A Comparative Analysis of Cyber Attacks against Satellite Internet*

Seungjin Baek, Hocheol Nam, and Min Suk Kang†

KAIST, Daejeon, Republic of Korea
{seungjinb,hcnam,minsukk}@kaist.ac.kr

Abstract

Satellite networks are rapidly expanding with the rise of large constellations such as Iridium, Globalstar, Starlink, and Eutelsat OneWeb, driving a global market projected to exceed USD 190 billion by 2029. As these services grow in scale and importance, securing their supporting infrastructure has become a critical challenge. In particular, ground stations—the gateways that connect space assets with terrestrial networks—represent a central attack surface exposed to a wide range of cyber and physical threats. This survey provides a comprehensive overview of security issues in ground station environments, with a focus on both attacks and defense mechanisms. We categorize major attack vectors, including user location inference, denial-of-service (DoS), spoofing, and vulnerabilities in satellite communication protocols, highlighting real-world cases and technical insights from recent research. On the defensive side, we examine core techniques such as authentication, secure protocols, and system evaluation, emphasizing how they mitigate threats and where they fall short. We further review emerging frameworks such as SPACE-SHIELD and SPARTA, which formalize attack models for satellite systems. Finally, we identify open challenges and research directions, including post-quantum cryptography adoption, resilient system design, and AI-driven intrusion detection. This survey aims to serve as a foundation for future work in securing ground stations and, by extension, the broader satellite ecosystem.

1 Introduction

Satellite communication has rapidly evolved into a critical pillar of global connectivity [34]. Large constellations in low and medium Earth orbit are being deployed to deliver broadband internet to underserved areas, to extend coverage across oceans and polar regions, and to support infrastructures ranging from disaster response to national defense [32, 10, 15, 13]. The scale of these deployments is unprecedented, with thousands of satellites forming dense constellations that provide low-latency, high-throughput communication worldwide. As reliance on satellite internet increases, the resilience and trustworthiness of these systems has become a central concern for governments, industry, and academia [39].

Unlike traditional terrestrial networks, satellite infrastructures combine space assets, ground stations, and widely distributed user terminals, each with distinct vulnerabilities [39]. Ground stations act as the bridge between orbit and terrestrial backbones, making them attractive targets for disruption or espionage. Satellites themselves operate under strict resource constraints and predictable orbital dynamics, which adversaries may exploit to degrade performance or infer sensitive information. User terminals, often deployed in large numbers and in untrusted environments, further expand the attack surface. This layered structure demands security models that integrate physical, network, and system-level considerations.

*Proceedings of the 8th International Conference on Mobile Internet Security (MobiSec'25), Article No. 59, December 16-18, 2025, Sapporo , Japan. © The copyright of this paper remains with the author(s).

†Corresponding author

The risks of satellite insecurity are not hypothetical. Recent incidents [36, 6, 5, 31, 24] have shown that both cyber and physical threats can disrupt services on a regional scale, with consequences extending to critical terrestrial infrastructures. At the same time, advanced threat actors continue to demonstrate sustained interest in satellite operators, motivated by espionage, sabotage, and strategic advantage. These developments highlight that satellite networks are not only enablers of connectivity but also high-value targets in modern conflict and competition.

In response, researchers and practitioners have begun to systematically explore the security of satellite systems [11, 7, 3, 20, 39]. New frameworks have been proposed to classify adversaries and attack vectors, while empirical studies have analyzed how the unique properties of orbital communication create new vulnerabilities. Other works have highlighted privacy concerns, such as the potential for location inference, and the susceptibility of satellite signals to manipulation [16, 23]. This growing body of knowledge underscores the need for holistic analyses that connect isolated findings into a coherent understanding of the threat landscape.

Defensive strategies are equally diverse, ranging from physical-layer authentication techniques to secure communication protocols and system-level evaluation frameworks. Some approaches focus on lightweight methods tailored to the constrained nature of satellite hardware, while others emphasize privacy-preserving routing [20] or cross-layer resilience [7]. Yet, despite promising progress, most defenses remain narrowly scoped, often addressing one dimension of the problem without considering broader integration. This fragmentation leaves open the challenge of designing comprehensive security architectures that can withstand both current and emerging threats.

In this survey paper, we aim to provide a structured overview of the evolving security landscape in satellite networking. We categorize prominent attack vectors (§4) and defensive approaches (§5), and we synthesize insights from recent research and operational experiences. By framing the discussion around confidentiality, availability, and trustworthiness, we highlight not only where progress has been made but also where significant gaps remain (§6). Ultimately, our goal is to outline the foundations for building secure and resilient satellite internet services that can support the critical demands of a globally connected society.

2 Background

Satellite Communication Overview. Satellite communication involves data exchange between orbiting satellites and terrestrial ground stations through radio frequency (RF) links. As illustrated in Figure 1, satellites can be deployed in different orbital regimes – Geostationary Earth Orbit (GEO), Medium Earth Orbit (MEO), and Low Earth Orbit (LEO) – each characterized by distinct altitude, coverage footprint, and satellite density. GEO satellites, positioned at approximately 36,000 km, provide wide coverage with relatively few satellites, but suffer from higher latency. MEO systems offer moderate coverage and latency trade-offs, while LEO constellations consist of thousands of satellites at altitudes below 2,000 km, enabling low-latency and high-throughput connectivity, but with higher deployment complexity. In practice, ground stations (or user terminals) act as gateways, relaying user traffic via *uplink* and *downlink* RF signals.

