Hindawi
IET Information Security
Volume 2023, Article ID 5604802, 15 pages
https://doi.org/10.1049/2023/5604802

Review Article

A Survey of Secure Communications for Satellite Internet Based on Cryptography and Physical Layer Security

Yu Zhang, [1,2] Shuangrui Zhao, [1,2] Ji He, [1,2] Yuanyu Zhang, [1,2] Yulong Shen, [1,2] and Xiaohong Jiang [3]

[1] *School of Computer Science and Technology, Xidian University, Xi'an, China*
[2] *Shaanxi Key Laboratory of Network and System Security, Xidian University, Xi'an, China*
[3] *School of Systems Information Science, Future University Hakodate, Hokkaido, Japan*

Correspondence should be addressed to Shuangrui Zhao; zhaoshuangrui@xidian.edu.cn

Received 9 June 2023; Revised 3 August 2023; Accepted 2 September 2023; Published 26 October 2023

Academic Editor: Tom Chen

Copyright © 2023 Yu Zhang et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Satellite internet serves as an indispensable component of the upcoming sixth-generation networks for providing global broadband internet access service. Due to the open nature of satellite-ground communication, security issue in satellite internet has always been an important concern for both industry and academia. Although many researchers focus on secure communications in satellite internet, the literature is surprisingly sparse, with no comprehensive overview of the state-of-the-art security techniques. This paper provides an in-depth survey of secure communications for various satellite internet scenarios. Based on different security mechanisms, we first categorize the existing works of secure communications in satellite internet into two categories: cryptography-based and physical layer security-based. The former includes classical encryption-based and quantum encryption-based secure communication, and the latter is further divided into precoding-based, cooperative jamming-based, relay selection-based, and physical-layer authentication-based secure communication depending on the applied techniques. Finally, we provide some future research directions.

1. Introduction

Satellite internet can bring a variety of benefits like wide coverage, low latency, and high throughput, and thus has great application potential in both civil and military applications, such as disaster rescue, surveillance, environmental inspection, and so on. As reflected by recent standardization endeavors, satellite internet is recognized as a highly promising technology to provide global broadband internet access services for the upcoming sixth-generation (6G) networks [1]. Recently, various projects around the world, including Starlink, OneWeb, Telesat, etc., have been established to construct satellite internet and have shown their effectiveness in providing both low-cost and high-speed global services. However, due to the open nature of the wireless medium, satellite internet is more vulnerable to communication security threats than conventional terrestrial internet. Therefore, how to guarantee secure communications in satellite internet is a critical issue that needs to be carefully addressed [2].

Traditionally, secure communication can be achieved by exploiting key-based cryptography in the upper layers of the protocol stack, which relies on computational complexity [3]. Recently, several initial works have explored the key-based secure communications in satellite internet. Most of the works focused on the improved advanced encryption standard (AES) algorithms with the same encryption and decryption keys [4–9]. While these improved AES-based cryptography schemes have been successful in preventing communications from being intercepted, recent advances in the computational power of satellite internet devices have caused some security threats [10]. Unlike the improved AES, quantum encryption is a new approach that uses quantum mechanics for key generation, ciphertext communication, and antieavesdropping [11]. It is notable that quantum encryption is not based on mathematical computational hardness but on physics and quantum mechanics. Thus, quantum encryption is highly promising to ensure secure communications in satellite internet.

In addition to the key-based secure communications, physical layer security (PLS)-based secure communications, e.g., via precoding, cooperative jamming, relay selection, and physical-layer authentication (PLA), in satellite internet have also drawn much attention. By exploiting the inherent randomness of the wireless medium, like fading, noise, and interference, PLS-based schemes ensure the communication security at the physical layer to supplement existing upper-layer schemes [12]. The fundamental principle of the PLS-based schemes is that when the quality of the main channel is superior to that of the wiretap channel, information can always be confidentially delivered through the main channel irrespective of the eavesdroppers' computing capability. Due to the advantages of high robustness, easy deployment, and low complexity, PLS-based secure communications have been considered another critical component for secure communications in satellite internet [13].

1.1. Existing Surveys and Tutorials. By now, a couple of surveys and tutorials related to secure communications of satellite internet have been presented in the literature [14–18], including cryptography-based secure communications and PLS-based secure communications, etc.

In particular, Bedington et al. [14] provided a detailed survey about satellite quantum encryption and discussed its protocols, infrastructures, and technical challenges. Pirandola et al. [15] introduced the state-of-the-art research progress in satellite quantum communications under different conditions, including space-link losses, low earth orbits (LEOs) and higher earth orbits, link in night and day, and so on. Taking into account the multiple-input multiple-output and nonorthogonal multiple access (NOMA) technologies, Xiao et al. [16] elaborated on the applicability and potential challenges of millimeter wave (mmWave) secure communications over the satellite internet. From the perspective of PLS, Li et al. [17] conducted a comprehensive survey on secure communications in satellite internet according to different application scenarios such as land mobile satellite networks, hybrid satellite-terrestrial relay networks (HSTRNs), and satellite-terrestrial integrated networks (STINs). Tedeschi et al. [18] presented a survey of the literature on the security of satellite-based communication systems from the perspectives of both PLS and cryptography. This survey covered several research branches, including physical layer secure communication, physical layer antispoofing, physical layer antijamming, cryptography-based authentication, key agreement, and quantum key distribution (QKD), providing a systematic classification of the literature, while it just roughly summarized the papers in each branch in a table according to several features without giving a detailed introduction to each paper. For example, the authors summarized and compared the papers addressing the physical layer secure communication issue according to channel state information (CSI) availability, adversary type (e.g., external, internal), adversarial receiving antennas (e.g., single, multiple), adversarial antenna type (e.g., omnidirectional, directional), and performance metrics (e.g., secrecy rate (SR), secrecy outage probability (SOP)).

1.2. Contributions. The aforementioned surveys help us understand the latest research status on the security of satellite-based communications, whereas they focused on either satellite quantum communications (e.g., [14, 16]) or PLS-related research (e.g., [15, 17]), failing to provide a comprehensive literature overview. Although Tedeschi et al. [18] introduced both cryptography-based and PLS-based research, their emphasis is on the summary and comparison of current works while providing little information about the security techniques applied in each work. Thus, a novel survey that analyzes satellite-based communication security from a more exhaustive technology-oriented viewpoint would be timely. In this survey, we aim to thoroughly review the latest research progress on secure communications in satellite internet and provide in-depth discussions on applied security techniques/mechanisms of each work from both the cryptography and PLS perspectives. In particular, we divide the existing works of the cryptography-based secure communications in satellite internet into classical and quantum encryption-based secure communications, and divide those of the PLS-based secure communications into precoding-based, cooperative jamming-based, relay selection-based, and PLA-based secure communications depending on the applied techniques. Then, we detail each research work, including the application scenario, optimization problem, security mechanism, secrecy performance, and so on. Finally, we point out potential security challenges faced by satellite internet and highlight possible future directions.

The rest of this paper is organized as follows. Section 2 introduces the architecture of satellite internet. The latest research progress on cryptography-based secure communications and PLS-based secure communications for satellite internet are provided in Section 3 and Section 4, respectively. Section 5 highlights the open problems to be tackled and future research directions, and Section 6 concludes the paper. We present the organization of this paper in Figure 1. The major abbreviations used throughout this paper have been listed in Table 1.

