–28 February 2025. [CrossRef]
28. Li, H.; Shi, D.; Wang, W.; Liao, D.; Gadekallu, T.R.; Yu, K. Secure Routing for LEO Satellite Network Survivability. *Comput. Netw.* **2022**, *211*, 109011. [CrossRef]
29. Tedeschi, P.; Sciancalepore, S.; Di Pietro, R. Satellite-Based Communications Security: A Survey of Threats, Solutions, and Research Challenges. *Comput. Netw.* **2022**, *216*, 109246. [CrossRef]
30. Abdrabou, M.; Gebali, F.; Shawky, M.A.; Alluhaidan, A.S.; Mansour, A.; El-Rahman, S.A.; Al-Ahwal, A.; Shamseldin, T. Advanced Security Framework for Low Earth Orbit Satellites in Space Information Network. *EURASIP J. Wirel. Commun. Netw.* **2024**, *2024*, 87. [CrossRef]
31. Surdi, S.A. Space Situational Awareness through Blockchain Technology. *J. Space Saf. Eng.* **2020**, *7*, 295–301. [CrossRef]
32. Wang, B.; Chang, Z.; Li, S.; Hämäläinen, T. An Efficient and Privacy-Preserving Blockchain-Based Authentication Scheme for Low Earth Orbit Satellite-Assisted Internet of Things. *IEEE Trans. Aerosp. Electron. Syst.* **2022**, *58*, 5153–5164. [CrossRef]
33. Li, C.; Sun, X.; Zhang, Z. Effective Methods and Performance Analysis of a Satellite Network Security Mechanism Based on Blockchain Technology. *IEEE Access* **2021**, *9*, 113558–113565. [CrossRef]
34. Farrea, K.A.; Baig, Z.; Doss, R.; Liu, D. Zero Trust-Based Authentication for Inter-Satellite Links in NextGen Low Earth Orbit Networks. *Ad Hoc Netw.* **2025**, *174*, 103817. [CrossRef]
35. Yang, B.; Liu, S.; Xu, T.; Li, C.; Zhu, Y.; Li, Z.; Zhao, Z. AI-Oriented Two-Phase Multifactor Authentication in SAGINs: Prospects and Challenges. *IEEE Consum. Electron. Mag.* **2024**, *13*, 79–90. [CrossRef]
36. Collins, R.J.; Amiri, R.; Fujiwara, M.; Honjo, T.; Shimizu, K.; Tamaki, K.; Takeoka, M.; Sasaki, M.; Andersson, E.; Buller, G.S. Experimental Demonstration of Quantum Digital Signatures over 43 dB Channel Loss Using Differential Phase Shift Quantum Key Distribution. *Sci. Rep.* **2017**, *7*, 3235. [CrossRef]
37. Roger, T.; Singh, R.; Perumangatt, C.; Marangon, D.G.; Sanzaro, M.; Smith, P.R.; Woodward, R.I.; Shields, A.J. Real-Time Gigahertz Free-Space Quantum Key Distribution within an Emulated Satellite Overpass. *Sci. Adv.* **2023**, *9*, eadj5873. [CrossRef]
38. Sidhu, J.S.; Brougham, T.; McArthur, D.; Pousa, R.G.; Oi, D.K.L. Finite Key Effects in Satellite Quantum Key Distribution. *NPJ Quantum Inf.* **2022**, *8*, 18. [CrossRef]
39. Dharminder, D.; Dadsena, P.K.; Gupta, P.; Sankaran, S. A Post-Quantum Secure Construction of an Authentication Protocol for Satellite Communication. *Int. J. Satell. Commun. Netw.* **2023** , *41*, 14–28. [CrossRef]
40. Islam, T.; Sidhu, J.S.; Higgins, B.L.; Brougham, T.; Vergoossen, T.; Oi, D.K.L.; Jennewein, T.; Ling, A. Finite-Resource Performance of Small-Satellite-Based Quantum-Key-Distribution Missions. *PRX Quantum* **2024**, *5*, 030101. [CrossRef]
41. Chen, Y.-A.; Zhang, Q.; Chen, T.-Y.; Cai, W.-Q.; Liao, S.-K.; Zhang, J.; Chen, K.; Yin, J.; Ren, J.-G.; Chen, Z.; et al. An Integrated Space-to-Ground Quantum Communication Network over 4600 Kilometres. *Nature* **2021**, *589*, 214–219. [CrossRef]
42. Mohamed Ihsan, P.M.; Arun, A.R.; Vetriselvi, V.; Gautham Kumar, G.; Praveen Kumar, R. QCrypt: Advanced Quantum-based Image Encryption for Secure Satellite Data Transmission. In Proceedings of the 2024 Third International Conference on Electrical, Electronics, Information and Communication Technologies (ICEEICT), Trichirappalli, India, 24–26 July 2024; pp. 1–9. [CrossRef]
43. Khare, S.; Singh, N. Securing Satellite Communication: Exploring Cybersecurity Measures in Satellite Networks. In Proceedings of the 2024 OPJU International Technology Conference (OTCON) on Smart Computing for Innovation and Advancement in Industry 4.0, Raigarh, India, 5–7 June 2024; pp. 1–5. [CrossRef]
44. Hsu, J.; Falco, G. Space Booby Traps: Hacking Back and Assured Cyber Deterrence in Space. In Proceedings of the 2023 IEEE International Conference on Assured Autonomy (ICAA), Laurel, MD, USA, 6–8 June 2023; pp. 115–118. [CrossRef]
45. Buenneke, R.H.; Abramson, R.L.; Shearer, T.D.; McArthur, P.B. Best Practices for Protection of Commercial Satellite Communications Infrastructure. In Proceedings of the AIAA, Keystone, CO, USA, 21–24 August 2006. [CrossRef]

46. Wan, M.; Fang, J.; Guo, C.; Geng, L.; Liu, Y.; Ma, W.; Xu, C.; Su, M. A Federated Learning-Based Intrusion Detection System for Satellite-Terrestrial Integrated Networks. In Proceedings of the IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP), Hyderabad, India, 6–11 April 2025; Volume 31. [CrossRef]
47. Saha, S.S.; Rahman, S.; Ahmed, M.U.; Aditya, S.K. Ensuring Cybersecure Telemetry and Telecommand in Small Satellites: Recent Trends and Empirical Propositions. *IEEE Aerosp. Electron. Syst. Mag.* **2019**, *34*, 34–49. [CrossRef]
48. Tariq, A.; Bibi, S.; Abbas, N. Protecting Satellite Communications and Smart Cities from AI-Powered Cyber Threats Using Deepfake Detection and Quantum Computing. *IEEE Access* **2025**, *13*, 11234–11256. [CrossRef]