International Journal of Computer Information Systems and Industrial Management Applications
ISSN 2150-7988 Volume 18(4s) 2026 pp. 394-402
https://doi.org/10.70917/ijcisim-2026-2524
Article

Analyzing the Security of Satellite-Based Internet Services

Vishakha Abhay Gaidhani[1], Archana Date[2], Arti Suryavanshi[3], Prashant Suryavanshi[4], Rahul Raut[5], Pratibha Gayke[6]

[1]Department of MBA, Sir Visvesvaraya Institute of Technology, Nashik, Maharashtra, India.
Email: vishakha.gaidhani@gmail.com
[2] Department of Electronics and Computer Engineering, HSBPVT's GOI Faculty of Engineering, Kashti – 414701, Ahilyanagar, Maharashtra, India.
Email: archanadate@gmail.com
ORCID: 0000-0001-9132-7946
[3] Department of Computer Engineering, HSBPVT's GOI Faculty of Engineering, Kashti – 414701, Ahilyanagar, Maharashtra, India.
Email: artips15@gmail.com
ORCID: 0009-0000-4703-8899
[4] Department of Computer Engineering, HSBPVT's Parikrama Polytechnic, Kashti – 414701, Ahilyanagar, Maharashtra, India.
Email: sprashant1234@gmail.com
ORCID: 0009-0000-3623-6726
[5] Department of Information Technology, Dr. Vithalrao Vikhe Patil College of Engineering (DVVP COE), Ahilyanagar – 414003, Maharashtra, India.
Email: raut_it@enggnagar.com
[6] Department of Information Technology, Dr. Vithalrao Vikhe Patil College of Engineering (DVVP COE), Ahilyanagar – 414003, Maharashtra, India.
Email: gayke_it@enggnagar.com
ORCID: 0009-0005-2008-5691

Abstract: — The introduction of satellite-based Internet services has already become an important part of the global connection, making it possible to obtain broadband in remote, rural, maritime, and after-disaster areas. New implementations of the large-scale low Earth orbit (LEO) constellation, as well as traditional medium Earth orbit (MEO) and geostationary Earth orbit (GEO) systems, have created much better coverage, capacity, and latency performance. Nevertheless, the peculiarities of satellite networks imply different security threats, which cannot be considered as the same ones as those of the Internet infrastructures on the ground. The paper reviews the security of satellite-based Internet services in terms of the architectural components and communication protocols, and operational restrictions. An in-depth threat model has been provided, including passive and active opponents in space, on the ground, and in the user segments. The major security issues are mentioned as being long distance wireless connections, high propagation delays, lack of sufficient on-board computational capabilities, and the extremely dynamic topology due to the movement of satellites. The paper also analyses the currently available cryptographic and authentication solutions applicable in satellite setups with particular focus on lightweight encryption, scalable key management, and strong access control protocols. This work by methodically studying the weaknesses and countermeasures indicates gaps in existing security designs and the differentiation of the adaptive, resource-conscious, and resilient security designs to suit the next generation satellite Internet systems. The results are to benefit the creation of secure satellite networking solutions that can provide reliable global connections.
Keywords: — Satellite Internet, Network Security, Threat Model, Lightweight Cryptography, Authentication Protocols