2. Background

In this section, we briefly introduce the architecture of satellite internet, as shown in Figure 2. Satellite internet interconnects the fifth-generation (5G) networks and emerging networks like the Internet of Things, unmanned aerial vehicle (UAV) networks, and HSTRNs to provide global broadband internet access service [19, 20]. Based on different orbit altitudes and various characteristics of communication nodes in satellite internet [17], we divided the architecture into a space-based backbone network, a space-based access network, and a terrestrial-based backbone network from space to the ground. Satellites in the space segment of the architecture usually conclude geostationary earth orbit (GEO) satellites, medium earth orbit (MEO) satellites, and LEO satellites. Note that GEO satellites are not suitable for supporting real-time communication services due to their high altitude and long delay, but they can act as managers. MEO satellites are defined as space relays, where the

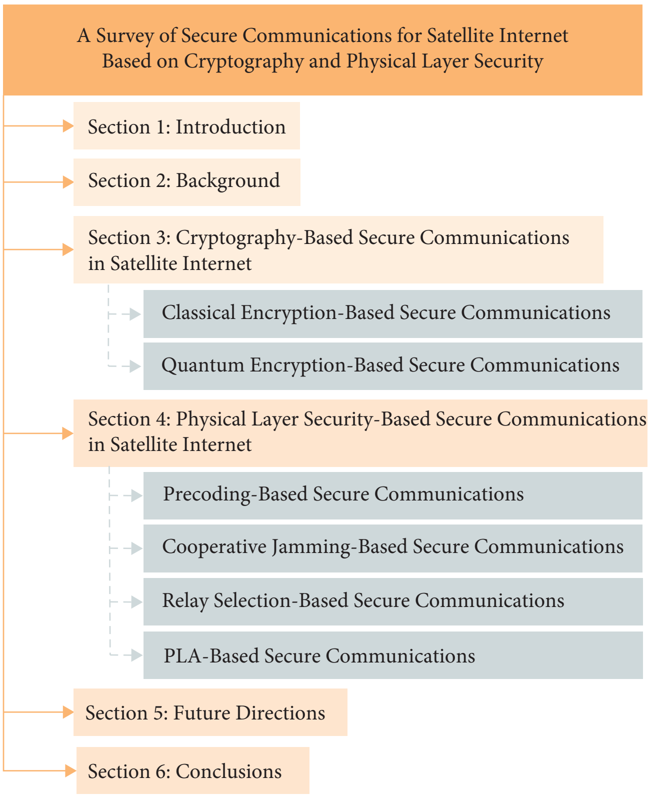
A Survey of Secure Communications for Satellite Internet Based on Cryptography and Physical Layer Security
Section 1: Introduction
Section 2: Background
Section 3: Cryptography-Based Secure Communications in Satellite Internet
Classical Encryption-Based Secure Communications
Quantum Encryption-Based Secure Communications
Section 4: Physical Layer Security-Based Secure Communications in Satellite Internet
Precoding-Based Secure Communications
Cooperative Jamming-Based Secure Communications
Relay Selection-Based Secure Communications
PLA-Based Secure Communications
Section 5: Future Directions
Section 6: Conclusions

Figure 1: Organization of this paper.

coverage and stability are inferior to GEO while the altitudes are higher than LEO. With the lowest orbital altitude and time delay, LEO satellites can bridge the space and ground segments in the satellite internet architecture.

The space-based backbone network is mainly composed of GEO satellites, such as remote sensing satellites, deep-space detection satellites, spy satellites, and so on [17], which are usually placed in orbits 36,000 km above the Earth. Compared with the space-based access network, the space-based backbone network controls a more stable network topology so as to manage route allocation of the entire satellite internet system. Until now, although the terrestrial network has enabled high-speed communication in densely populated regions, it still cannot provide internet access to some remote regions. Fortunately, the space-based backbone network could guarantee broadband internet access in these regions for military defense, environmental monitoring, and geological prospecting [21]. In addition, direct transmission links can also be established between the space-based access network and terrestrial for long-term monitoring services with no delay requirements.

The space-based access network is responsible for connecting the space-based backbone network and the terrestrial-based backbone network, which consists of MEO satellites and LEO satellites orbiting between 500 and 36,000 km [22]. Due to the strong processing power of MEO satellites and the shortest space-ground latency of LEO satellites, the space-based access network can catch the topology information and handle the accessing tasks of devices from terrestrial networks directly.

Table 1: Major abbreviations used in this paper.

Notation	Meaning
AES	Advanced encryption standard
AF	Amplify-and-forward
AO	Alternating optimization
BB84	Bennett–Brassard 1984
BS	Base station
CPSO	Cooperative particle swarm optimization
CSI	Channel state information
CSTN	Cognitive satellite-terrestrial network
CTR	Counter block cipher
DF	Decode-and-forward
FSL	Free space loss
GEO	Geostationary earth orbit
HAP	High-altitude platform
HSTRN	Hybrid satellite-terrestrial relay network
IoT	Internet of Things
IRS	Intelligent reflecting surface
ISHAPN	Integrated satellite and HAP network
LEO	Low Earth orbit
MBSS	Multibeam satellite systems
MEO	Medium Earth orbit
MIMO	Multiple-input multiple-output
MISO	Multiple-input single-output
MRT	Maximal ratio transmission
NLoS/LoS	Nonline of sight/line of sight
NOMA	Nonorthogonal multiple access
PLA	Physical-layer authentication
PLS	Physical layer security
QKD	Quantum key distribution
SCA	Successive convex approximation
SDR	Semidefinite relaxation
SEE	Secrecy energy efficient
SISO	Single-input single-output
SNR	Signal-to-noise ratio
SOCP	Second-order cone programing
SOP	Secrecy outage probability
SR	Secrecy rate
STIN	Satellite-terrestrial integrated network
UAV	Unmanned aerial vehicles

The terrestrial-based backbone network is mainly composed of the core network, wireless local area networks, special gateways, data centers, a large number of terminal devices, etc. The special gateways, termed satellite operators, enable the interconnection between satellites and huge terrestrial networks due to their powerful data distribution capabilities. Computing tasks with high data traffic generated by terminal devices, including aircraft and tanks in the military and mobile phones and vehicles in the civilian, are sent to the data center. Because of more computing resources than satellites, the data center can calculate all the computing tasks unloaded from the whole space and ground segments. Although the terrestrial-based backbone network has proved a greater success in SR and throughput than others in the

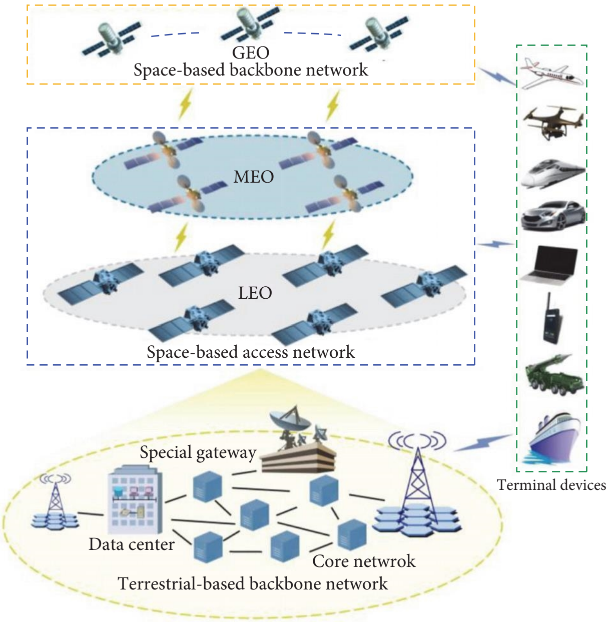
GEO
Space-based backbone network
MEO
LEO
Space-based access network
Terminal devices
Special gateway
Data center
Core netwrok
Terrestrial-based backbone network

FIGURE 2: Architecture of satellite internet.

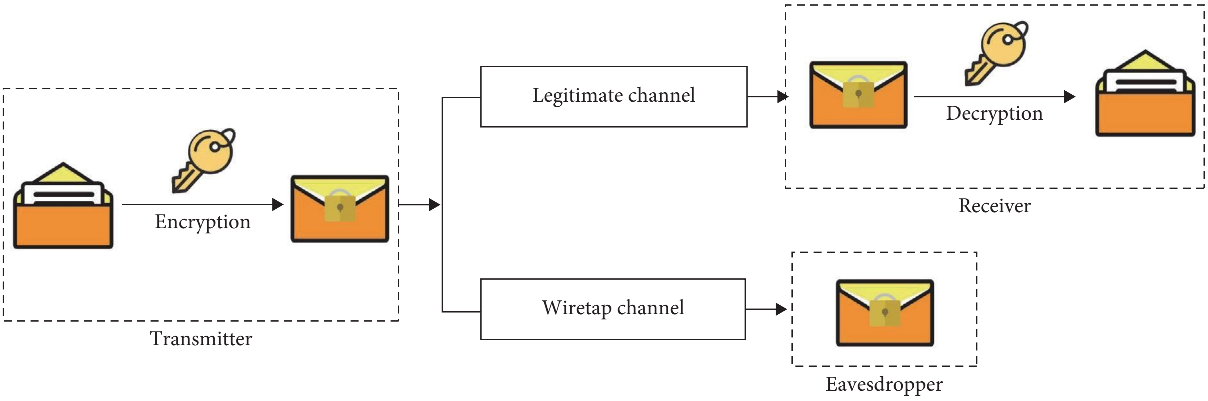

FIGURE 3: Classical encryption-based secure communications.

space segment, it is vulnerable to natural disasters such as the destruction of base stations (BSs) caused by a rainstorm.

