2025 IEEE/CIC International Conference on Communications in China (ICCC Workshops) | 978-1-6654-7801-4/25/$31.00 ©2025 IEEE | DOI: 10.1109/ICCCWorkshops67136.2025.11148232

Towards a Security Architecture for Satellite Internet: A Standardization Perspective

Jun Liu[1,2], Jiejie Zhao[2], Yue Chen[3], Hewu Li[1,2], Qian Wu[1,2], YuanJie Li[1,2], Han Qiu[1,2], Zeqi Lai[1,2]
[1]Institute for Network Sciences and Cyberspace, Tsinghua University
[2]*Zhongguancun Laboratory*
[3]CNCERT/CC

Abstract—**In the 6G era of striving for global connectivity, Satellite Internet emerges as a crucial infrastructure by providing network coverage to remote and underserved regions. However, it confronts more intricate security threats than terrestrial networks, encompassing dual perils from the physical and network realms. This paper reviews the classic architectures of Satellite Internet and dissects the novel security challenges it encounters, such as the harsh space environment, orbit and spectrum congestion, and the resource disparity between satellites and terrestrial nodes. It further scrutinizes the existing cybersecurity regulations and standards, highlighting their inadequacies in tackling these emerging threats. Against this backdrop, the paper proposes a new security architecture standard for Satellite Internet, which encompasses physical environment domain, electromagnetic domain, control domain, and forwarding domain security. Finally, the paper outlines the future trend of standardization efforts for Satellite Internet, underlining the necessity of bolstering active security technologies to counteract unknown intelligent security risks.**

Keywords—Satellite Internet, Standardization, Security Architecture

I. INTRODUCTION

Terrestrial wireless networks indeed made remarkable progress in enhancing communication speeds and quality of service. However, they still face significant challenges in providing coverage to remote or underserved areas, which hinders the achievement of 6G era's goal of connecting everyone and everything. Satellite Internet [1], with their inherent wide-area coverage capabilities, offer a direct solution to this coverage gap. Recently, various Satellite Internet mega-constellation projects have been established using Low Earth Orbit (LEO) satellites, such as SpaceX's Starlink[2], OneWeb[3], Amazon's Kuiper[4], and Telesat[5]. These launched constellations are extending the boundary of today's Internet to construct an integrated space-terrestrial network. Equipped with high-speed inter-satellite links (ISLs)[6] and ground-satellite links (GSLs)[7], they can interconnect with other satellites and terrestrial facilities for providing planet-wide Internet service.

Satellite Internet can boost the potential of a wide range of applications[8]. For example: LEO Satellite-Assisted Computing: Provides computing services in remote areas. Intelligently Connected Vehicle Networks: Offers high-precision positioning and navigation for traffic management. Smart City, Agriculture, and Healthcare: Supports infrastructure monitoring, city planning, weather forecasting, and environmental surveillance. Emergency and Rescue Operations: Acts as a last-resort communication tool in hard-to-reach regions. IoT and M2M Communications: Facilitates access, forwarding, and edge computing for IIoT devices. Hence, the value and impact of Satellite Internet on economic growth and technological advancement are anticipated to be immense and far-reaching. In April 2020, Satellite Internet, as a representative of communication network infrastructure, was included in the category of new infrastructure information infrastructure for the first time. This marked the elevation of Satellite Internet construction to a national strategic project and a key high ground in the international space race.

Compared to terrestrial networks, Satellite Internet faces more severe security risks, due to the following inherent limitations: **Complex Surrounding Environment**: Satellites operate in harsh space conditions, where cosmic radiation may impair the electronic devices on board. **Asymmetric Capabilities between Space and Terrestrial Segments**: The LEO satellites have limited power, storage capacity, and computation capabilities. As a result, they are unable to implement complex encryption algorithms to protect themselves. **Inherent Defensive Disadvantages**: Satellites cannot be easily upgraded post-launch. This makes traditional patch-based security measures ineffective against evolving cyber threats. **High Dynamic Changes in Space and Time**: The high mobility and limited access time of LEO satellites further complicate security management. These constraints leave Satellite Internet more vulnerable to cyber threats than terrestrial networks. Therefore, the new security architecture for Satellite Internet is needed rather than reactive fixes.