Satellite Internet Service. Recently, satellite-based internet services have rapidly expanded, driven by large-scale LEO and MEO constellation projects such as Iridium [15], Globalstar [13], Starlink [32], and Eutelsat OneWeb [10]. These systems aim to deliver broadband connectivity to underserved regions, enable global coverage, and support critical infrastructures. Reflecting this trend, the global satellite services market was valued at about USD 142 billion in 2024 and

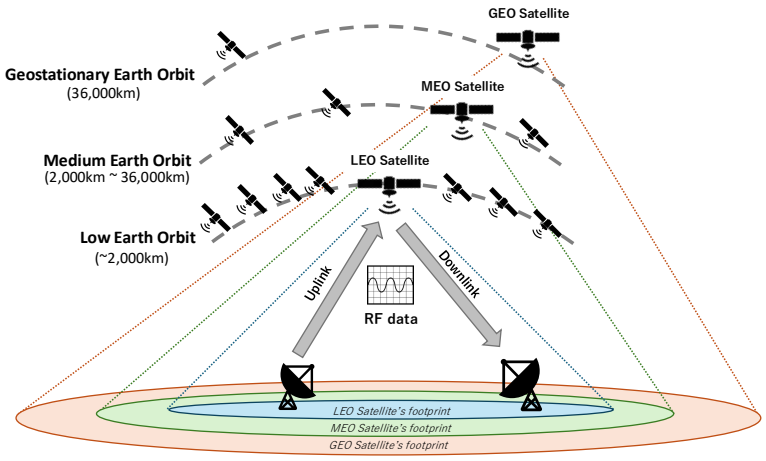


Figure 1: Satellite communication infrastructures.

is projected to reach nearly USD 194 billion by 2029 [34].

Satellite and Ground Station Security. With this expansion comes greater attention to security, particularly for ground stations that serve as the critical interface between satellites and terrestrial networks. To address emerging cyber threats in this domain, new attack matrices such as SPACE-SHIELD [9] and SPARTA [1] have been developed, offering structured frameworks for classifying adversaries, attack stages, and vulnerabilities in satellite and ground infrastructure. In parallel, there has been a noticeable increase in academic and industrial studies on satellite and ground station security, covering topics such as RF jamming, intrusion detection, supply-chain vulnerabilities, and resilient communication protocols, highlighting the growing recognition of cybersecurity as a cornerstone for the sustainable development of satellite networks.

Real-World Incidents. The vulnerability of satellite infrastructures has been repeatedly exposed through real-world cyber and electronic attacks. In February 2022, the *KA-SAT attack* disrupted Viasat's satellite internet services across Europe. Attackers gained access to a ground-based VPN management server and deployed a destructive wiper malware, *AcidRain*, which disabled tens of thousands of user modems and even disrupted terrestrial operations such as wind turbine control in Germany [36].

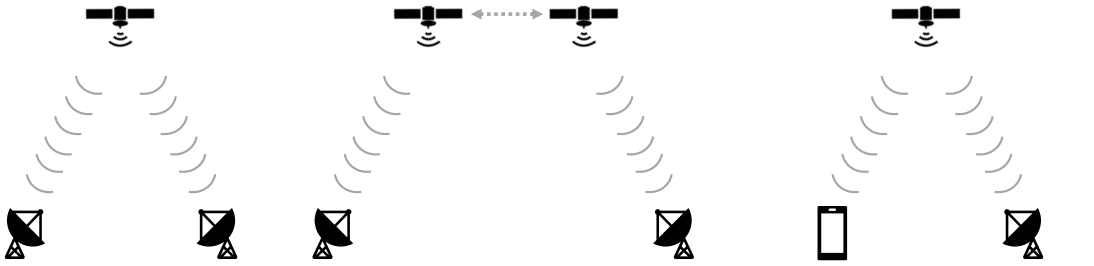
In parallel, U.S. cybersecurity agencies reported that Russia's APT28 (Fancy Bear) infiltrated a U.S. satellite communications provider, maintaining long-term persistence for espionage and intelligence collection [6, 5]. These findings aligned with broader U.S. government attributions linking Russian state-sponsored actors to coordinated attacks against commercial SATCOM providers in support of wartime operations [6].

Beyond Russian operations, other advanced persistent threat (APT) groups have actively targeted the satellite ecosystem. The espionage group *Thrip* was observed attacking satellite, telecom, and defense sectors in the U.S. and Southeast Asia using custom malware and "living-off-the-land" techniques [31]. More recently, the Iranian-linked group *Peach Sandstorm* (APT33/Elfin) launched large-scale password spray campaigns against high-value targets, including satellite and telecommunications firms, as a precursor for deeper intrusions and intelligence collection [24].

Together, these incidents underscore that satellite networks are high-value targets under

Category	Model	Description	Use Cases
Transmission-based Classification	Bent-Pipe (Transparent Relay)	Satellite transparently relays signals by amplification and frequency conversion; simple and low-cost but requires dense ground stations.	Broadcast satellites, VSAT
	Inter-Satellite Link (ISL)	Satellites connect via optical/RF crosslinks to form a mesh; reduces ground reliance but adds high cost and pointing complexity.	Starlink, OneWeb (future), military constellations
	Direct-to-Cell / Direct-to-Device	Satellites directly connect to mobile/IoT devices without dedicated terminals; enables ubiquitous coverage but limited by spectrum and bandwidth.	Starlink Direct-to-Cell, Lynk, AST SpaceMobile
Processing-based Classification	Store-and-Forward	Satellite stores data onboard until ground contact; useful for remote areas but adds latency and requires onboard storage/power.	Orbcomm, EO satellites, DTN messaging
	Regenerative (Onboard Processing)	Satellite demodulates, processes, and remodulates signals; improves efficiency and QoS but increases payload cost and power demand.	Viasat-3, advanced HTS, Cisco IRIS

Table 1: Satellite communication models categorized by transmission path and processing.