3. Cryptography-Based Secure Communications in Satellite Internet

In this section, we review the existing works of classical and quantum encryption-based secure communications in satellite internet.

3.1. Classical Encryption-Based Secure Communications. According to the encryption principles, classical encryption can be divided into symmetric encryption and asymmetric encryption [23]. As shown in Figure 3, a transmitter and a receiver use the same secret key for encryption and decryption in symmetric encryption, whereas they use a pair of public and private keys in asymmetric encryption. Although the latter has higher-level security than the former, it also brings a greater communication overhead, which is unacceptable for satellite internet with low latency requirements and limited resources. Therefore, most existing classical encryption studies in satellite internet communications focused on symmetric encryption with slightly lower security but less delay [24–27].

Bensikaddour et al. [4] considered a satellite image transmission network under statistical attacks and proposed an AES-Geffe image encryption scheme to achieve excellent satellite image encryption performance. Then, Bentoutou et al. [5] proposed an improved satellite image encryption algorithm based on chaotic mapping and AES for vehicular earth observation, where high-level security was achieved subject to a single event disruption constraint. Under a cipher feedback mode, Jeon and Choi [6] proposed a novel encryption method by combining the AES encryption with a turbo channel coding in satellite communications, meeting the requirements of processing time gain, security enhancement,

Table 2: Comparison of existing works: classical encryption-based secure communications in satellite internet.

Ref.	Year	Scenario	Algorithm	Cipher mode
[4]	2017	Satellite images encryption	Modified AES-Geffe encryption	AES-CTR block cipher mode
[5]	2020	Satellite images encryption	Chaotic maps and AES-CTR encryption	AES-CTR block cipher mode
[6]	2019	Satellite-based communication	Combined AES encryption and turbo coding	Cipher feedback mode
[7]	2019	Satellite-based communication	Parallel cipher-based message authentication coding	CTR and parallel cipher mode
[8]	2020	Satellite-based communication	Improved high-throughput encryption algorithm	AES-CTR block cipher mode
[9]	2020	Satellite images encryption	Fridrich-based multispectral image encryption method	Generic chaotic block cipher mode

and bit-error-rate reduction simultaneously. Pirzada et al. [7] studied the encryption algorithms with high throughput and proposed a parallel encryption mechanism based on cipher and message authentication code to achieve faster encryption for satellite internet. Pirzada et al. [8] further considered a satellite communication system with the demands of high-speed computation and lightweight implementation, and developed a high-throughput AES algorithm to improve the security performance. Bensikaddour et al. [9] proposed a new multispectral image encryption method based on the Fridrich scheme with high performance and low overhead. The above works are compared in Table 2, which allows readers to capture the critical information of classical encryption-based secure communications in a short time.

3.2. Quantum Encryption-Based Secure Communications. Although most satellites that have been launched used classical encryption to guarantee secure communications, some rolled out a relatively new cryptographic primitive named quantum encryption, pushing the boundaries of satellite communication security. Quantum encryption is an absolutely secure communication mechanism that cannot be deciphered, which consists of two main stages: the QKD stage via a quantum channel and the private message transmission stage via a traditional channel. In the first stage, the two parties (a transmitter and a receiver in terrestrial) obtain a pair of quantum keys that are entirely random through the quantum channel, as shown in Figure 4(a). In the second stage, the obtained quantum keys are used to encrypt the source messages at the transmitter and then decrypt the encrypted messages at the receiver, as shown in Figure 4(b). In other words, the information transmitted in the QKD stage of quantum encryption is equivalent to the secret keys of classical encryption and plays a core role in the whole quantum encryption-based communication process.

In 2017, a launched quantum satellite Micius became the milestone of quantum encryption. Liao et al. [28] launched the LEO quantum satellite Micius to realize decoy-state QKD and first broke the limitation of long-distance channel loss. Then, intercontinental quantum communications were achieved by using the Micius as a trusted relay [29]. In a two-way satellite-terrestrial network, Dai et al. [30] proposed a quantum encryption communication scheme to distribute high-precision time information and conducted experiments on the scheme at the Micius. Yin et al. [31] demonstrated a tenfold increase in the security distance of entanglement-based quantum encryption between two ground separation stations at a finite key rate, where the entangled quantum pairs were launched by Micius towards the ground station. Lim et al. [32] performed a limited fundamental security analysis in a satellite-terrestrial network, reducing the block length constraint of the standard channel protocol, and demonstrated the analysis with a modified Micius satellite.

In addition to studies on quantum satellite Micius, Agnesi et al. [33] proposed a novel polarization encoder system for satellite quantum encryption by exploiting photonic degrees of freedom and attested the security of quantum encryption links. Kish et al. [34] demonstrated the feasibility of quantum encryption using continuous variables in longer satellite-to-Earth links, while previous studies all concentrated on short-range terrestrial links. Pan and Djordjevic [35] evaluated the lower bound on secure key rates for continuous-variable quantum encryption in satellite internet to better investigate the eavesdropper's wiretap strategy, which provided a high-security level for the 6G networks. Alshaer et al. [36] developed a secrecy performance analysis of a ground-to-satellite free-space optical system with continuous-variable quantum encryption protocol by using a bipolar pulse amplitude modulation over modulated gamma fading channel, where various parameters of communication nodes were considered. Based on the above results, Dequal et al. [37] further examined the establishing quantum keys in a satellite-to-ground downlink configuration using continuous variables and provided a practical solution compatible with classical optical communication systems first. Table 3 highlights the diverse scenarios, protocols, and main contributions of the existing quantum encryption-based secure communications in satellite internet.

4. PLS-Based Secure Communications in Satellite Internet

As a compelling complementary to the upper-layer security mechanism, the PLS mechanism exploits the inherent features of wireless channels, such as the characteristics of multipath, reciprocity, and spatial uniqueness, to guarantee

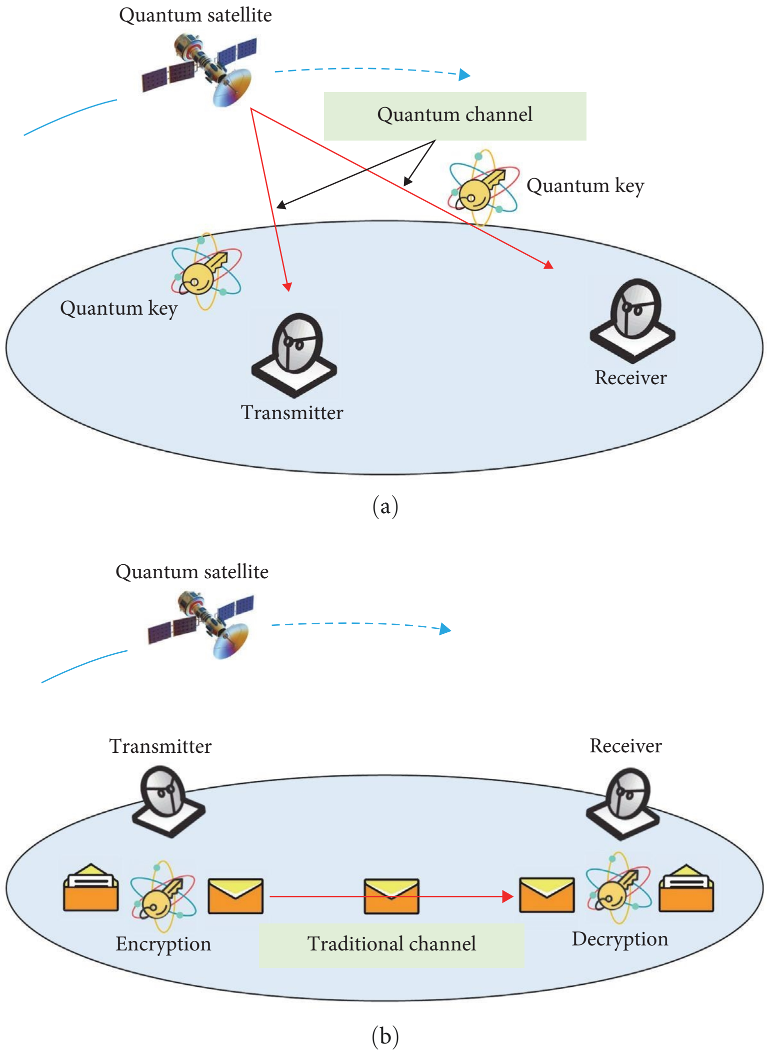

FIGURE 4: Quantum encryption-based secure communications: (a) the QKD stage; (b) the private message transmission stage.