1. Introduction

Internet Internet services that are based on satellites have been receiving a new focus as a practical resolution to the problem of attaining global connectivity indeed. The satellite Internet systems are capable of delivering wide-area coverage over oceans, deserts, mountainous areas and any disaster-laden area as opposed to terrestrial networks which utilize dense infrastructure and are usually limited by geography. The development of satellite technology, reusable launch vehicles and mass-produced small satellites have increased the rate of large constellations, especially in low earth orbit (LEO) allowing lower latency and increased throughput than traditional geostationary earth orbit (GEO) systems. Consequently, satellite Internet is being considered an ever-growing part of the heterogeneous networks of the future, with its use in the remote education, telemedicine, emergency communications, Internet of Things (IoT), and military operations. Although these benefits are realized, security of Internet services over satellites is a primary issue of concern. The satellite networks run on long distance wireless connection which is more prone to eavesdropping, jamming, spoofing and manipulation of signals as compared to wired earth network [1]. In addition, the broadcasting feature of the satellite communication increases the surface of attack, which means that adversaries with rather limited resources can attack a relatively huge area. Such vulnerabilities are especially worrisome in the context of increased dependence on satellite Internet as a platform to provide important services because, in case of successful attacks, millions of customers may experience a loss of connectivity or sensitive information may be lost. Security design is also complicated by the fact that satellite Internet has architectural features that make it hard to ensure security. A satellite system comprises various segments, which are interconnected such as the space segment (satellites and inter-satellite links), the ground segment (gateways, network control centers) and user terminals [2]. All of these segments have different vulnerabilities and assumptions of trust. Besides this, the current satellite constellations have extremely dynamic topologies as the satellites move quickly, there are frequent handovers and changing routing paths. Figure 1 demonstrates built-in architecture, threats, challenges, and cryptographic schemes on satellite security. Such dynamics are problematic to older security systems that take a relatively stable network topology. The issue of resource constraints is also important in determining satellite security [3].

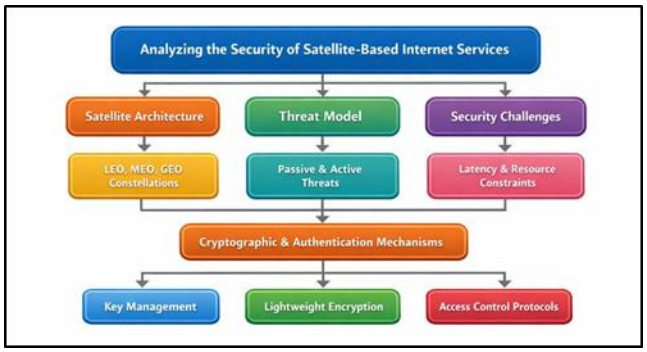

Fig.1. Illustrating the Security Analysis Framework for Satellite-Based Internet Services

Satellites particularly those in LEO constellation are constrained in onboard computational capability, energy supply, and storage. The deployment of robust cryptographic algorithms and complicated security measures should thus be well-balanced with the performance, latency and life-span issues. Additionally, propagation delays and intermittent connectivity could impede the timely authentication process, key dispensing and detection of intrusion [4]. It is against this background that there is an urgent need to have a rational examination of the security threats and defense mechanisms towards the Internet services that are based on satellites. To meet this requirement, the paper will discuss this underlying architecture, specifications of a detailed threat model, and the analysis of some of the main security issues specific to satellite environments [5]. It also goes through cryptography and authentication strategies that can be used in resource limited and extremely dynamic satellite networks. By identifying current solutions and unsolved research gaps, this paper seeks to make its contribution to the generation of resilient, scalable, and secure satellite Internet platforms that could be used to handle next-generation communication needs at a global level [6].

2. Related Work

The topic of security in satellite-based Internet services has been a long-standing research subject over the past decades, with some of the earliest documentations dedicated to the conventional geostationary satellites utilized in broadcasting and military communications. The first effort focused on link-layer encryption, anti-jamming methods, and physical-layer security to ensure that long-range satellite links are secure against eavesdropping and interference. These are the studies that have formed the basis of knowing the vulnerabilities that are inherent in wireless satellite channels, especially the vulnerabilities that are caused when the broadcast is open and when the coverage footprints