To this end, in this work, we aim to introduce a new security architecture for Satellite Internet from a standardization perspective. Specifically, we begin by reviewing the classic architectures of Satellite Internet, highlighting different implementation paradigms in its development. Next, we analyze the new security threats facing Satellite Internet, considering security threats from the physical and network perspectives. We then examine existing cybersecurity regulations and standards for Satellite Internet, identifying gaps in current standards in responding to these threats. Based on this analysis, we propose a new security architecture standard for Satellite Internet, incorporating advanced solutions to address the identified threats. Finally, we discuss prospective standardization efforts on Satellite Internet needed to enhance its resilience and security.

II. A TAXONOMY OF SATELLITE INTERNET ARCHITECTURE

The classic architectures of Satellite Internet includes four type. Here, we introduces these Satellite Internet architectures, providing specific scenarios for analyzing its security risks.

A. One-to-One

The One-to-One architecture relies on Geostationary Orbit (GSO) satellites and ground stations. GSO satellites are positioned about 35,786 kilometers above Earth to achieve wide coverage. These satellites maintain a relatively station-

978-1-6654-7801-4/25/$31.00 ©2025 IEEE

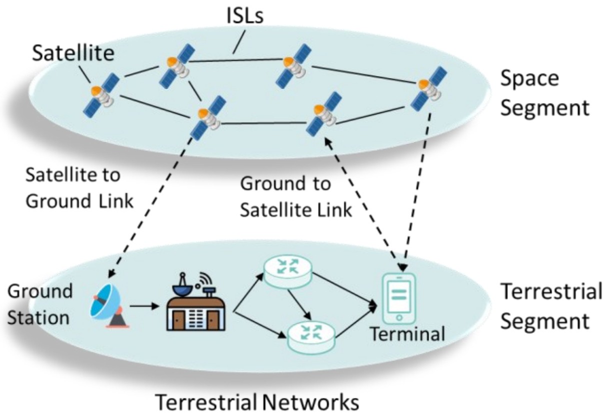

Figure 1. The architecture of Integrated Satellite-Terrestrial Networks.

ary position relative to the ground and communicate directly with ground stations via feeder beams. Each satellite provides physical connections to users within its coverage range through user beams. Importantly, at any given time, one GSO satellite can only connect to one ground station. Therefore, GSO satellites send user data to the corresponding ground station, which then handles further processing and delivery.

B. *One-to-Many*

Compared to the "*One-to-One*" architecture, this architecture uses multiple Non-Geostationary Orbit (NGSO) satellites to provide faster broadband services than a GSO satellite. Thus, this architecture requires more NGSO satellites for global coverage due to their limited coverage area. Additionally, since NGSO satellites move quickly relative to the ground, they necessitate continuous switching between the ground station and feeder beams to maintain network service. Specifically, user service areas are divided based on ground station locations. NGSO satellites first route data to the corresponding ground stations and then leverage terrestrial networks to route data to users. Thus, the terrestrial network enables NGSO satellites to connect to many ground stations at a given time.

C. *Many-to-Many*

In scenarios where ground stations cannot be established outside national territory, the network connections between satellites should be built using ISLs to expand the satellites' service coverage. In "*Many-to-Many*" architecture, different network protocols are used between satellite networks and terrestrial networks. Under this architecture, a single NGSO satellite provides services to users within its limited coverage range. If no ground station is available within its coverage, the satellite transmits user data to a remote ground station via ISLs. If a ground station is available, data is landed locally to conserve ISLs resources. This architecture enables NGSO satellites to maintain connectivity with multiple ground stations simultaneously through a combination of ISLs and terrestrial networks.