secure communications [38]. Some early works have studied the PLS-based communication issues in satellite scenarios [39–42], including secrecy performance analysis, secure transmission design, secrecy capacity optimization, etc. This section reviews the existing studies on precoding-based, cooperative jamming-based, relay selection-based, and PLA-based secure communications in diverse scenarios of satellite internet depending on the applied techniques.

4.1. Precoding-Based Secure Communications. Precoding-based secure communications have recently been actively studied in satellite internet. Its core idea is to optimize the precoder at the transmitter to turn the uniform scattering of the transmitter signal into the desired direction, as shown in Figure 5. As a result, the received signal strength at particular receivers is greatly improved, while that at the eavesdroppers is reduced.

Yan et al. [43] designed an optimal secure precoding strategy at a relay in the satellite-relay-destination system, where the relay forwarded secret messages toward the destination while sending artificial noise toward eavesdroppers simultaneously, subject to the relay power constraint. In a multibeam satellite communication system, Lin et al. [44] proposed a robust precoding scheme at the multibeam satellite by comprehensively considering the effects of beam gain, channel loss, and rain attenuation to enhance the sum SR of the system. Lin et al. [45] further proposed a novel precoding-based transmission scheme in a multibeam satellite system to maximize the SEE by alternate optimizing the precoding vector and power allocation vector at the multibeam satellite.

In addition to the above precoding schemes implemented at a single communication node, there is another line of research that designed the precoding schemes at multiple nodes. The multinode cooperative precoding performs much better than the single-node precoding because it can provide higher spectral efficiency, robustness, and beam gain [46–48]. However, since the multiple precoders are hard to optimize, the problem of multinode cooperative precoding design is more challenging than that of the single-node precoding design [49, 50]. Some research efforts have been devoted to the multinode precoding design for secure communications in satellite internet. Assuming the perfect CSI, Lin et al. [51] proposed two schemes for the joint

Table 3: Comparison of existing works: quantum encryption-based secure communications in satellite internet.

Ref.	Year	Scenario	Protocol	Contribution
[28]	2017	Satellite-to-ground link (LEO)	Decoy-state BB84 QKD	The point-to-point quantum encryption was achieved between a quantum satellite with a ground station up to 1,200 km away
[29]	2018	Satellite-to-ground link (LEO)	Decoy-state BB84 QKD	The quantum communication distance was extended to intercontinental distances
[30]	2020	Satellite-to-ground two-way link	Polarization-encoding BB84 QKD	The high-precision time synchronization in a quantum communication system was achieved
[31]	2020	Satellite-to-ground link	BBM92 QKD	The secure distance of quantum transmission on the ground was increased
[32]	2021	Quantum space communication	Entanglement-based BBM92 QKD	The block length requirement of the finite key was reduced
[33]	2019	Satellite-to-ground link	BB84 QKD	The security of quantum encryption implementations was enhanced by using the proposed self-compensating polarization encoder
[34]	2020	Satellite-to-ground link	Coherent state QKD	The feasibility of continuous-variable QKD over the much longer satellite-to-Earth channel was proved
[35]	2020	Satellite-to-satellite link	Generic QKD	The secure key rate lower bounds of continuous-variable quantum encryption for realistic free space were analyzed
[36]	2020	Ground-to-satellite free-space optical system	Continuous-variable QKD	The security performance of the current quantum encryption system using a bipolar pulse amplitude modulation was evaluated
[37]	2021	Satellite-to-ground link (LEO)	No-switching continuous-variable QKD	The feasibility of combined quantum communication with classical optical communication systems was proved

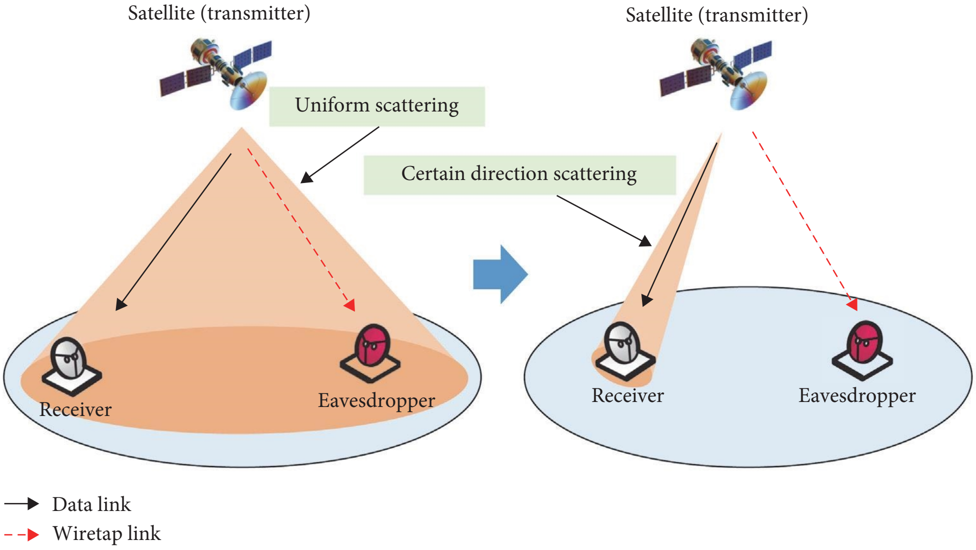

Figure 5: Precoding-based secure communications.

Table 4: Comparison of existing works: precoding-based secure communications in satellite internet.

Ref.	Year	Scenario	Type of precoder	CSI availability	Channel model	Objective	Solution approach
[43]	2016	HSTRN	Relay	Perfect CSI	Satellite channel: shadowed-Rician fading Terrestrial channel: Rayleigh fading	SR maximization	SDR, one-dimensional search
[44]	2019	STIN	Satellite	Imperfect CSI	Satellite channel: FSL, rain attenuation, satellite beam gain	SR maximization	SCA, S-procedure method
[45]	2022	MBSS	Satellite	Perfect CSI	Satellite channel: FSL, rain attenuation, satellite beam gain	SEE maximization	AO, SCA
[51]	2018	CSTN	Satellite, BS	Perfect CSI	Satellite channel: FSL, rain attenuation, satellite beam gain Terrestrial channel: LoS	Total transmit power minimization	SOCP, penalty function, gradient algorithm
[52]	2021	NOMA-based CSTN	Satellite, BS	Imperfect CSI	Satellite channel: rain attenuation, satellite beam gain Terrestrial channel: Rayleigh fading	SR maximization	SCA, SDR
[53]	2018	STIN	Satellite, BS	Perfect CSI	Satellite channel: LoS Terrestrial channel: scattered multipath	SR maximization	CPSO, path-pursuit iteration based algorithm
[54]	2019	ISHAPN	Satellite, HAP	Imperfect CSI	Satellite channel: FSL, rain attenuation, satellite beam gain HAP channel: LoS, NLoS	SR maximization	Penalty function, discretization method
[55]	2023	STIN	Satellite, BS	Imperfect CSI	Satellite channel: FSL, rain attenuation, satellite beam gain Terrestrial channel: LoS, NLoS	SR maximization	SCA, SDP

design of precoders at a GEO satellite and a terrestrial BS to guarantee secure communication in a software-defined architecture-cognitive satellite-terrestrial network (CSTN), in which a broadband satellite network was considered the primary network and a terrestrial cellular network was the second network. Then, considering the imperfect CSI, Li et al. [52] proposed a combined precoding scheme at a satellite and terrestrial BS for the secure downlink transmission of NOMA-based CSTN and maximized the SR of satellite users under the transmit power limits. Besides, Du et al. [53] investigated secure communication in a combined satellite and terrestrial cellular network, and designed a joint precoding scheme at an adaptive satellite and multiple ground stations to enhance the received signal quality of eavesdropped terminals. In an integrated satellite and HAP network, Lin et al. [54] first proposed a joint precoding scheme at a GEO satellite and HAP to maximize the SR and simultaneously minimize the total transmit power. In a NOMA-aided full-duplex cell-free STIN, Gao et al. [55] further improve the spectral efficiency by jointly optimizing the satellite and terrestrial beamforming, where the effects of realistic imperfect channel estimation and imperfect successive interference cancelation are considered. With the aid of Table 4, we summarize the key research gaps of existing precoding-based secure communications in satellite internet, such as the type of precoder, channel model, objective and solution approach, etc.