are large [7]. As the Internet based on broadband satellite services came up, scientists started looking at end-to-end security concerns, such as secure routing, authentication and key management. Some of them examined the suitability of traditional Internet security protocols in the satellite setting, and noted their shortcomings under high latency and interrupted connectivity [8]. These works established that mainstream systems used in terrestrial networks tend to experience undue delay in handshaking and signalling overheads when used in satellite networks. Even more recent studies have turned their attention to the so-called low Earth orbit (LEO) mega-constellations and their distinct security consequences. The effects that have been studied by scholars on the issue of secure routing and trust management include the effect of changing network topology, frequent handovers, and inter-satellite links. The solutions that have been proposed are hierarchical authentication modeling, pre-distributed key schemes and predictive handover based security schemes to minimize re-authentication latency [9]. Most of these designs however, presuppose safety to some extent of ground infrastructure or demand intricate coordination, which cannot scale effectively with thousands of satellites. The other critical body of research covers the lightweight cryptography and resource-conscious security protocols. Since there are limited computational and energy capabilities on satellites and user terminals, researchers have considered lightweight encryption algorithms and the use of elliptic-curve-based key exchange and streamlined authentication processes [10]. Although these techniques lower overhead, research reports the possibility of trade-offs between security level and long-term resistance against sophisticated attackers. New threats have also been highlighted as a result of survey, prior to which spoofing of the navigation signals, navigation control-channel attacks and cyber-physical attacks on satellite command and control have been highlighted. Despite the value these works bring in terms of threat taxonomies and countermeasure discussion, most of them do not have a holistic assessment of all segments of the satellite network. Table 1 is the comparison of current satellite Internet security strategies, effects, advantages and research trends. As a result, the lack of literature can be identified as a deficiency in integrated security models that can all be informative of the architectural diversity, adversary models, and operational constraints of next-generation satellite Internet services.

Table 1. Comparative Review of Related Work on Security of Satellite-Based Internet Services

Focus Area	Satellite Type	Threats Addressed	Impact	Benefits	Future Trend
Link-layer security	GEO	Eavesdropping, jamming	Improved data confidentiality	Simple integration	Adaptive PHY-layer security
Authentication schemes [11]	GEO/MEO	Spoofing, impersonation	Strong identity assurance	High security strength	Latency-aware authentication
Key management	GEO	Key compromise	Secure session establishment	Proven reliability	Decentralized key management
Secure routing [12]	LEO	Route hijacking, DoS	Enhanced routing resilience	Improved availability	AI-driven secure routing
Lightweight cryptography	LEO	Eavesdropping	Reduced computation cost	Energy efficiency	Post-quantum lightweight crypto
Physical-layer security	GEO/MEO	Jamming, interception	Improved signal robustness	Low protocol overhead	Intelligent anti-jamming

Control-channel protection [13]	GEO	Command injection	Safer satellite operations	High reliability	Autonomous control security
User terminal security	LEO	Device compromise	Improved endpoint security	Protects user data	Hardware-backed trust
Cross-layer security [14]	LEO/MEO	Multi-vector attacks	Holistic threat mitigation	Comprehensive protection	Cross-layer AI security
Survey / framework [15]	All	Multiple threats	Identified research gaps	Design guidance	Unified adaptive frameworks

3. Overview of Satellite-Based Internet Architecture

A. LEO, MEO, and GEO satellite constellations

Internet services that are offered by satellites are constructed on top of constellations that are placed in various orbits around the earth and they provide different performance and security features. The satellites in Geostationary Earth Orbit (GEO) are positioned at about 35,786 km of heights and are stationary with respect to the surface of the earth. Their extensive coverage allows them to serve globally or continental wide with only a few satellites meaning they are applicable in broadcasting and conventional broadband access. GEO systems, however, have high propagation delays usually over 500 ms round-trip time, which affects latency sensitive applications and makes real-time security systems difficult. MEO satellites exist in an altitude of between 2,000 km and 20,000 km, and are usually employed in navigation and the developing communications services. MEO constellations provide a compromise between latency and coverage, and they have less delay than GEO and less satellites than LEO systems. Security wise, MEO networks also have long-range link vulnerability and have less dynamic topology compared to LEO constellations. Low Earth Orbit (LEO) satellites are satellites that have been positioned at an altitude of less than 2000km to create mega-constellations comprising of hundreds or thousands of satellites. LEO systems have much lower latency, high throughput and the user experience is better. New security issues are however brought up by rapid movement of satellites, numerous handovers, and dynamic routing. These sizes and movement of LEO constellations increase the attacker surface, which requires extremely scalable, adaptive, and automated security responses throughout the network.