D. *Integrated Satellite-Terrestrial Networks*

In contrast to "*Many-to-Many*" where satellite networks and terrestrial internet have long developed separately and independently, "integrated satellite-terrestrial networks" aim to unify satellite and terrestrial network protocols, as shown in Figure 1. This unification allows satellites and terrestrial nodes to become routing peers, facilitating agile network expansion. However, this integration is challenging and is currently in the stage of in-depth technical evaluation by satellite operators.

III. Security Threats Faced by Satellite Internet

Unlike the Terrestrial Internet, Satellite Internet is exposed to a complex, harsh, and uncontrolled space environment. As a result, it faces dual security threats from both the physical and network perspectives. Thus, this section analyzes the new security risks faced by Satellite Internet from the physical and network perspectives.

A. *Security Threats in a Physical Perspective*

1) Dynamic Topology Due to High Mobility

Satellite Internet is established through the interconnection of satellites positioned in various high, Medium and low earth orbits, as well as terrestrial nodes. Unlike Terrestrial Internet, the high-speed movement of satellites results in a highly dynamic network topology, which often goes beyond the control range. This leads to more fragile network links and nodes. Once the satellites move out of the control area, it becomes extremely challenging to effectively detect and prevent globalized, diversified, and intelligent attacks.

2) Orbital Congestion and Spectrum Interference

Nowadays, the low earth orbits where LEO satellites operate are exceptionally crowded. Specifically, these orbits are currently occupied by over 8,300 satellites and more than 27,000 pieces of space debris. These satellites and space fragments travel at speeds of up to 15,700 miles per hour and have diameters of 10 centimeters or larger. Given that the satellites are from different countries and organizations, and it is difficult to effectively collaborate, collisions in space are highly likely to occur.

Once a collision happens, a satellite will disintegrate into hundreds or even thousands of pieces of space debris, further increasing the risk of space collisions (this is known as the "Kessler Syndrome"). Meanwhile, as satellite communication spectrum resources are scarce, the sharp increase in the number of satellites in orbit leads to a dramatic rise in inter-satellite communication interference. Therefore, Satellite Internet faces extremely serious security threats such as physical destruction and electromagnetic interference.

3) Challenges of the Harsh Space Environment

The complex and harsh space environment constantly threatens the reliability of satellite applications in orbit. The in-orbit satellites are surrounded by cosmic rays, solar radiation, and high-energy charged particles. Without the protection of the Earth's atmospheric barrier, these particle irradiations can cause permanent and temporary damage to the electronic components of satellite payloads, especially commercial semiconductor devices (such as memory bit flip errors). If not corrected in time, it will not only damage the devices but also cause most orbital applications to fail, thereby affecting the normal operation of satellites.

4) Asymmetric Capabilities between Space and Terrestrial Segments

The essence of security lies in the game between attack and defense, and the essence of this game is the contest of capabilities between the two sides. Satellites, with their limited resources and inability to upgrade once in orbit, fall behind terrestrial nodes in computing, storage, and networking over their 5-10 year lifespan. This produces an asymmetry in the attack and defense capabilities between space and terrestrial segment, making traditional "patching"-style passive defense inadequate to effectively address the globalized, diversified, and intelligent security risks of Satellite Internet. As a result, a situation of "easy to attack but difficult to defend" emerges.

B. *Security Threats in a Network Perspective*

1) Security Risks of Open Interconnection

To enhance socio-economic benefits, Satellite Internet will inevitably shift from proprietary network communication protocols to open ones, ultimately establishing an open and interconnected satellite-terrestrial integrated networks. However, this transition will expand its attack surface and spread the vulnerabilities and weakness of open network communication protocols to satellites, thereby posing significant security threats to Satellite Internet. Since satellite are always in an open state, data transmission is at risk of unauthorized access and eavesdropping, with the potential for data to be hijacked or tampered with. Therefore, ensuring the security of node access and the security of transmitted data is particularly crucial for the security of the Satellite Internet.