(a) Bent-pipe topology (b) Inter-satellite link topology (c) Direct-to-cell / Direct-to-device

Figure 2: Transmission-based satellite communication model

continuous threat from state-level and APT adversaries. They highlight the urgent need for resilient architectures, intrusion detection, and coordinated threat intelligence sharing to secure both orbital and terrestrial assets.

3 Architectural Models of Satellite Communication

Satellite communication systems can be realized through several architectural models, each balancing performance, infrastructure cost, and operational complexity in different ways. Table 1 summarizes the main modes along with their descriptions and representative use cases, while Figure 2 and Figure 3 illustrate their structural differences. These models can be broadly grouped into *transmission-based* (§3.1) and *processing-based* (§3.2) classifications: The former focuses on how data is delivered across the satellite network, while the latter concerns how data is handled onboard the satellite. In the following, we elaborate on each category in detail.

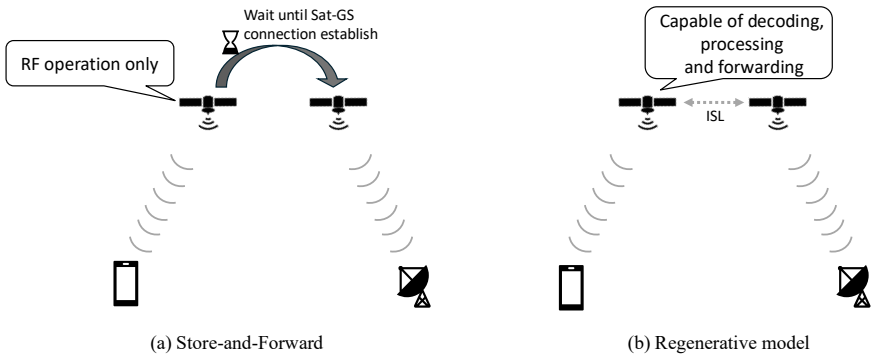


Figure 3: Processing-based satellite communication model

3.1 Transmission-based Classification

Bent-Pipe (Transparent Relay). As illustrated in Figure 2(a), the bent-pipe model is the simplest and most traditional form of satellite communication. The satellite functions as a transparent repeater that amplifies and shifts the uplink frequency to the downlink without any onboard processing. Its strengths are low implementation cost, proven reliability, and suitability for broadcast services such as TV and VSAT. The key limitation, however, is its heavy reliance on a dense network of ground stations, which restricts scalability for modern large-scale broadband constellations.

Inter-Satellite Link (ISL). The ISL-based model (Figure 2(b)) allows satellites to exchange data directly through optical or RF crosslinks, creating a space-based mesh. This design reduces the need for ground gateways and enables more flexible routing, as data can traverse multiple satellites before reaching the earth. Such capability is particularly attractive for global constellations that seek continuous service coverage with a limited number of gateways. The trade-off lies in payload complexity and cost, as ISLs demand precise pointing, acquisition, and tracking subsystems.

Direct-to-Cell / Direct-to-Device. As shown in Figure 2(c), direct-to-device architectures connect satellites directly to unmodified mobile phones or IoT devices. This model extends coverage to underserved or emergency regions without requiring dedicated satellite terminals, making it one of the most visible examples of non-terrestrial networks (NTNs) in practice. Recent trials by Starlink, Lynk, and AST SpaceMobile illustrate its feasibility. Nevertheless, technical and regulatory challenges remain, including spectrum coordination, limited per-user bandwidth, and seamless interoperability with terrestrial networks.

3.2 Processing-based Classification

Store-and-Forward (S&F). The store-and-forward model (Figure 3(a)) enables satellites to buffer data onboard and transmit it once a ground station comes into view. This architecture is valuable for regions with sparse ground infrastructure, such as polar or maritime areas. It has long been used in earth observation missions and delay-tolerant networking (DTN) experiments. The drawback is high latency, ranging from minutes to hours depending on orbit, and the additional requirements for onboard storage and power.

Regenerative (Onboard Processing). The regenerative model (Figure 3(b)) equips satellites with onboard processing capabilities, allowing signals to be demodulated, decoded, pro-

Attack Type	Description / Techniques	Impact / Examples
Denial of Service (DoS)	Link-flooding attacks (LFAs), topology exploits, energy-drain attacks	Service disruption via bottleneck congestion; ICARUS [11], SKYFALL [7], StarMaze [37], StarMelt [40], SatOver [22]
User Location Inference	Exploits predictable signals, mobility patterns, or passive reception of satellite messages	Compromises user privacy; DCator [23], RECORD [16]
Satellite Spoofing	Downlink overshadowing, VSAT signal injection, GNSS spoofing	Misleading receivers or ground stations; GNSS-WASP [35], VSAT modem injection [2]

Table 2: Summary of major attack categories against satellite networks.

cessed (e.g., error correction or switching), and remodulated before retransmission. This approach enhances link efficiency, reduces reliance on ground infrastructure, and enables advanced functions such as traffic shaping and quality-of-service support. At the same time, it increases payload cost and power consumption, which can constrain satellite lifetime due to thermal and energy limitations. Recent projects also explore regenerative payloads as part of NTN research, where partial network functions may be migrated into orbit to support tighter integration with terrestrial systems.