4.2. Cooperative Jamming-Based Secure Communications. Cooperative jamming techniques seek to design and implement a high-performance PLS for secure satellite communications. As shown in Figure 6, the core concept of cooperative jamming is to send artificial noise/jamming signals to eavesdroppers while a transmitter sends secret messages to a legitimate receiver. The artificial noise/jamming signals can be sent from the transmitter, the receiver, or external helper nodes called jammers. Such a technique greatly enlarges the difference between the legitimate and the eavesdropping channels in a positive manner, thereby improving communication security.

Different performances can be achieved by cooperating with different kinds of jammers on satellite internet. Under the SOP constraint, Cui et al. [56] proposed a cooperative jamming scheme in which a multibeam satellite and multiple terrestrial earth stations serve as friendly jammers to suppress eavesdroppers to minimize the power consumption of current STIN. In a CSTN, Lin et al. [57] investigated a friendly jamming strategy and exploited the rate-splitting multiple access technique at the BS jammer to improve the SEE of the destination subject to the destination's SR and the BS's transmission power.

Apart from using communication nodes as jammers, special external nodes can also be used as jammers to suppress eavesdroppers. Yan et al. [42] proposed a cooperative jamming strategy to maximize the SR at the destination in an HSTRN, in which the other terrestrial relays emitted jamming signals to the eavesdropper when a relay forwarded messages to the destination, and studied the effects of relay numbers in the proposed scheme on the SR. Bankey and Upadhyay [58] proposed a cooperative jamming scheme in a downlink land mobile satellite system by using friendly UAV jammers in the presence of eavesdroppers on the ground. Bouabdellah and Bouanani [59] proposed a PLS

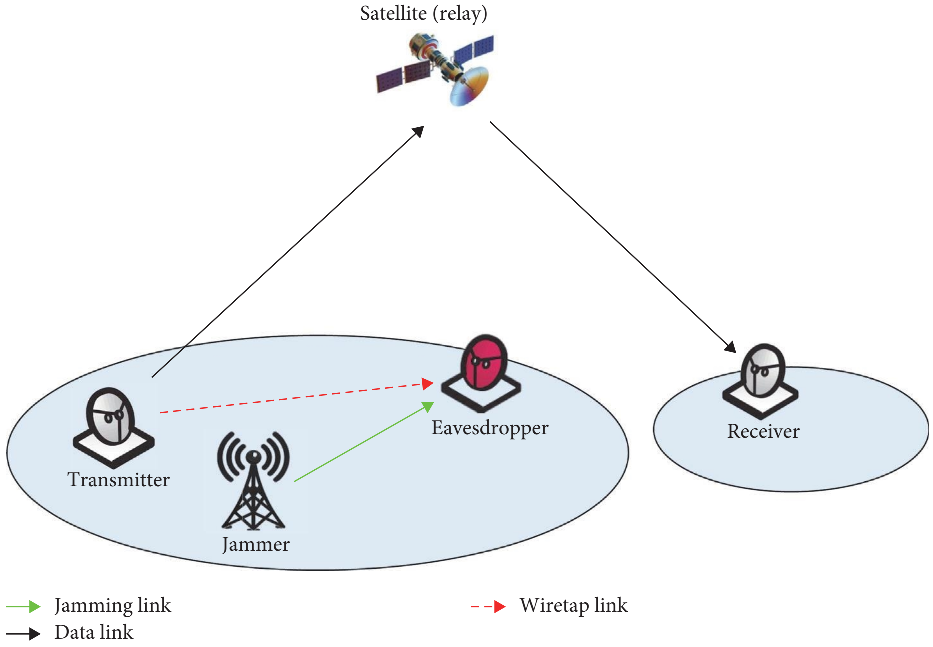

Figure 6: Cooperative jamming-based secure communications.

Table 5: Comparison of existing works: cooperative jamming-based secure communications in satellite internet.

Ref.	Year	Scenario	Type of jammer	CSI availability	Channel model	Objective
[56]	2020	STIN	Satellite, destination	Imperfect CSI	Satellite channel: FSL, rain attenuation, satellite beam gain Terrestrial channel: Rayleigh fading	Power consumption minimization
[57]	2020	CSTN	BS	Imperfect CSI	Satellite channel: FSL, rain attenuation, satellite beam gain Terrestrial channel: LoS, NLoS	SEE maximization
[42]	2019	HSTRN	External terrestrial node	Perfect CSI	Satellite channel: FSL, rain attenuation, satellite beam gain Terrestrial channel: Rayleigh fading	SR maximization
[58]	2020	STIN	External aerial node	Perfect CSI	Satellite channel: shadowed-Rician fading UAV channel: LoS, NLoS	SOP analysis
[59]	2021	CSTN	External terrestrial node	Perfect CSI	Satellite channel: shadowed-Rician fading Terrestrial channel: Rayleigh fading	Intercept probability analysis

scheme by using a free user as a friendly jammer in an interference-based hybrid CSTN, where the jammer broadcasted artificial noises constantly when a source transmits confidential messages to an optical ground station with a satellite relay. The comparison of the latest cooperative jamming-based secure communications is presented in Table 5, which clearly indicates the current research gaps in the type of jammer, CSI availability, objective, etc.

4.3. Relay Selection-Based Secure Communications. As a technique to utilize multiple relays for PLS, the core principle behind relay selection is to select an optimal relay from multiple relays that maximizes the channel difference between the legitimate and illegal channels, thereby enhancing communication security while maintaining transmission link connectivity, as shown in Figure 7. Currently, relay selection techniques have been widely used in secure communications in satellite internet, which are summarized as follows.

To improve transmission security, Cao et al. [41] proposed an optimal relay selection scheme based on the Round-Robin scheduling in an HSTRN with multiple terrestrial relays and a single destination, where the relays forwarded secrecy messages by turns under the perfect CSI of all links. Then, Guo et al. [60] also studied the relay selection problem in an HSTRN with multiple DF relays but multiple destinations and eavesdroppers, and proposed an optimal threshold-based relay selection scheme, selecting the two-hop link with maximal average secrecy capacity from all the links subject to the SNR constraint to enhance the secrecy performance. Considering a MISO HSTRN with multirelay and multidestination, Bankey and Upadhyay [61] presented two opportunistic link selection strategies under noncolluding