2) Security Challenges of Heterogeneous Protocols

The integration of satellite-terrestrial heterogeneous networks has led to a more complex network architecture and more dynamic connections. Historically, satellites and terrestrial networks have been isolated and heterogeneous, and are incompatible with each other. After integration, frequent interactions across protocol layers, network domains, and heterogeneous systems occur among nodes such as satellites, ground stations, terrestrial routers, and cloud services. This results in an expanded attack surface and a significant increase in new zero-day vulnerabilities. Moreover, due to their independent evolution, integrated satellite-terrestrial networks and terminals have a weak basis for mutual trust, making it difficult to collaboratively defend against security risks.

3) Expanded Security Risks from Diverse Services

As satellite communication, navigation, remote sensing, and computing capabilities continue to improve, Satellite Internet will serve as a satellite-terrestrial integrated infrastructure, potentially providing diverse information services such as communication, navigation, and remote sensing to users in space-based, airborne, land-based, and maritime platforms. This leads to an expansion of Satellite Internet security from traditional cybersecurity to an integrated security of communication, navigation, remote sensing, computing, and data, further expanding the attack surface and making the security situation more severe.

4) Security Implications of On-Board AI

As the number of satellites increases and hardware capabilities improve, the volume of on-board data is growing much faster than the data transmission capabilities between satellites and the terrestrial infrastructures. To address this, satellite edge computing has been proposed. It leverages the computing platforms of satellite payloads to process on-board data, thereby reducing transmission demands or running tasks directly on the satellite. With AI on-board, satellite payloads now serve as new computing power leasing platforms. This shift extends the attack surface to computing power, making it harder to monitor and detect unauthorized users who launch on-board side-channel attacks by using the on-board computing resources in uncontrolled areas.

IV. Cybersecurity Regulations and Standards for Satellite Internet

A. *International Cybersecurity Regulations*

From an international perspective, the United States, as a representative country, has been committed to accelerating the layout of Satellite Internet cybersecurity strategy, to grasp the initiative in space security.

- In September 2020, the **Fifth Space Policy Directive** explicitly required the integration of cybersecurity into the entire life cycle of satellite network development to enhance the cybersecurity of space systems.
- In April 2022, the U.S. Congress passed the **Satellite Cybersecurity Act**, which required the formulation of cybersecurity recommendations for U.S. satellite operators and the provision of resources to them to address the cybersecurity and threats of commercial satellite systems.
- In March 2023, the U.S. National Science and Technology Council released the **National Low Earth Orbit Research and Development Strategy**, proposing the establishment of a Low Earth orbit national laboratory by the U.S. National Aeronautics and Space Administration (NASA) to strengthen several cutting-edge research areas, including satellite cybersecurity.
- In April 2023, the U.S. Cyberspace Solarium Commission recommended that the Department of Homeland Security designate space systems as critical infrastructure to reduce satellite cybersecurity vulnerabilities.
- In May 2023, the U.S. Department of State, in its **Framework for Space Diplomacy Strategy** document, proposed the continuous strengthening of space cybersecurity and information and communication technologies, represented by Satellite Internet, and the enhancement of the security and resilience of critical infrastructure related to space.
- In November 2023, the U.S. Department of Defense announced that it was developing its first **Department of Defense Commercial Space Integration Strategy** to promote the integration of commercial technologies and ensure viable commercial space solutions during competition, crisis, and conflict.

B. *International Standardization Development*

1) International Standardization Development

- NIST: The US National Institute of Standards and Technology (NIST) has released four satellite cybersecurity risk management guidance frameworks to help commercial satellite operators identify cybersecurity risks in space, ground, user segments and hybrid satellite networks[9]. Commercial satellite-related entities should refer to a set of standards to incorporate cybersecurity risk management into their overall risk management plans.
- CCSDS: The Consultative Committee for Space Data Systems (CCSDS) aims to develop communication

protocols and data processing standards for space telemetry and data transmission systems[10]. It categorizes security threats into active (e.g., jamming) and passive (e.g., eavesdropping)[11]. In 2003, it formed the Security Working Group (SEC-WG) to provide security recommendations and solutions, develop security mechanisms and policies, and guide other working groups on security considerations. This group has produced standards and guidelines on space security architecture, threat documentation, security protocols, key management, and encryption/ authenticication algorithms.