4 Attacks Against Satellite Networks

Satellite networks face a diverse range of threats that can undermine confidentiality, availability, and trustworthiness of services. Among the most critical are attacks that exploit inherent characteristics of satellite communications to expose user privacy, disrupt service continuity, or manipulate system behavior. In this section, we examine three major categories of such threats: *denial of service (DoS)*, *user location inference*, and *spoofing*. Table 2 provides a structured overview of these categories, summarizing their techniques, impacts, and representative works.

4.1 Denial of Service

Link-Flooding Attacks (LFA). Link-flooding attacks overwhelm capacity-limited, time-varying bottlenecks by generating or steering high-volume flows to saturate a network link [33, 18]. In LEO constellations, such floods can be timed to hit a beam, gateway, or inter-satellite link precisely when it becomes the network's critical choke point. Because LEO routing and beam footprints change predictably (satellites move, handovers occur), an attacker that times traffic bursts or amplifies flows can produce transient but severe congestion that degrades service for many users served by that link.

ICARUS [11] demonstrates that attackers can exploit this predictability by launching volumetric floods synchronized with satellite mobility and routing dynamics. By targeting specific ground-satellite or inter-satellite links, ICARUS shows that even modest attack volumes can trigger disproportionate disruption, causing temporary outages across significant portions of a constellation.

Skyfall [7] extends this perspective by analyzing how bottleneck links in LEO constellations emerge and shift over time due to moving beams and varying link capacities. Using real constellation and ground-station data, the study shows that attackers who continuously adapt to

these dynamic congestion points can substantially reduce legitimate throughput, highlighting the limitations of conventional LFA defenses designed for terrestrial networks.

Topology Exploits. Attacks that exploit constellation topologies manipulate routing or forwarding logic to steer traffic, so that a relatively small amount of malicious traffic or a modest number of compromised endpoints produces outsized disruption. Unlike blunt high-bandwidth flooding, topology exploits take advantage of predictable routing decisions, time-varying link availability, and the constrained set of inter-satellite and gateway paths to concentrate load on a few critical links or nodes. By doing so, an attacker can amplify congestion, increase queuing and latency, and provoke cascading route oscillations without supplying commensurate raw bandwidth.

StarMaze [37], introduces a ring-based attack that systematically disables a subset of ISLs along orbital rings. Even with only partial disruption, the attack funnels traffic into maze-like detours and local minima, amplifying latency and, under certain routing strategies, rendering destinations unreachable.

Direct-to-Cell Signaling Exploits. Beyond link-flooding or topology-aware exploits, recent work highlights how vulnerabilities inherited from terrestrial LTE/5G protocols can be amplified in direct-to-cell (D2C) satellite mega-constellations. Liu et al. [22] introduce SatOver, a cross-layer control-plane attack that leverages plaintext registration and broadcast signalings in LTE/5G to hijack commodity phones or IoT devices and delay their access to satellites. Unlike traditional jamming or registration-reject attacks that disrupt only a single cell or service area, SatOver exploits the constellation's extreme scale and centralized ground-station processing to induce signaling congestion and enforce backoff timers, effectively blocking all logical service areas at once. Moreover, by rapidly reconfiguring forged identities and mimicking the RF/geometry dynamics of mobile satellites, SatOver obfuscates its presence and sustains long-lasting denial of service across urban-scale regions. This demonstrates that protocol-layer weaknesses, when combined with LEO constellations' unique mobility and scale, can undermine availability as seriously as high-volume data-plane floods.

Energy-Drain Attacks. Energy-drain attacks force satellites or user terminals to perform repeated power-intensive activity (wake-ups, retransmissions, or high power signaling) to exhaust limited energy budgets and cause service loss. StarMelt [40] persistently injects carefully routed malicious traffic through the forwarding paths of a victim satellite to prevent hibernation, effectively reducing battery lifetime.

4.2 User Location Inference

A user location inference attack in satellite networks refers to an adversary's ability to determine where a user is located based on the signals exchanged with satellites, even when the user does not intend to reveal this information. Such attacks are critical because they compromise privacy at a global scale: satellites cover vast regions, and even coarse-grained localization can expose sensitive information about individuals, organizations, or governments.

DCator [23] investigate this threat in the context of direct-to-cell systems, where satellites connect directly to mobile phones. It shows that the way signals are transmitted and the mobility patterns of users inherently leak information about their location, making ordinary communication susceptible to tracking without any active attack.

In contrast, RECORD [16] demonstrates a practical, passive attack that does not rely on the user's transmissions at all. Instead, it leverages only the reception of broadcast satellite messages to infer the user's regional position with triangulation. This highlights that location privacy risks exist not only in active communication but also in passive scenarios where a user

simply receives data from satellites.

4.3 Satellite Spoofing

Downlink Shadowing. A satellite link has two directions: the uplink (ground → satellite) and the downlink (satellite → ground); security differs between them because transmit power, antenna gain, and reachability change. Downlink can be an attack surface when attacker sends a stronger or otherwise preferable counterfeit signal, so the victim locks onto the attacker instead of the satellite.

Salkield et al. [30] measure the attacker power required for downlink overshadowing as a function of victim receive power, antenna sidelobe attenuation, and modulation/noise margins, and validate this budget with measurements and simulations. Their results show most tested satellite links are vulnerable at short range and that practical spoofing can be carried out with modest transmit power and equipment often on the order of $2k.

VSAT Signal Injection. VSAT is a class of ground terminal (Very Small Aperture Terminal) used for two-way satellite communications—a small dish plus a modem that connects remote sites to satellite networks. The satellite link and the modem's RF/physical interfaces are both attack surfaces: an attacker can transmit crafted radio waves at the air interface or feed malformed frames that the modem will receive and process.