B. Space Segment, Ground Segment, and User Terminals

Satellite Internet architecture is usually categorized into three major parts which are space segment, ground segment, and user terminals. Commonly provided in space, the space segment will include satellites with communication payloads, onboard processors and in the more recent systems, inter-satellite links providing direct forwarding of data without necessarily requiring ground relay. These satellites have the obligation of transmitting, routing and occasionally the basic network management functions. The space segment is known to be especially susceptible to the risks of physical capture, signal interception, and attacks on control channels due to the lack of onboard resources, physical deployment remoteness. The ground segment comprises of gateway stations and network operation centers and control facilities which control the operation of satellites, routing of traffic and allocation of resources. Ground infrastructure is often used as the connection point between a satellite network and the terrestrial Internet, which is why it is an expensive target of cyberattacks. Attack on ground stations may cause massive disruption of services or unauthorized control of satellites, hence the need to ensure high perimeter and operational security. User terminals include fixed or mobile devices that include satellite modems, antennas and inbuilt user equipment.

C. Communication Protocols and Frequency Bands

Internet services provided by satellite are based on a stacked communications protocol and function on more than one frequency band to provide consistent connectivity. At the physical and link layer, satellite systems are typically operating on specialized modulation, coding and multiple access designs that are optimized on long-range wireless transmission. DVB-S2/S2X and proprietary waveform designs are common protocols used to increase spectral efficiency and interference resistance. These lower level technologies have the direct impact in affecting security in that they affect the ability to resist jamming, interception and manipulation of signals. IP-based communication is being increasingly supported in the network and transport layers by satellite Internet to ensure the compatibility with terrestrial networks. Figure 2 shows the protocols and frequency bands that form layers that support secure satellite Internet communication. Nevertheless, classical Internet protocols are not only unable to perform well in a satellite setting, as they are characterized by a high latency and loss of packets.

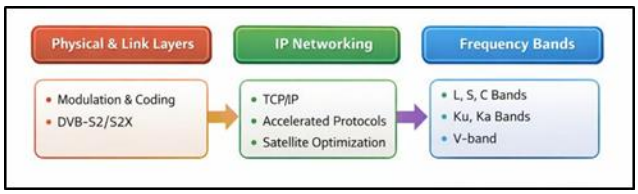

Fig.2. Illustrating Communication Protocols and Frequency Bands in Satellite-Based Internet Services

In response to this satellite-optimized variants and acceleration methods are also frequently considered, potentially adding more security concerns unless well thought out. Satellite systems are working on various frequencies bands such as L-band, S-band, C-band, Ku-band, Ka-band and developing V-band allocations.

4. Threat Model and Adversary Capabilities

A. Attack surfaces in satellite communication systems

The satellite communication system has a wide and heterogeneous attack surface because it has a distributed structure and depends on long-range wireless connections. The radio frequency (RF) communications channels, that are utilized in the uplink, downlink, and inter-satellite links are one of the main attack points. These media are open and broadcast-based in nature and hence prone to eavesdropping, jamming, replay attacks and signal spoofing. The enemies may use the loopholes in the modulation, coding or beamforming methods to interfere or alter data flow. The plane of satellite networks control and management is another attack surface which is critical. High-value targets would be telemetry, tracking, and command (TT&C) links that are used to control satellites because their integrity could be compromised to allow a rogue command injection, alteration of the orbit or even interference with the payload. These risks can be highly increased by vulnerabilities in authentication or key management mechanisms. Moreover, routing and handover protocols in dynamic constellations create software based attack surfaces such as manipulation of routing, denial-of-service, and exploitation of the protocol. Infrastructure Ground infrastructure increases the attack surface further.