- ITU: ①The ITU-R's WP4B working group focuses on satellite network standards, covering FSS, BSS, and MSS systems' air interfaces, performance, and applications. In 2010, it initiated research on the integration of satellites with IMT-Advanced, completing a report on visions and requirements in 2012. The ITU-R M.2083 recommendation highlighted the need for anytime, anywhere service access, leading to the development of the ITU-R M.[NGAT_SAT][12] standard for 5G satellite networks, which was completed in March 2018 and defined key aspects like applications, network structure, and technologies. ②ITU-T SG13 has also taken the lead in proposing the technical concept and standard system of fixed, mobile, and satellite convergence (FMSC), which is the world's first series of international standards for integrated satellite-terrestrial networks. At the ITU-T SG13 plenary meeting, China Mobile led the completion of three standardization projects, further improving the FMSC standard system and evolving the topic group into "IMT-2030 Network: Fixed, Mobile and Satellite Convergence" in the new research period[13].
- 3GPP/ETSI: 3GPP has been working to adapt 5G NR, NB-IoT, and LTE-M to meet satellite communication needs. Releases R15 to R18 progressively address satellite-5G integration, from basic requirements to detailed solutions for network architecture, protocol stacks, and functional requirements for different network components[14]-[17].

2) Development of International Standardization

- CCSA TC12[18]: In 2020, CCSA established TC12 to focus on space communication standards and research. Over three years, TC12 has worked on standards for VSAT, mobile satellite protocols, airborne communications, IoT, integrated 5G networks, GEO, and BeiDou short messaging. It has also explored topics like ATG, DVB-S2X, 5G enhancements, bearer networks, and applications. As Satellite Internet and smartphone-to-satellite links gain attention, various channels are actively involved in satellite communication standard-setting and research[19]-[22].
- TC425[23]: TC425 is guided by the Standardization Administration of China. It focuses on national standards for space product design, production, integration, testing, satellite applications, project management, materials, processes, data and information transmission. TC425 develops China's standard system and roadmap for space data and information transmission, including Satellite Internet, and drafts relevant white papers. It has six subgroups covering space environment, electronics, data transmission, assembly and testing, debris, and materials [24]-[26].

China's satellite internet market is growing rapidly with increased cybersecurity focus, but legislation and standardization lag. As critical infrastructure with broader coverage than terrestrial networks, its security impacts are greater. China faces two gaps: no dedicated satellite cybersecurity laws and inadequate standards—many outdated and incompatible with new technologies and threats. Cybersecurity and satellite experts must collaborate urgently to build a comprehensive security framework.

V. New Security Architecture for Satellite Internet

A. Design Principles

1）Openness

The security architecture should be easily accessible, and its licensing should be reasonable and non-discriminatory. The use of proprietary technologies is not excluded, but the open standards and protocols, open security tools and frameworks, and general security technologies (e.g., encryption algorithms) that are used should be provided in a non-restrictive manner.

2）Scalability

The architecture should be scalable and evolvable to allow for the incorporation of new security measures, such as those needed to address new threats or mission requirements. It is desirable to permit remote upgrades of deployed systems.

3）Flexibility

The architecture should allow for the development of different security systems that will be suitable for most satellite missions. The use of the security architecture should permit mission-specific configurations to ensure compatibility with each other.

4）Domain Separation

Security is achieved through domain separation mechanisms. The use of multi-domain security enhances the overall system security, with all domains forming an integrated whole that does not expose the system to the risk of compromise.

5）Fault Tolerance

Security mechanisms should be able to recover from failures. Recovery mechanisms should not expose vulnerabilities in the system. However, special cases may indicate the need to degrade security mechanisms, such as recovering by entering a predefined safe state to perform tasks. These cases should be identified and evaluated as part of the mission recovery design.