Bisping et al. [2] identify vulnerabilities across VSAT modems' RF front ends, baseband parsers, and firmware that allow adversaries to corrupt internal state or cause the device to execute unintended behavior. By injecting carefully crafted RF signals or malformed packets, an attacker can trigger erroneous commands or denial-of-service—often achievable with modest, short-range equipment.

GNSS Spoofing. GNSS is a global navigation satellite system that provides positioning, navigation, and timing information. GNSS spoofing can lead to incorrect location or timing data, which can affect transportation, aviation, and critical infrastructure.

GNSS-WASP [35] introduces a wide-area spoofing technique using a small constellation of synchronized transmitters that can mislead any number of GNSS receivers within a region, without tracking their precise locations. By preserving relative distances and movements, the attack can divert fleets or swarms while evading countermeasures that rely on multi-receiver consistency or sudden-movement detection. A prototype with off-the-shelf SDRs shows the feasibility of such large-scale, coordinated spoofing, with errors small enough to remain hidden in normal GNSS noise.

5 Defense Techniques

To protect satellite networks and their ground infrastructure, a range of defense techniques have been proposed that address different layers of the system [27, 19, 17, 3, 28, 8, 39, 25, 38]. Effective security requires ensuring that only trusted entities can interact with satellites, that communication channels remain confidential and tamper-resistant, and that deployed systems are rigorously tested against evolving threats. In this section, we focus on three key defense approaches—*authentication*, *secure protocols*, and *system evaluation*—that together provide the foundation for building resilient satellite communication environments. Table 3 summarizes these categories, highlighting their mechanisms and representative works.

Defense Category	Mechanism / Techniques	Representative Works
Identification & Authentication	Physical-layer fingerprinting, orbit-based timing authentication, lightweight certificate validation	PAST-AI [27], Orbit-based Auth [17], V'CER [19]
Secure Protocols	Redesign of encryption/PEP for satellite links, secure ranging, resilient and privacy-preserving routing	QPEP [28], LEO-Range [4], ICARUS [11], Skyfall [7], AnonSat [20], StarVeri [14]
System & Analysis	Health monitoring, fault injection, experimental system studies	Chirper [25], RADSIM [38]

Table 3: Summary of major defense techniques in satellite networks.

5.1 Identification & Authentication

Physical Layer Authentication. Physical-layer authentication exploits signal or propagation characteristics that are inherently difficult for attackers to forge.

Physical-layer authentication leverages characteristics of signals or propagation environments that are inherently difficult for adversaries to forge. Orbit-based authentication [17] exploits predictable timing differences caused by orbital mechanics: by comparing observed time-difference-of-arrival (TDOA) signatures across multiple receivers with those expected from public orbital data, it can reliably distinguish legitimate satellites from spoofed transmitters. This approach offers a lightweight security enhancement without requiring cryptographic keys or hardware changes.

Building on a different principle, PAST-AI [27] applies deep learning to classify satellite transmitters based on subtle, hardware-induced features in their physical-layer emissions. Using over 100 million I/Q samples from Iridium satellites, the study shows that even satellites of the same constellation and type exhibit distinct radio fingerprints, enabling accurate transmitter authentication.

Cryptography. Cryptographic validation remains a cornerstone of secure communications, but traditional certificate checks are often too resource-heavy for constrained or satellite-based networks.

V'CER [19] redesigns certificate validation to solve the problem of timely revocation in constrained networks such as satellites without the heavy resource use of traditional methods. The scheme utilizes Sparse Merkle Trees (SMTs) to perform lightweight revocation checks and enables devices to collaborate, allowing validation information to spread epidemically. This distributed approach minimizes communication overhead and significantly reduces the need for devices to contact centralized authorities for updates, making secure TLS handshakes feasible in low-power, intermittently connected environments.

Cross-System Approach. Cross-system approaches provide another way to detect spoofing by leveraging independent satellite constellations.

Oligeri et al. [26] proposes using the Iridium communication satellites as an auxiliary reference. This technique exploits publicly-available IRIDIUM Ring Alert (IRA) messages to provide an independent position estimate that can be cross-checked against GNSS data, making it difficult for an attacker to forge synchronized signals across both systems. Crucially, this opportunistic solution requires only a single receiving antenna and no dedicated hardware, making it highly suitable for remote or unattended environments like open seas.

5.2 Secure Protocol

Satellite and Mobile Phones. Satellite links are increasingly integrated into mobile devices, but the protocols enabling satphone connectivity or smartphone satellite messaging introduce unique security concerns.

Classen et al. [3] successfully reverse-engineered Apple's proprietary iOS satellite messaging stack, finding flaws that could permit adversaries to send unauthorized data and exploit privacy leaks through the channel.

Similarly, Driessen et al. [8] analyzed the legacy GMR-1 and GMR-2 satphone standards by extracting their proprietary ciphers from firmware, demonstrating practical attacks that can compromise session keys or even succeed with ciphertext-only analysis.

Low Layer Re-Design. In high-latency satellite links, traditional network stack may suffer from performance degradation, so redesigning the lower layers can reconcile performance and security.

QPEP [28] introduced a hybrid QUIC-based Performance Enhancing Proxy (PEP)/VPN system that encrypts traffic by default while demonstrably improving page load times over Geostationary Earth Orbit (GEO) links compared to traditional VPNs.

For security at the physical layer, LEO-Range [4] proposes a novel ranging scheme compatible with OFDM for Low Earth Orbit (LEO) satellites and devices, offering provable security against distance-reduction attacks to verify the secure time-of-arrival.