B. Passive vs. Active Adversaries

The opponents of Internet services offered through satellites can be divided into two main groups: passive and active hackers, depending on whether they interfere with the communication system or not. Passive adversaries do not want to change the behavior of the system and just monitor and gather information. Passive attacks that are typical in satellite networks include stealing of uplink or downlink transmissions, traffic observation, and control or user data stealing. Passive attackers can be located in remote locations with relatively cheap equipment due to the larger range of coverage of satellite signals. Even though passive attack does not interfere with service, it is very dangerous to the confidentiality of information, privacy of users, and sensitive operational information. Active enemies, in turn, deliberately interfere or disrupt the work of satellites. These intruders can either inject some harmful signals, satirize the communication channels, spoof the valid satellites or gateways, or replay and man-in-the-middle attack. The active attacks may cause service interruptions, corruption of data, unauthorized access, and even loss of control of the satellites. In dynamic satellite constellations, active adversaries can also use regular handovers and routes update to initiate denial-of-service attacks or route hijacking attacks. The difference between passive and active adversaries the security design should take note of is that passive adversaries only need solid encryption and traffic security, whereas active adversaries need effective authentication, intrusion detection, and robust resilience systems. In reality, more advanced attackers can be using both options at the same time, initially surveying the system behavior before they make targeted active attacks to ensure they produce the greatest effect.

C. Space-Borne, Ground-Based, and User-Side Threats

The threats to the satellite Internet services may also be categorized depending on the place of origin, space-borne, ground-based, or user side. Space-borne threats are a result of the space segment and involve malicious or compromised satellites, hostile spaceships or debris-related interference. The signal interception, spoofing, or inter-satellite links interference are some of the methods the adversarial satellites can try. Even though this is technically difficult, they are dangerous because they are physical presence to the target system and they cannot intervene physically. One of the most feasible and common is the ground-based threats. These are jamming and spoofing attacks through ground transmitters, cyberattacks on ground stations and network operation centers and insider threats on satellite service providers. Physical attackers can use software vulnerabilities, misconfigurations, or supply-chain vulnerabilities to compromise unauthorized access or cause havoc to vast amounts of the network. Threats on the user side include hacked or rogue terminals of the user. The user equipment can be deployed in remote or unsecured locations, and therefore attackers can physically interfere with terminals, steal cryptographic keys, or pose as legitimate users. Damaged terminals may also serve as the point of entry of more extensive attacks, like distributed denial-of-service or unauthorized access to a network.

5. Security Challenges in Satellite Internet Services

A. Long-distance communication and latency constraints

The satellite Internet services include the long-distance communication, which is a characteristic feature, and which raises serious security concerns. The signals have to cover thousands of kilometers between satellites, ground stations, and user terminals and have a non-negligible propagation delay. In geostationary installations, the latency round trip may take many hundreds of milliseconds and even the constellation of low Earth orbit systems have their delay varying as they undergo frequent handovers and multi-hop routes. The mentioned latency properties have a direct influence on the design and performance of security protocols that are based on the timely exchange of messages. Figure 3 shows propagation delays and latency impacts on satellite Internet security. Most traditional security systems including multi-round authentication handshakes, certificate validation and regular key renegotiation are inefficient or unfeasible in a high-latency environment. Unreasonable signaling overhead would diminish the user experience and make them more vulnerable to denial-of-service attacks. Moreover, this is complicated by delayed feedback that hinders real-time intrusion detection, attack mitigation and fast reaction to security incidents. Opponents can use time windows due to latency to retransmit messages, destabilize protocols or monopolize system resources.

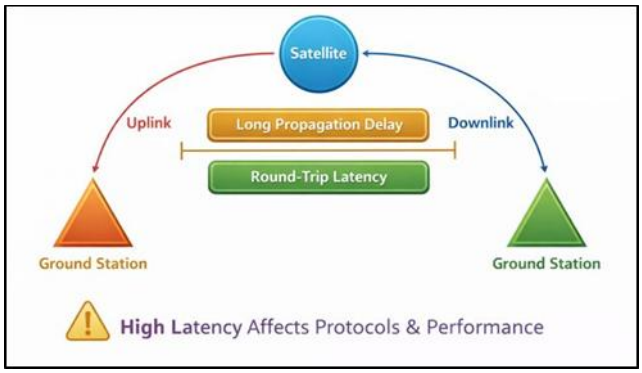

Fig.3. Illustrating Long-Distance Communication and Latency Constraints in Satellite Internet Services

The long distance wireless also becomes more prone to signal attenuation, interference, and effects on the environment that leads to increased packet loss and retransmission. Security measures should hence be hardened against distrustful channels but the integrity and confidentiality ensures should be maintained.