B. Security Requirements in Satellite Internet

1）Physical Environment Security Requirements

These include the physical environment security requirements for the space segment (satellites) and terrestrial segment (terrestrial information systems, RF antennas, etc.).

2）Communication Network Security Requirements

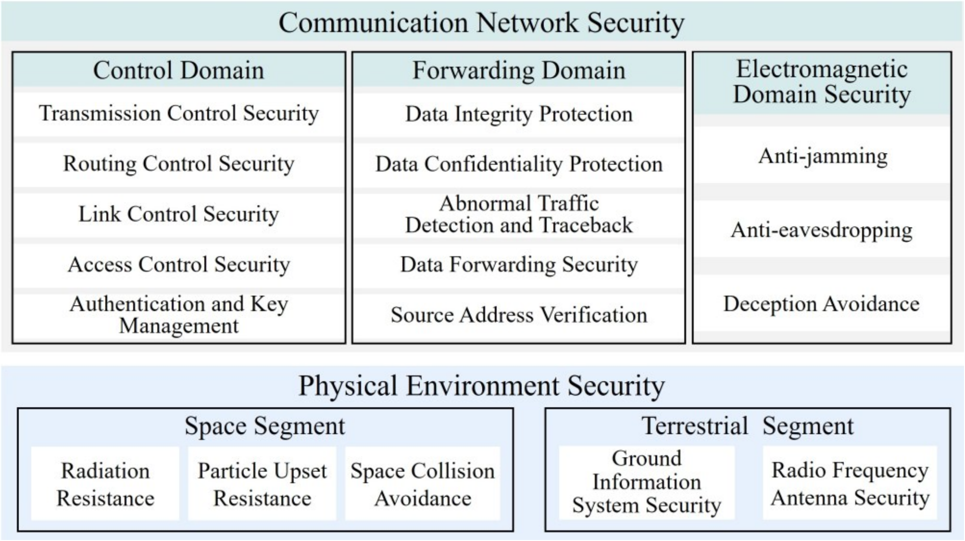
Communication Network Security
Control Domain
Transmission Control Security
Routing Control Security
Link Control Security
Access Control Security
Authentication and Key Management
Forwarding Domain
Data Integrity Protection
Data Confidentiality Protection
Abnormal Traffic Detection and Traceback
Data Forwarding Security
Source Address Verification
Electromagnetic Domain Security
Anti-jamming
Anti-eavesdropping
Deception Avoidance
Physical Environment Security
Space Segment
Radiation Resistance
Particle Upset Resistance
Space Collision Avoidance
Terrestrial Segment
Ground Information System Security
Radio Frequency Antenna Security

Figure 2. The framework of designed new security architecture of Satellite Internet.

These include security requirements in electromagnetic, control, and forwarding domains. Specifically:

- *Electromagnetic Domain Security Considerations*: These mainly involve ISLs, feeder circuits between satellites and ground stations, and user links between satellites and ground stations.
- *Control Domain Security Considerations*: These mainly involve the control functions of terrestrial networks and satellite networks with onboard processing capabilities.
- *Forwarding Domain Security Considerations*: These mainly involve the data forwarding functions of terrestrial networks and satellite network with onboard processing capabilities.

C. New Security Architecture of Satellite Internet

The security architecture of the Satellite Internet is shown in Figure 2 and is divided into physical environment security, and communication network security. Among them, physical environment security is divided into space segment and terrestrial segment physical environment security, and communication network security includes electromagnetic domain, control domain, and forwarding domain security.

1) Physical Environment Security

The physical environment in which satellites operate is complex and harsh, with frequent movements and control levels affected by high spatiotemporal dynamics. To counter these threats, it is necessary to design technologies such as autonomous driving obstacle avoidance, particle upset mitigation, and electromagnetic interference resistance to ensure the physical environment safety of both the space segment satellites and the ground segment.