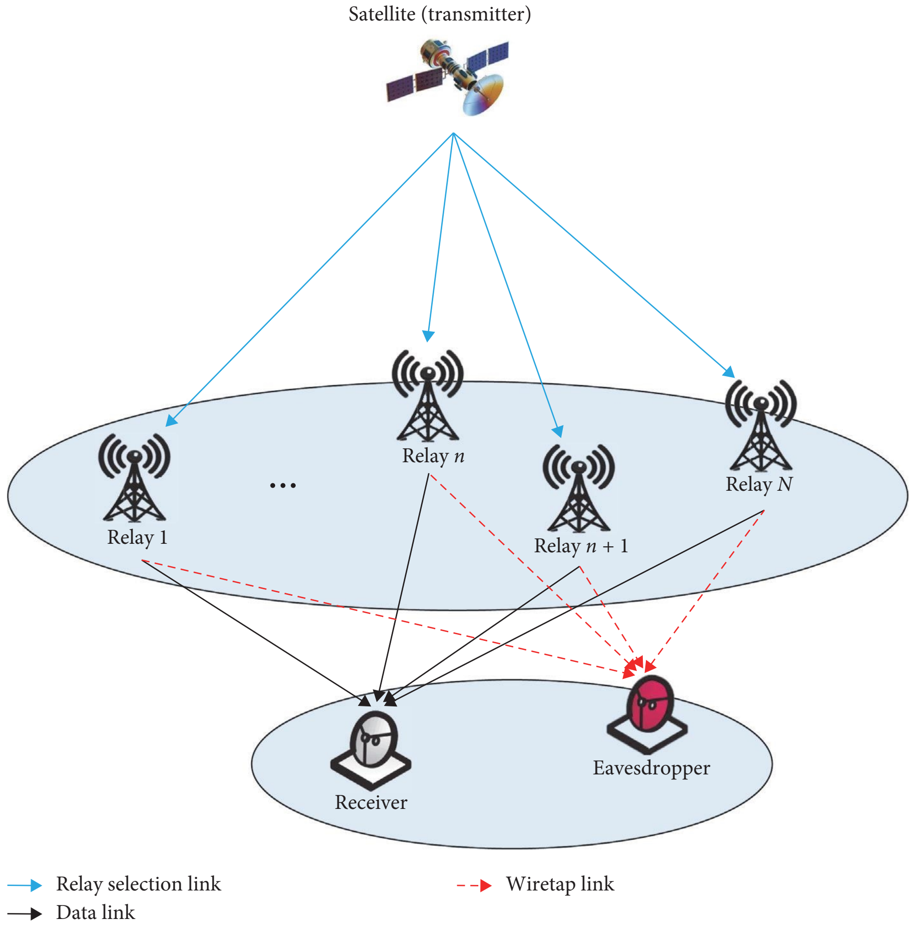

Figure 7: Relay selection-based secure communications.

and colluding wiretapping scenarios to minimize the SOP, respectively, in which the optimal relay and destination were selected based on the received instantaneous SNR. Li et al. [62] also studied the SOP performance in a MISO HSTRN under the conditions of known instantaneous CSI and statistical CSI, and proposed a relay selection scheme for cooperative interference relays based on the minimum of the SOP performance. Guo et al. [63] first analyzed the secrecy performance for a two-way ISTRN along with an opportunistic relay selection scheme, in which multiple legitimate users, eavesdroppers, and terrestrial two-way relays are considered. Table 6 shows a comparison of the aforementioned works in diverse system setups for readers further discussing the development of relay selection-based secure communications in satellite internet.

4.4. PLA-Based Secure Communications. PLA is another critical PLS technique that draws much attention in satellite internet. Its fundamental principle is to verify the identities of legitimate users by exploiting the physical-layer features of signals and wireless channels [64–67]. Different from the previously mentioned PLS techniques that only prevent secret messages from being passively eavesdropped, PLA can defend against passive and active attacks, such as spoofing, replay, and jamming [68, 69]. Due to the advantages of high robustness, low cost, and easy implementation in heterogeneous network environments, PLA has emerged as a promising way to guarantee secure communication in satellite internet.

Recently, some research efforts have been devoted to designing PLA-based secure communication schemes for satellite systems. Fu et al. [70] first proposed a Doppler frequency shift-based PLA scheme for land mobile satellite systems, where the downlink satellite system information signaling is authenticated before initial access. Topal and Kurt [71] provided a new PLA scheme to validate the identity of LEO satellites by comparing multiple measured Doppler frequency shift values with the reference values in constellations, where the reference values are calculated based on the satellites' velocities and locations. Then, Abdrabou and Gulliver [72] proposed a PLA scheme for LEO satellites based on Doppler frequency shift as well as received power characteristics and trained a one-class classification support vector machine to discriminate between legitimate and illegitimate satellites. In combination with convolutional neural networks, Oligeri et al. [73] proposed an alternative PLA scheme for satellites by generating physical-layer fingerprints with I/Q samples of Iridium signals. They also used Iridium Ring Alert messages

Table 6: Comparison of existing works: relay selection-based secure communications in satellite internet.

Ref.	Year	Scenario	System setup	Antenna setup	Relaying protocol	Channel model	Objective
[41]	2017	HSTRN	Single-satellite (GEO), multirelay (terrestrial), single-destination, single-eavesdropper	SISO	DF	Satellite-destination: shadowed-Rician fading channel Relay-destination: Rayleigh fading channel	SOP minimization
[60]	2018	HSTRN	Single-satellite (GEO), multirelay (terrestrial), multidestination, multieavesdropper	SISO	DF	Satellite-destination: shadowed-Rician fading channel Relay-destination: Rayleigh fading channel	SR maximization
[61]	2019	HSTRN	Single-satellite, multirelay (terrestrial), multidestination, multieavesdropper	MISO	AF, DF	Satellite-destination: shadowed-Rician fading channel Relay-destination: nakagami-m distribution channel	SOP minimization
[62]	2019	HSTRN	Single-satellite, multirelay (aerial), single-destination, single-eavesdropper	MISO	AF	Satellite-destination: Rician fading channel Relay-destination: Rician and Rayleigh fading channel	SOP minimization
[63]	2022	HSTRN	Single-satellite, multirelay (terrestrial), multidestination, multieavesdropper	SISO	DF	Satellite-destination: shadowed-Rician fading channel Relay-destination: Rayleigh fading channel	SOP minimization

Table 7: Comparison of existing works: PLA-based secure communications in satellite internet.

Ref.	Year	Scenario	Authentication features	Metrics	Type of attack	Channel model
[70]	2020	Satellite communication system, downlink satellite-ground channel	Doppler frequency shift	False alarm rate, miss detection rate	Spoofing attack	Binary hypothesis testing, nominal power spectral density sample decisions
[71]	2022	LEO satellites constellation, inter-satellite channel	Doppler frequency shift	Spoofing detection rate, false alarm rate	Spoofing attack	Decision fusion with OR rule, AND rule, majority rule
[72]	2022	Satellite communication system, downlink satellite-ground channel	Doppler frequency shift, received power	Authentication rate, false alarm rate, miss detection rate	Spoofing attack	Machine learning, one-class classification support vector machine
[73]	2022	Satellite communication system, intra-constellation channel, downlink satellite-ground channel	Radio fingerprinting, I–Q samples	True positive rate, false positive rate	Spoofing attack	PAST-AI, convolutional neural networks
[74]	2020	IRIDIUM satellite constellation, downlink satellite-ground channel	IRIDIUM ring alert messages	Waiting time, false positive rate	Spoofing attack	Reverse engineering, opportunistic IRIDIUM ring alert

to verify the actual GNSS location [74]. The above works on PLA-based secure communications are compared in Table 7, which indicates the current research gaps in the scenario, authentication features, metrics, type of attack, and methods.

5. Future Directions

Secure communications in satellite internet have made great progress so far, whereas some unresolved issues still remain. In this section, we discuss the challenges that secure communication of satellite internet faces and point out some potential research directions.

5.1. QKD. Some recent works have proved the feasibility of QKD in certain satellite-based communication scenarios, such as QKD from a geostationary orbit [75], QKD utilizing the decoy-state BB84 protocol in LEO satellite-ground link [76] and the continuous variable-QKD in satellite-based downlink transmission [34]. However, the practical application of QKD is still not entirely demonstrated.

As stated in an NSA policy report on QKD, several limitations, including the necessity of specific equipment, the difficulty of security verification, and the high risk of denial of service, need to be overcome before the large-scale application of QKD [77]. In particular, QKD-based security schemes are challenging to be integrated with existing communication nodes due to the requirements of dedicated fibers or physically free-space transmitters. Besides, QKD still has to find solutions to reduce its communication costs due to the massive access needs of terminal devices on satellite internet. Furthermore, integrating quantum communication networks into global satellite-terrestrial networks is challenging because the attenuation of quantum signals through terrestrial fiber-optic networks increases exponentially with distance.

In conclusion, the aforementioned limitations of QKD-based secure communication should be extensively studied in the future, which would open new avenues for satellite internet security.