Secure Routing. Choosing the proper route is crucial in the satellite network for security [12]. Unlike terrestrial networks, LEO constellations introduce highly dynamic topologies and bottleneck links, which create new attack surfaces. ICARUS [11] demonstrates that adversaries can exploit the predictable routing and publicly known satellite orbits to launch volumetric link-flooding attacks, congesting critical inter-satellite or ground-to-satellite links with relatively low bandwidth. Their analysis shows that even a few thousand compromised terminals suffice to disrupt connectivity between large terrestrial regions, highlighting the need for routing strategies that balance latency with resilience [12].

Similarly, Skyfall [7] focuses on the time-varying nature of bottleneck links in LEO networks. By profiling spatio-temporal bottleneck characteristics, Skyfall shows that compromised user terminals can continuously overload dynamic downlink channels, reducing legal traffic throughput. The system further emphasizes that conventional LFA countermeasures from terrestrial networks are insufficient, calling for LEO-specific defenses such as adaptive traffic scheduling and multi-path routing.

Beyond resilience against flooding, routing security must also ensure that forwarding paths avoid high-risk regions where adversaries may intercept or hijack traffic. STARVERI [14] addresses this challenge by introducing an efficient verification framework for risk-avoidance routing in LEO satellite networks. It combines dynamic relay selection with lightweight segment-based path verification, ensuring that actual forwarding paths comply with operator-defined avoidance policies. Unlike crypto-based methods that impose heavy computation on all satellites or delay-based methods that suffer from inaccuracy under dynamic topologies, STARVERI achieves near-100% verification accuracy with minimal communication overhead, while scaling to constellations with thousands of nodes:contentReference[oaicite:1]index=1. This makes it particularly suitable for operators seeking both efficiency and trustworthiness in next-generation satellite internets.

On the other hand, routing security is not only about availability but also about privacy. AnonSat [20] addresses the critical risk of user localization through triangulation of satellite signals, a threat that has proven lethal to journalists and activists in conflict zones. AnonSat

reroutes users' traffic through a mesh of distant satellite gateways connected by long-range wireless links (such as LoRa), preventing adversaries from directly mapping uplink signals to users' true locations. By periodically changing the output gateway, the system ensures that triangulation attempts cannot reliably trace back to the origin, thereby enhancing anonymity and protecting human rights defenders under surveillance.

5.3 System & Analysis

Security System. Several recent studies have focused on developing additional systems to enhance the safety and reliability of satellites. Chirper [25] introduces an isolated health monitoring system designed to detect and respond to faults in satellite subsystems without interfering with their primary operations, thereby improving system resilience and mission longevity. RADSIM [38] presents an automated framework for simulating single-bit flip errors in satellite firmware, enabling a thorough evaluation of how cosmic radiation affects the effectiveness of software-based exploit mitigations.

Case Study & SoK. With the rapid growth of the space sector, it is important to study real systems and summarize current knowledge. Willbold et al. [39] analyze firmware from operational LEO satellites, providing a taxonomy of vulnerabilities in CubeSats and other small satellites. Remy et al. [29] categorize attack surfaces across space, satellite, and ground segments and review existing defenses. Koisser et al. [21] examine trust and privacy issues, including PKI vulnerabilities and risks of unauthorized location tracking in satellite networks.

6 Discussion

Satellite networks present a complex and evolving attack surface, shaped by the unique characteristics of space-based communication systems. The review of both attack strategies and defense mechanisms highlights several key insights.

First, the inherent predictability and constrained resources of satellite systems make them susceptible to specialized attacks, such as link-flooding, energy-drain, and user location inference. LEO constellations, in particular, are vulnerable due to their dynamic beam footprints and time-varying routing topologies, which can be exploited by attackers for transient but severe disruptions. Attacks like ICARUS [11] and Skyfall [7] demonstrate that even moderate adversary capabilities can induce widespread service degradation when exploiting routing and congestion patterns. Meanwhile, spoofing attacks—including GNSS and VSAT signal manipulation—illustrate that the physical and RF layers of satellite systems remain critical points of vulnerability.

Second, recent defense mechanisms show promise but also reveal trade-offs between security, performance, and practicality. Physical-layer authentication, orbit-based identification, and cross-system verification offer lightweight yet effective protections against spoofing without relying solely on computationally expensive cryptography. Protocol enhancements, including QPEP [28] and LEO-Range [4], illustrate that secure communications can be maintained even over high-latency satellite links, while systems like AnonSat[20] protect user privacy by mitigating localization risks. Furthermore, evaluation frameworks such as Chirper and RADSIM provide tools to analyze vulnerabilities under realistic operational conditions, reinforcing the importance of proactive system testing.

Finally, the interplay between attacks and defenses underscores that satellite network security is inherently multidisciplinary. Effective protection requires integrating cryptography, signal processing, network architecture, and operational monitoring. Defenses that target a

single layer are insufficient; instead, resilient systems must combine physical, protocol, and analytical strategies to anticipate both current and emerging threats.

7 Conclusion

Satellite networks are critical infrastructure supporting communication, navigation, and global connectivity, yet they face distinctive security challenges arising from their physical, protocol, and operational characteristics. Our review of attacks demonstrates that LEO constellations and ground terminals are susceptible to link-flooding, energy-drain, location inference, and spoofing attacks. At the same time, emerging defense strategies—ranging from physical-layer authentication to secure routing protocols and robust system evaluation frameworks—highlight effective approaches for mitigating these threats.