2) Electromagnetic Domain Security

The open wireless channels, long-distance transmission, wide coverage, and complex and harsh operating environment of satellite Internet make it more susceptible to physical domain attacks than terrestrial wireless networks, such as interference, eavesdropping, and deception. These attacks threaten the confidentiality, availability, and integrity of satellite Internet. The electromagnetic domain security technologies of satellite Internet mainly addresses anti-jamming, eavesdropping prevention, and deception avoidance.

3) Control Domain Security

The control domain of satellite Internet is responsible for core control functions such as satellite link access, authentication and authorization, access control, and routing transmission. It is the "brain" of satellite Internet. Therefore, the control domain is a key target for satellite Internet attacks. The control domain security technologies of satellite Internet mainly includes identity authentication and key management, access, link, routing, and transmission control.

4) Forwarding Domain Security

The forwarding domain of satellite Internet is responsible for routing and forwarding network data and needs to ensure the confidentiality, integrity, availability, and traceability of data forwarding. The security and trustworthiness of the forwarding domain are crucial to its service quality. It includes source address verification, data forwarding security, abnormal traffic detection and tracing, data confidentiality protection, and data integrity protection.

VI. FUTURE POTENTIAL STANDARDS IN SATELLITE INTERNET

We believe that as the satellite Internet evolves to an integrated satellite-terrestrial Internet, new global, diverse, and intelligent security risks will continue to emerge. Traditional "patching" passive defense will be insufficient. Thus, it is needed to shift to active security and trustworthy technologies, enhancing the satellite Internet's ability to immunize, coexist with, and "live with" unknown intelligent security risks. Here, we outline the future trend of standardization efforts for Satellite Internet.

1）Physical Domain Security Technical Specifications

The satellite Internet is a cyber-physical network operating in a complex environment, where cyber and physical security are interwoven. Future research will focus on enhancing cyber security in the uncontrolled, highly dynamic space environment. This includes collaborative design with satellite autonomous driving, radiation resistance, and electromagnetic interference mitigation. Cross-disciplinary innovation between network and aerospace fields will be key to achieving integrated security protection.

2） Control Domain Security Technical Specifications

Exposed satellite nodes, open channels, and dynamic network topology make the satellite Internet's core functions more vulnerable. Frequent interoperability across different protocols and systems further expands the attack surface. Future research will focus on active suppression of multi-dimensional security risks, with breakthroughs in collaborative threat detection and protection technologies to evolve from single-point to multi-point collaborative defense.

3） Data Domain Security Technical Specifications

The essence of data domain security technology is the contest of capabilities between offense and defense. Satellite Internet, with its asymmetric capabilities between space and terrestrial segments, is vulnerable to attacks such as data tampering/listening, source address forgery, and DDoS. Future research should focus on collaborative active defense to amplify defense capabilities, increase attack costs, and change the current vulnerable situation of passive defense.

4） Service Domain Security Technical Specifications

As the number of satellites increases and their capabilities improve, satellite Internet will integrate network communication, navigation, remote sensing, and computing into comprehensive services. However, the security of these integrated services needs to be enhanced, especially considering the current isolation and heterogeneity of traditional satellites. Therefore, it is crucial to proactively research the integrated services' security technologies of satellite Internet communication, navigation, remote sensing, and computing to ensure the future development of diverse satellite Internet services.

VII. Conclusion

This paper proposes a new security architecture for Satellite Internet from a standardization perspective. The architecture provides comprehensive coverage of security technologies across the physical environment domain, electromagnetic domain, control domain, and forwarding domain through multi-layered protection of the physical environment and communication network security. It not only addresses the unique challenges of Satellite Internet, such as the complex space environment, orbit and spectrum congestion, and asymmetric resources between satellites and terrestrial nodes, but also offers targeted solutions to enhance the active security and trustworthiness of Satellite Internet. In addition, the paper explores the direction of future standardization efforts, emphasizing the importance of improving the immune capability, coexistence capability, and “living with” capability of Satellite Internet in the face of unknown intelligent security risks. In summary, enhancing the active security and trustworthiness of Satellite Internet is crucial for its development.