5.2. Intelligent Reflecting Surface (IRS). In recent years, IRS, also known as reconfigurable intelligent surface (RIS), has attracted considerable attention as an extension of the PLS techniques. An IRS is a special surface that integrates low-cost passive reflective elements on a metallic plate. By dynamically adjusting the reflection amplitude and phase shift of the elements, IRS can reconfigure the wireless propagation channel to send signals in desired directions, realizing the similar idea of beamforming and precoding. Unlike beamforming and precoding, which change the direction of the signal at the transmitter, IRS acts as a passive reflector of the signal in the propagation path. Therefore, IRSs can be deployed between a transmitter and a receiver to enhance the received signal strength of the receiver while degrading that at eavesdroppers. Besides, compared with classical PLS techniques, the IRS technique passively reflects incident signals with no need of active radio frequency chains, thus can achieve secure communications in satellite internet with lower energy consumption and hardware costs.

Recently, some research efforts have been devoted to IRS-assisted secure satellite-terrestrial communication in different scenarios. Xu et al. [78] first proposed an IRS-assisted secure cooperative transmission scheme for a satellite-terrestrial downlink communication system, where the IRS was deployed near a single-antenna primary user to enhance the signal strength at the user as well as degrade the received signal at an eavesdropper. Ngo et al. [79] proposed an IRS-assisted cache-enabled secure transmission strategy for two-hop satellite-terrestrial networks to maximize the system secure transmission probability, where the satellite-IRS link was dominant due to the heavy shadowing in the satellite-user direct link. Lin et al. [80] first proposed a beamforming optimization scheme in a refracting RIS-assisted HSTRN to minimize the total power of both the satellite and BS, in which the incident signals can pass through the RIS.

Although research on IRS-assisted secure communications in satellite internet has already been in progress, the main focus is on terrestrial IRSs. Thanks to the advantages of low power consumption and easy deployment, IRS can be deployed at any object of satellite internet in principle, such as satellites, UAVs, BSs, and terminals, to assist in secure communication. We expect increasing attention toward the application of IRSs at different locations and objects to secure satellite-based communications.

5.3. Cross-Layer Security Mechanism. Both upper-layer security solutions based on conventional cryptography and PLS solutions have their pros and cons. Another future research direction is to design cross-layer security mechanisms that combine security techniques from the physical layer and others from the upper layer, providing more benefits for satellite-based communication security, such as finer-grained security guarantees and do-it-yourself security schemes. For example, Jeon et al. [81] first proposed a novel cross-layer secure scheme in a satellite network, combining the cipher feedback-AES and the turbo encoding technology, which improved the security performance.

However, there are still several problems to address when applying cross-layer security mechanisms. For example, the security at the physical layer is usually mathematically quantifiable based on well-defined metrics, such as SR, SOP, etc., while that of cryptographic schemes is usually measured based on the secret key length. Therefore, a critical issue is to develop a unified security evaluation system that is able to measure both the security performance of PLS solutions and that of upper-layer cryptographic schemes. Another critical issue is to determine the pattern of cross-layer design, which can be at the scheme layer or function level. By scheme level, we mean independent schemes at both layers can be combined to meet diverse security requirements. By function level, we mean part of the functions of the cryptographic schemes, such as secret key generation, can be implemented at the physical layer.

6. Conclusion

In this paper, we provided a comprehensive survey on the state-of-the-art research efforts for secure communications in satellite internet. According to different security mechanisms, existing studies of secure communications in satellite internet were divided into cryptography-based and PLS-based. Specifically, we first reviewed the up-to-date results on cryptography-based secure communications in satellite internet under different encryption algorithms, such as AES, quantum encryption, and so on. Based on various physical layer techniques in satellite internet, we then presented a detailed overview of research results on PLS-based secure communications. Some future research directions were also suggested in the paper to enhance security performance and tackle different challenges of the satellite internet. It is anticipated that this survey will serve as a significant guide for researchers working on this innovative field of satellite internet communications.

Data Availability

The data used to support the findings of this study are included within the article.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was supported in part by the Major Research plan of the National Natural Science Foundation of China under grant no. 92267204, in part by the National Natural Science Foundation of China under grant nos. 62202355, 62220106004, 61972308, 62202354, and 62102303, in part by the Innovation Capability Support Program of Shaanxi (program no. 2023-CX-TD-02), in part by Qin Chuangyuan Innovation and Entrepreneurship Talent Project of Shaanxi (grant no. QCYRCXM-2022-144), in part by the Basic and Applied Basic Research Fund of Guangdong Province (grant no. 2021A1515111017), in part by the Fundamental Research Funds for the Central Universities and the Innovation Fund of Xidian University.

References

[1] G. Gui, M. Liu, F. Tang, N. Kato, and F. Adachi, "6G: opening new horizons for integration of comfort, security, and intelligence," *IEEE Wireless Communications*, vol. 27, no. 5, pp. 126–132, 2020.

[2] Q. Wu, W. Mei, and R. Zhang, "Safeguarding wireless network with UAVs: a physical layer security perspective," *IEEE Wireless Communications*, vol. 26, no. 5, pp. 12–18, 2019.

[3] J. Lai, R. H. Deng, C. Guan, and J. Weng, "Attribute-based encryption with verifiable outsourced decryption," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 8, pp. 1343–1354, 2013.

[4] E.-H. Bensikaddour, Y. Bentoutou, and N. Taleb, "Satellite image encryption method based on AES-CTR algorithm and GEFFE generator," *International Conference on Recent Advances in Space Technologies*, pp. 247–252, 2017.

[5] Y. Bentoutou, E.-H. Bensikaddour, N. Taleb, and N. Bounoua, "An improved image encryption algorithm for satellite applications," *Advances in Space Research*, vol. 66, no. 1, pp. 176–192, 2020.

[6] S. Jeon and J. P. Choi, "CFB-AES-TURBO: joint encryption and channel coding for secure satellite data transmission," in *ICC 2019-2019 IEEE International Conference on Communications (ICC)*, pp. 1–7, IEEE, Shanghai, China, 2019.

[7] S. J. H. Pirzada, A. Murtaza, L. Jianwei, and T. Xu, "The parallel CMAC authenticated encryption algorithm for satellite communication," in *2019 IEEE 9th International Conference on Electronics Information and Emergency Communication (ICEIEC)*, pp. 1–5, IEEE, Beijing, China, 2019.

[8] S. J. H. Pirzada, M. N. Hasan, Z. W. Memon, M. Haris, T. Xu, and L. Jianwei, "High-throughput optimizations of AES algorithm for satellites," in *2020 International Symposium on Recent Advances in Electrical Engineering & Computer Sciences (RAEE & CS)*, pp. 1–6, IEEE, Islamabad, Pakistan, 2020.

[9] E.-H. Bensikaddour, Y. Bentoutou, and N. Taleb, "Embedded implementation of multispectral satellite image encryption using a chaos-based block cipher," *Journal of King Saud University- Computer and Information Sciences*, vol. 32, no. 1, pp. 50–56, 2020.

[10] S. Zhao, J. Liu, Y. Shen, X. Jiang, and N. Shiratori, "Secure and energy-efficient precoding for MIMO two-way untrusted relay systems," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 3371–3386, 2021.

[11] L. Gyongyosi and S. Imre, "A survey on quantum computing technology," *Computer Science Review*, vol. 31, pp. 51–71, 2019.

[12] M. Bloch and J. Barros, *Physical-layer Security: from Information Theory to Security Engineering*, Cambridge University Press, Cambridge, U.K., 2011.

[13] N. Yang, L. Wang, G. Geraci, M. Elkashlan, and M. Di Renzo, "Safeguarding 5G wireless communication networks using physical layer security," *IEEE Communications Magazine*, vol. 53, no. 4, pp. 20–27, 2015.

[14] R. Bedington, J. M. Arrazola, and A. Ling, "Progress in satellite quantum key distribution," *npj Quantum Information*, vol. 3, Article ID 30, 2017.

[15] S. Pirandola, U. L. Andersen, M. Berta et al., "Advances in quantum cryptography," *Advances in Optics and Photonics*, vol. 12, no. 4, pp. 1012–1236, 2020.

[16] K. Xiao, S. Zhang, K. Michel, and C. Li, "Study of physical layer security in mmwave satellite networks," in *2018 IEEE International Conference on Communications (ICC)*, pp. 1–6, IEEE, Kansas City, MO, USA, 2018.