B. Limited Onboard Computational Resources

There are very strong limits on the amount of computational power, energy supply, memory, and hardware complexity in satellites, especially in satellites in constellations of low Earth orbit. These constraints have a great effect on the possibility of implementing sophisticated security systems. Intensive cryptographic algorithm, regular exchange of keys, and multifaceted intrusion detection systems may create substantial processing and energy overheads, which may cut down the lifetime of the satellites or worsen communication capabilities. Satellites do not like terrestrial servers that can be easily upgraded and repaired once deployed. Therefore, security measures need to

be light, strong, and have a high resistance to long-term threats. Public-key cryptography that is resource intensive or constant monitoring may not be feasible to implement on an onboard system and is particularly not feasible in small satellites with low payload capacity. The limitation gives rise to a trade-off between the level of security and the level of operational efficiency, whereby a designer will be compelled to choose carefully algorithms and protocol parameters. Secure key storage and management is also influenced by limited resources. It is difficult to ensure that cryptographic keys cannot be extracted or compromised in the case of limited or missing hardware security modules. Also, the onboard software should be extremely optimized and able to withstand failures because even the software vulnerabilities can be used remotely with possibly irreparable effects. To overcome these weaknesses, studies have revolved around lightweight cryptographic primitives, hardware-aided security and offloading some security capabilities to ground stations. Nevertheless, overreliance on ground infrastructure creates further dependency of trust and latency. One of the core problems of satellite Internet services is to acquire a high level of autonomous security with a stringent resource base.

C. Dynamic Topology and Satellite Mobility

One characteristic of the current satellite Internet systems, especially those that rely on the constellations of low Earth orbit, is dynamic topology. Satellites are traveling at high velocities in comparison to the surface of the earth and this implies that the network connectivity, paths of the routing, and link availability changes frequently. Connections between satellites are swapped over by user terminals thus, inter-satellite connections are constantly built and dismantled. This great level of mobility makes it difficult to have stable security associations. Conventional security controls normally presuppose fairly fixed network arrangements and persistent connections. Satellite networks, on the other hand, need a fast authentication system, automatic updating keys and handover systems that are secure to avoid service interruption. Re-authentication can also be a burden on signaling and latency, and improperly considered handover processes can suffer from temporary vulnerabilities, which can be used by the attacker to perform spoofing or session hijacking. Access control and trust management is also problematic by dynamic topology. The satellites might deal with a vast and dynamic group of peers, so the reliability of relationships between the satellites and their policies to grant authorization cannot be always maintained. The issue of routing security is also complicated since the enemy can also seek to corrupt dynamic routing data in order to reroute or discard traffic. Also, mobility makes both monitoring and incident response challenging as the location and connectivity of affected components continually change. Such an environment warrants adaptive, automated and predictive security mechanisms that are capable of functioning efficiently even when the environment is on a continuous motion. The next-generation satellite Internet services are challenged with designing scalable security frameworks that should be able to support dynamic topology without any harm to performance and robustness.