However, the ongoing evolution of satellite constellations, the increasing interdependence of space and terrestrial networks, and the resource constraints inherent to satellites imply that security research must remain adaptive. Future work should emphasize cross-layer resilience, real-time threat detection, and privacy-preserving protocols, ensuring that satellite networks remain robust against both known and emerging threats. Ultimately, a holistic approach that integrates physical, cryptographic, and operational measures is essential for building trustworthy and resilient space-based communication infrastructures.

8 Acknowledgments

This work was supported by the Institute of Information & Communications Technology Planning & Evaluation(IITP) grant funded by the Korea government(MSIT) (No.RS-2025-02263143, Development of Cybersecurity Threat Response Technologies for Satellite Ground Stations)

References

[1] Aerospace Corporation. Space Attack Research & Tactic Analysis (SPARTA). [Online], 2021. https://sparta.aerospace.org/.

[2] Robin Bisping, Johannes Willbold, Martin Strohmeier, and Vincent Lenders. Wireless Signal Injection Attacks on VSAT Satellite Modems. In *33rd USENIX Security Symposium (USENIX Security 24)*, pages 6075–6091, 2024.

[3] Jiska Classen, Alexander Heinrich, Fabian Portner, Felix Rohrbach, and Matthias Hollick. Starshields for ios: Navigating the security cosmos in satellite communication. In *2025 Network and Distributed System Security Symposium (NDSS)*, 2025.

[4] Daniele Coppola, Arslan Mumtaz, Giovanni Camurati, Harshad Sathaye, Mridula Singh, and Srdjan Capkun. Leo-range: Physical layer design for secure ranging with low earth orbiting satellites. In *34th USENIX Security Symposium (USENIX Security 25)*, pages 7059–7075, 2025.

[5] CyberScoop News. CISA researchers: Russia's Fancy Bear infiltrated US satellite network. [Online], 2022. https://cyberscoop.com/apt28-fancy-bear-satellite/.

[6] Cybersecurity and Infrastructure Security Agency (CISA). U.S. Government Attributes Cyberattacks on SATCOM Networks to Russian State-Sponsored Malicious Cyber Actors. [Online], 2022. https://www.cisa.gov/news-events/alerts/2022/05/10/us-government-attributes-cyber attacks-satcom-networks-russian-state-sponsored-malicious-cyber-actors.

[7] Yangtao Deng, Qian Wu, Zeqi Lai, Chenwei Gu, Hewu Li, Yuanjie Li, and Jun Liu. Time-varying Bottleneck Links in LEO Satellite Networks: Identification, Exploits, and Countermeasures. In *2025 Network and Distributed System Security Symposium (NDSS)*, 2025.

[8] Benedikt Driessen, Ralf Hund, Carsten Willems, Christof Paar, and Thorsten Holz. Don't trust satellite phones: A security analysis of two satphone standards. In *2012 IEEE Symposium on Security and Privacy (SP)*, pages 128–142. IEEE, 2012.

[9] European Space Agency. Space Attacks and Countermeasures Engineering Shield (SPACESHIELD). [Online], 2023. https://spaceshield.esa.int/.

[10] Eutelsat Group. Eutelsat OneWeb. [Online], 2012. https://www.eutelsat.com/satellite-network/oneweb-leo-constellation.

[11] Giacomo Giuliari, Tommaso Ciussani, Adrian Perrig, and Ankit Singla. ICARUS: Attacking low Earth orbit satellite networks. In *2021 USENIX Annual Technical Conference (USENIX ATC 21)*, pages 317–331, 2021.

[12] Giacomo Giuliari, Tobias Klenze, Markus Legner, David Basin, Adrian Perrig, and Ankit Singla. Internet backbones in space. *ACM SIGCOMM Computer Communication Review*, 50(1):25–37, 2020.

[13] Globalstar. Globalstar - satellite solutions & services. [Online], 2024. https://www.globalstar.com/en-us.

[14] Chenwei Gu, Qian Wu, Zeqi Lai, Hewu Li, Jihao Li, Weisen Liu, Qi Zhang, Jun Liu, and Yuanjie Li. Starveri: Efficient and accurate verification for risk-avoidance routing in leo satellite networks. In *2024 IEEE 32nd International Conference on Network Protocols (ICNP)*, pages 1–11. IEEE, 2024.

[15] Iridium Communications Inc. Iridium Satellite Communications. [Online], 2005. https://www.iridium.com/.

[16] Eric Jedermann, Martin Strohmeier, Vincent Lenders, and Jens Schmitt. RECORD: A RECeption-Only Region Determination Attack on LEO Satellite Users. In *33rd USENIX Security Symposium (USENIX Security 24)*, pages 6113–6130, 2024.

[17] Eric Jedermann, Martin Strohmeier, Matthias Schäfer, Jens Schmitt, and Vincent Lenders. Orbit-based authentication using TDOA signatures in satellite networks. In *Proceedings of the 14th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, pages 175–180, 2021.

[18] Min Suk Kang, Soo Bum Lee, and Virgil D Gligor. The crossfire attack. In *2013 IEEE symposium on security and privacy*, pages 127–141. IEEE, 2013.

[19] David Koisser, Patrick Jauernig, Gene Tsudik, and Ahmad-Reza Sadeghi. V'CER: Efficient certificate validation in constrained networks. In *31st USENIX Security Symposium (USENIX Security 22)*, pages 4491–4508, 2022.

[20] David Koisser, Richard Mitev, Marco Chilese, and Ahmad-Reza Sadeghi. Don't Shoot the Messenger: Localization Prevention of Satellite Internet Users. In *2024 IEEE Symposium on Security and Privacy (SP)*, pages 426–444. IEEE, 2024.