Acknowledgment

This work was supported by the National Key Research and Development Program of China under Grant 2022YFB3105203. This work was also supported by the Zhongguancun Laboratory.

References

[1] Heo J, Sung S, Lee H, et al. MIMO satellite communication systems: A survey from the PHY layer perspective[J]. IEEE Communications Surveys & Tutorials, 2023, 25(3): 1543-1570.

[2] Starlink. https://www.starlink.com/.

[3] Oneweb. https://www.oneweb.world/.

[4] Amazon kuiper. https://www.geekwire.com/2019/amazon-project-kuiper-broadband-satellite/.

[5] Telesat. https://www.telesat.com/.

[6] Spacex successfully tests inter-satellite starlink connectivity via lasers. https://wccftech.com/spacex-starlink-satellite-laser-test/.

[7] The mass-produced spacecraft carry a communications payload using the ku, ka and e frequency bands. https://space.skyrocket.de/doc_sdat/starlink-v2-0-ss.htm.

[8] Luo X, Chen H H, Guo Q. LEO/VLEO satellite communications in 6G and beyond networks–technologies, applications, and challenges[J]. IEEE Network, 2024, 38(5): 273-285.

[9] Matthew Scholl, Theresa Suloway, NIST Interagency Report NIST IR 8270 Introduction to Cybersecurity for Commercial Satellite Operations, July 2023.

[10] CCSDS Guide for Secure System Interconnection. Report Concerning Space Data System Standards, CCSDS 350.4-G-1. Green Book. Issue 1. Washington, D.C.: CCSDS, Nov 2007.

[11] Security Threats against Space Missions. Report Concerning Space Data System Standards, CCSDS 350.1-G-1. Green Book. Issue 1. Washington, D.C.: CCSDS, Oct 2006.

[12] Draft new Report ITU-R M. [NGAT_SAT], Key elements for integration of satellite systems into Next Generation Access Technologies, July 2019.

[13] new Recommendation ITU-T Y.FMSC-TS: “Traffic scheduling for fixed, mobile and satellite convergence in IMT-2020 network and beyond “, Mar 2023.

[14] TR 38.811, "Study on New Radio (NR) to support non-terrestrial networks", REL-15 SI FS_NR_nonterr_nw, RAN, Jun 2018.

[15] TR 22.822, "Study on using satellite access in 5G", REL-16 SI FS_5GSAT, SA1 Jun 2018.

[16] TS 38.108, "NR; Satellite Access Node radio transmission and reception", REL-17 WI NR_NTN_solutions, RAN4 Jun 2022.

[17] TR 38.882,”Study on requirements and use cases for network verified UE location for Non-Terrestrial-Networks (NTN) in NR", REL-18 SI FS_NR_NTN_netw_verif_UE_loc, RAN Jun 2022.

[18] TC12. https://ccsa.org.cn/station/?title=TC12.

[19] Research on Space-Ground Integrated Addressing Technology for Large-Scale Low-Earth Orbit Constellation Networks (Draft for Comments), 2024B58, May 2024.

[20] Research on Deterministic Transmission Technology for Space-Ground Integrated Networks (Draft for Comments), B-202311171146, May 2024.

[21] Research on QoS Optimization and Assurance Technology for Space-Ground Integrated Networks (Draft for Comments), 2023B122, May 2024.

[22] Research on Traffic Scheduling for Space-Ground Integrated Networks (Draft for Comments), 2023B121, May 2024.

[23] TC425. https://std.samr.gov.cn/search/orgDetailView?tcCode=TC425.

[24] Space Data and Information Transfer Systems—Spacecraft Information System Software Architecture, GB/T 43374-2023, November 2023.

[25] Space Data and Information Transfer Systems—Licklider Transmission Protocol (LTP), GB/T 42649-2023, May 2023.

[26] Space Data and Information Transfer Systems—Lossless Data Compression, GB/T 42636-2023, May 2023.