6. Cryptographic and Authentication Mechanisms

A. Key management in satellite networks

Cryptographic keys and cryptographic keys: Key management is one of the essential elements of secure satellite Internet services because confidentiality, integrity and authentication depend on the use of cryptographic keys on any communication connections. The long communication delays, intermittent connectivity and large-scale and distributed architecture of a satellite network make key management complicated. The conventional key distribution methods are typically ineffective because most traditional methods of key distribution may be centralized encountering latency and single points of failures due to constant interaction with ground authorities. Satellite networks are known to deal with such challenges by using pre-distributed keys, hierarchical key management or hybrid implementations combining onboard storage with periodical updates on the ground. By loading cryptographic content before the booting, autonomy of operation is possible, but the absence of flexibility and difficulty of key revocation in the event of compromise. Hierarchical designs, where master keys are administered by trusted ground stations and session keys are locally generated, are more scalable at the cost of depending more on secure ground infrastructure. The use of dynamic constellations also complicates key management because the regular handovers will necessitate the creation of secure connections between satellites and user terminals very fast. Key refresh and rekeying mechanisms should be efficient to ensure that the signaling overhead is minimized and the security is also guaranteed. Moreover, safe storage of keys as well as safekeeping of keys on satellites and user devices is also a burning issue, especially in the context of physical access risk and insufficient hardware security features. New studies are being done to understand distributed and decentralized key management methods, such as group keying and blockchain-inspired, to achieve a higher degree of resilience and scalability. Nevertheless, the issue of striking a balance between autonomy, efficiency, and security in the major management is yet to be solved in satellite Internet systems.

B. Lightweight Encryption for Spaceborne Systems

Because of high limitations on the power of computations, power, and memory. Small LEO satellites (and satellites in general) are not capable of running any heavyweight cryptographic algorithm without affecting the performance of the mission and the working life. Consequently, security designers have to choose encryption schemes that offer sufficient security and also incur the least processing and energy cost. Symmetric-key cryptography is very popular in satellite environment due to its efficiency over the public-key methods. Light block ciphers and stream ciphers are widely used in order to encrypt and decrypt data and regulate streams. These algorithms not only make the computation complexities less, but also allow real time encryption without using too much latency. Nevertheless, the use of symmetric encryption raises the significance of the safe distribution and control of keys. Public-key cryptography is frequently restricted to infrequent operations (such as initial authentication or key establishment), and in some cases is based on elliptic-curve cryptographic schemes, which have a high level of security with smaller key sizes. Efficiency may also be further enhanced by hardware-aided encryption such as radiation-hardened cryptographic accelerators, which are more expensive and complex to design. Lightweight encryption will enhance performance although it can decrease the resistance to future cryptanalytic improvements unless carefully chosen. Long-range missions require algorithms that have adequate security margins. Continuous analysis and standardization of lightweight cryptography primitives is therefore important to provide long-term confidentiality and integrity to satellite Internet services.

C. Authentication and Access Control Protocols

Authentication and access control mechanisms also make sure that only the legitimate entities will access satellite Internet services and network resources. These mechanisms have to be efficient in the context of satellite environments, which has a high latency, intermittent connectivity, and frequent mobility. Conventional multi-step authentication schemes implemented in earth-based networks may add too much delay and overhead to signalling in the case of a satellite connection. To address these problems, satellite systems typically reduce the authentication schemes to a simplified version that has fewer rounds of a handshake and allows rapid re-authentication in case of handovers. To avoid the spoofing and impersonation attacks, mutual authentication of the satellites, ground stations, and the user terminals are necessary. Authentication is also typically enhanced with pre-established trust relationship and credential caching in order to prevent loss of security. The policies should also be able to support dynamic topology and users in large numbers. Attributes or role-based access control models are becoming more and more popular to facilitate scalable and flexible authorization decisions. Nevertheless, the problem of imposing access control on satellites at the fine grains is difficult because of the lack of resources and the necessity to make quick decisions. The other most important issue is secure authentication of the control and management channels because the failure of the links can have disastrous outcomes. It is also essential to protect command and control activities by means of strong authentication with support of integrity protection and anomaly detection.