[21] David Koisser, Richard Mitev, Nikita Yadav, Franziska Vollmer, and Ahmad-Reza Sadeghi. Orbital trust and privacy: SoK on PKI and location privacy challenges in space networks. In *33rd USENIX Security Symposium (USENIX Security 24)*, pages 6093–6111, 2024.

[22] Wei Liu, Yuanjie Li, Hewu Li, Yimei Chen, Yufeng Wang, Jingyi Lan, Jianping Wu, Qian Wu, Jun Liu, and Zeqi Lai. The Dark Side of Scale: Insecurity of Direct-to-Cell Satellite Mega-Constellations. In *2024 IEEE Symposium on Security and Privacy (SP)*, pages 445–464. IEEE, 2024.

[23] Weisen Liu, Zeqi Lai, Qian Wu, Hewu Li, Yuxuan Weng, Wei Liu, Qi Zhang, Jihao Li, Yuanjie Li, and Jun Liu. Mind the location leakage in leo direct-to-cell satellite networks. In *2025 IEEE Symposium on Security and Privacy (SP)*, pages 1064–1080. IEEE, 2025.

[24] Microsoft Threat Intelligence. Peach Sandstorm password spray campaigns enable intelligence collection at high-value targets. [Online], 2023. https://www.microsoft.com/en-us/security/blog/2023/09/14/peach-sandstorm-password-spray-campaigns-enable-intelligence-collection-at-high-value-targets/.

[25] Sujay Narayana, R Venkatesha Prasad, and T Venkata Prabhakar. Sos: Isolated health monitoring

system to save our satellites. In *Proceedings of the 19th Annual International Conference on Mobile Systems, Applications, and Services (Mobisys)*, pages 283–295, 2021.

[26] Gabriele Oligeri, Savio Sciancalepore, and Roberto Di Pietro. Gnss spoofing detection via opportunistic iridium signals. In *Proceedings of the 13th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, pages 42–52, 2020.

[27] Gabriele Oligeri, Savio Sciancalepore, Simone Raponi, and Roberto Di Pietro. Past-ai: Physical-layer authentication of satellite transmitters via deep learning. *IEEE Transactions on Information Forensics and Security*, 18:274–289, 2022.

[28] James Pavur, Martin Strohmeier, Vincent Lenders, and Ivan Martinovic. QPEP: An Actionable Approach to Secure and Performant Broadband From Geostationary Orbit. In *2021 Network and Distributed System Security Symposium (NDSS)*, 2021.

[29] Jose Luis Castanon Remy, Ekzhin Ear, Caleb Chang, Antonia Feffer, and Shouhuai Xu. Sok: Space infrastructures vulnerabilities, attacks and defenses. In *2025 IEEE Symposium on Security and Privacy (SP)*, pages 1028–1046. IEEE, 2025.

[30] Edd Salkield, Marcell Szakály, Joshua Smailes, Sebastian Köhler, Simon Birnbach, Martin Strohmeier, and Ivan Martinovic. Satellite spoofing from a to z: On the requirements of satellite downlink overshadowing attacks. In *Proceedings of the 16th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, pages 341–352, 2023.

[31] Security.com Threat Intelligence Team. Thrip: Espionage Group Hits Satellite, Telecoms, and Defense Companies. [Online], 2018. https://www.security.com/threat-intelligence/thrip-hits-satellite-telecoms-defense-targets.

[32] Starlink. SpaceX Starlink. [Online], 2018. https://www.starlink.com/.

[33] Ahren Studer and Adrian Perrig. The coremelt attack. In *European Symposium on Research in Computer Security*, pages 37–52. Springer, 2009.

[34] The Business Research Company. Satellite Services Global Market Report. [online], 2025. https://www.thebusinessresearchcompany.com/report/satellite-services-global-market-report.

[35] Christopher Tibaldo, Harshad Sathaye, Giovanni Camurati, and Srdjan Capkun. Gnss-wasp: Gnss wide area spoofing. In *USENIX Security 2025*, 2025.

[36] Viasat Inc. KA-SAT Network cyber attack overview. [Online], 2022. https://www.viasat.com/perspectives/corporate/2022/ka-sat-network-cyber-attack-overview/.

[37] Yikun Wang, Hewu Li, Zeqi Lai, and Jihao Li. Starmaze: Ring-based attack in satellite internet constellations. In *2024 IEEE/ACM 32nd International Symposium on Quality of Service (IWQoS)*, pages 1–10. IEEE, 2024.

[38] Johannes Willbold, Tobias Cloosters, Simon Wörner, Felix Buchmann, Moritz Schloegel, Lucas Davi, and Thorsten Holz. Space radsim: Binary-agnostic fault injection to evaluate cosmic radiation impact on exploit mitigation techniques in space. In *2025 IEEE Symposium on Security and Privacy (SP)*, pages 1047–1063. IEEE, 2025.

[39] Johannes Willbold, Moritz Schloegel, Manuel Vögele, Maximilian Gerhardt, Thorsten Holz, and Ali Abbasi. Space odyssey: An experimental software security analysis of satellites. In *2023 IEEE Symposium on Security and Privacy (SP)*, pages 1–19. IEEE, 2023.

[40] Yaoying Zhang, Qian Wu, Zeqi Lai, Yangtao Deng, Hewu Li, Yuanjie Li, and Jun Liu. Energy drain attack in satellite internet constellations. In *2023 IEEE/ACM 31st International Symposium on Quality of Service (IWQoS)*, pages 1–10. IEEE, 2023.