7. Conclusion

Internet services provided by satellites are quickly becoming part of the global communication system, providing ubiquitous connectivity in remote and underserved locations as well as mission-critical and remote settings. The shift of the conventional geostationary systems to the dynamic low earth orbit and hybrid constellations has greatly enhanced the Latency, throughput and coverage however, complex security issues arise which are fundamentally different than those of terrestrial networks. This paper has examined the security of satellite Internet services in terms of architectural elements, threat model and operational limitations. As noted in the discussion, satellite networks are vulnerable to a broad spectrum of threats by definition owing to their broadcast wireless networks, extensive coverage, and distributed network across space, earth, and user space. The distance of communication and the latency restriction restrict the efficiency of the traditional security measures, the limited onboard processing resources require lightweight but physically resistant cryptographic algorithms. Moreover, the topology which is highly dynamic due to the mobility of satellites makes it difficult to perform authentication, key management as well as establishing trust, which can be exploited during handovers and routing information updates. In the analysis of cryptographic and authentication schemes, it was noted that scalability of key management, resource efficient encryption and intelligent access control depending on resource limited and mobile satellite situations are important. Although there are solutions that can be utilized to deal with certain elements of satellite security, none of them can effectively deal with the complex issues of latency, mobility, scalability, and long-term resilience. This shows a serious gap in the existing research and practice.

References

1. Kang, M.; Park, S.; Lee, Y. A Survey on Satellite Communication System Security. Sensors 2024, 24, 2897.
2. Zhang, L.; Wu, S.; Lv, X.; Jiao, J. A Two-Step Handover Strategy for GEO/LEO Heterogeneous Satellite Networks Based on Multi-Attribute Decision Making. Electronics 2022, 11, 795.
3. Li, G.; Li, T.; Yue, X.; Hou, T.; Dai, B. High Reliable Uplink Transmission Methods in GEO–LEO Heterogeneous Satellite Network. Appl. Sci. 2023, 13, 8611.
4. Lv, W.; Yang, P.; Ding, Y.; Wang, Z.; Lin, C.; Wang, Q. Energy-Efficient and QoS-Aware Computation Offloading in GEO/LEO Hybrid Satellite Networks. Remote. Sens. 2023, 15, 3299.
5. Kapsis, T.T.; Lyras, N.K.; Panagopoulos, A.D. Optimal Power Allocation in Optical GEO Satellite Downlinks Using Model-Free Deep Learning Algorithms. Electronics 2024, 13, 647.
6. Choi, H.; Pack, S. Cooperative Downloading for LEO Satellite Networks: A DRL-Based Approach. Sensors 2022, 22, 6853.
7. Xia, L.; Lin, B.; Zhao, S.; Zhao, Y. A Centralized–Distributed Joint Routing Algorithm for LEO Satellite Constellations Based on Multi-Agent Reinforcement Learning. Appl. Sci. 2025, 15, 4664.
8. Shi, Y.; Wang, W.; Zhu, X.; Zhu, H. Low Earth Orbit Satellite Network Routing Algorithm Based on Graph Neural Networks and Deep Q-Network. Appl. Sci. 2024, 14, 3840.
9. Tirmizi, S.B.R.; Chen, Y.; Lakshminarayana, S.; Feng, W.; Khuwaja, A.A. Hybrid Satellite–Terrestrial Networks toward 6G: Key Technologies and Open Issues. Sensors 2022, 22, 8544.
10. Diro, A.; Kaisar, S.; Vasilakos, A.V.; Anwar, A.; Nasirian, A.; Olani, G. Anomaly detection for space information networks: A survey of challenges, techniques, and future directions. Comput. Secur. 2024, 139, 103705.
11. Wang, Z.; Cao, J.; Di, X. Anomaly detection method for satellite networks based on genetic optimization federated learning. Expert Syst. Appl. 2025, 295, 128627.
12. Driouch, O.; Bah, S.; Guennoun, Z. CANSat-IDS: An adaptive distributed Intrusion Detection System for satellites, based on combined classification of CAN traffic. Comput. Secur. 2024, 146, 104033.
13. Le, H.D.; Park, M. Enhancing Multi-Class Attack Detection in Graph Neural Network through Feature Rearrangement. Electronics 2024, 13, 2404.
14. 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.
15. Q. Naaz, M. R. Beg, H. R. Khan, and H. U. Rahman, “ExecuChat: A Secure AI-Integrated Web-Based Chat Application with Code Debugging and Execution”, Int Journal Adv Comp Theory Engg, vol. 14, no. 1, pp. 214–218, May 2025.