[17] B. Li, Z. Fei, C. Zhou, and Y. Zhang, "Physical-layer security in space information networks: a survey," *IEEE Internet of Things Journal*, vol. 7, no. 1, pp. 33–52, 2020.

[18] P. Tedeschi, S. Sciancalepore, and R. Di Pietro, "Satellite-based communications security: a survey of threats, solutions, and research challenges," *Computer Networks*, Article ID 109246, 2022.

[19] Z. Qu, G. Zhang, T. Hong, H. Cao, and W. Zhang, "Architecture and network model of time–space uninterrupted space information network," *IEEE Access*, vol. 7, pp. 27677–27688, 2019.

[20] K. Xue, W. Meng, S. Li, D. S. Wei, H. Zhou, and N. Yu, "A secure and efficient access and handover authentication protocol for internet of things in space information networks," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 5485–5499, 2019.

[21] L. Kuang, X. Chen, C. Jiang, H. Zhang, and S. Wu, "Radio resource management in future terrestrial-satellite communication networks," *IEEE Wireless Communications*, vol. 24, no. 5, pp. 81–87, 2017.

[22] J. Shen, C. Wang, S. Ji, T. Zhou, and H. Yang, "Secure emergent data protection scheme for a space-terrestrial integrated network," *IEEE Network*, vol. 33, no. 1, pp. 44–50, 2019.

[23] S. Kansal and M. Mittal, "Performance evaluation of various symmetric encryption algorithms," in *2014 International Conference on Parallel, Distributed and Grid Computing*, pp. 105–109, IEEE, Solan, India, 2014.

[24] A. Ostad-Sharif, D. Abbasinezhad-Mood, and M. Nikooghadam, "Efficient utilization of elliptic curve cryptography in design of a three-factor authentication protocol for satellite communications," *Computer Communications*, vol. 147, pp. 85–97, 2019.

[25] G. Caparra, S. Ceccato, S. Sturaro, and N. Laurenti, "A key management architecture for GNSS open service navigation message authentication," in *2017 European Navigation Conference (ENC)*, pp. 287–297, IEEE, Lausanne, Switzerland, 2017.

[26] I. Altaf, M. A. Saleem, K. Mahmood, S. Kumari, P. Chaudhary, and C.-M. Chen, "Agreement and authentication scheme for satellite-communication systems," *IEEE Access*, vol. 8, pp. 46278–46287, 2020.

[27] M. Qi, J. Chen, and Y. Chen, "A secure authentication with key agreement scheme using ECC for satellite communication

systems," *International Journal of Satellite Communications and Networking*, vol. 37, no. 3, pp. 234–244, 2019.

[28] S.-K. Liao, W.-Q. Cai, W.-Y. Liu et al., "Satellite-to-ground quantum key distribution," *Nature*, vol. 549, pp. 43–47, 2017.

[29] S.-K. Liao, W.-Q. Cai, J. Handsteiner et al., "Satellite-relayed intercontinental quantum network," *Physical Review Letters*, vol. 120, no. 3, 2018.

[30] H. Dai, Q. Shen, C.-Z. Wang et al., "Towards satellite-based quantum-secure time transfer," *Nature Physics*, vol. 16, pp. 848–852, 2020.

[31] J. Yin, Y.-H. Li, S.-K. Liao et al., "Entanglement-based secure quantum cryptography over 1,120 kilometres," *Nature*, vol. 582, pp. 501–505, 2020.

[32] C. C.-W. Lim, F. Xu, J.-W. Pan, and A. Ekert, "Security analysis of quantum key distribution with small block length and its application to quantum space communications," *Physical Review Letters*, vol. 126, no. 10, Article ID 100501, 2021.

[33] C. Agnesi, M. Avesani, A. Stanco, P. Villoresi, and G. Vallone, "All-fiber self-compensating polarization encoder for quantum key distribution," *Optics Letters*, vol. 44, no. 10, pp. 2398–2401, 2019.

[34] S. P. Kish, E. Villaseñor, R. Malaney, K. A. Mudge, and K. J. Grant, "Feasibility assessment for practical continuous variable quantum key distribution over the satellite-to-Earth channel," *Quantum Engineering*, vol. 2, no. 3, Article ID e50, 2020.

[35] Z. Pan and I. B. Djordjevic, "Security of satellite-based CV-QKD under realistic assumptions," in *2020 22nd International Conference on Transparent Optical Networks (ICTON)*, pp. 1–4, IEEE, Bari, Italy, 2020.

[36] N. Alshaer, T. Ismail, and M. E. Nasr, "Performance evaluation and security analysis of ground-to-satellite FSO system with CV-QKD protocol," *IET Communications*, vol. 14, no. 10, pp. 1534–1542, 2020.

[37] D. Dequal, L. Trigo Vidarte, V. Roman Rodriguez et al., "Feasibility of satellite-to-ground continuous-variable quantum key distribution," *npj Quantum Information*, vol. 7, Article ID 3, 2021.

[38] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: a survey," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 3, pp. 1550–1573, 2014.

[39] Y. Xiao, J. Liu, Y. Shen, X. Jiang, and N. Shiratori, "Secure communication in non-geostationary orbit satellite systems: a physical layer security perspective," *IEEE Access*, vol. 7, pp. 3371–3382, 2019.

[40] Z. Yin, M. Jia, W. Wang et al., "Secrecy rate analysis of satellite communications with frequency domain NOMA," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 12, pp. 11847–11858, 2019.

[41] W. Cao, Y. Zou, Z. Yang, and J. Zhu, "Secrecy outage probability of hybrid satellite-terrestrial relay networks," in *GLOBECOM 2017-2017 IEEE Global Communications Conference*, pp. 1–5, IEEE, Singapore, 2017.

[42] S. Yan, X. Wang, Z. Li, B. Li, and Z. Fei, "Cooperative jamming for physical layer security in hybrid satellite terrestrial relay networks," *China Communications*, vol. 16, no. 12, pp. 154–164, 2019.

[43] Y. Yan, B. Zhang, D. Guo, S. Li, H. Niu, and X. Wang, "Joint beamforming and jamming design for secure cooperative hybrid satellite-terrestrial relay network," in *2016 25th Wireless and Optical Communication Conference (WOCC)*, pp. 1–5, IEEE, Chengdu, 2016.

[44] Z. Lin, M. Lin, J. Ouyang, W.-P. Zhu, A. D. Panagopoulos, and M.-S. Alouini, "Robust secure beamforming for multibeam satellite communication systems," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 6, pp. 6202–6206, 2019.

[45] Z. Lin, K. An, H. Niu et al., "SLNR-based secure energy efficient beamforming in multibeam satellite systems," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 59, no. 2, pp. 2085–2088, 2023.

[46] H.-M. Wang, Q. Yin, and X.-G. Xia, "Distributed beamforming for physical-layer security of two-way relay networks," *IEEE Transactions on Signal Processing*, vol. 60, no. 7, pp. 3532–3545, 2012.

[47] C. Wang and H.-M. Wang, "Robust joint beamforming and jamming for secure AF networks: low-complexity design," *IEEE Transactions on Vehicular Technology*, vol. 64, no. 5, pp. 2192–2198, 2015.

[48] S. Hong, C. Pan, H. Ren, K. Wang, and A. Nallanathan, "Artificial-noise-aided secure MIMO wireless communications via intelligent reflecting surface," *IEEE Transactions on Communications*, vol. 68, no. 12, pp. 7851–7866, 2020.

[49] D. Bepari, S. Mondal, A. Chandra et al., "A survey on applications of cache-aided NOMA," *IEEE Communications Surveys & Tutorials*, vol. 25, no. 3, pp. 1571–1603, 2023.

[50] L. Zhu, Z. Xiao, X.-G. Xia, and D. O. Wu, "Millimeter-wave communications with non-orthogonal multiple access for B5G/6G," *IEEE Access*, vol. 7, pp. 116123–116132, 2019.

[51] M. Lin, Z. Lin, W.-P. Zhu, and J.-B. Wang, "Joint beamforming for secure communication in cognitive satellite terrestrial networks," *IEEE Journal on Selected Areas in Communications*, vol. 36, no. 5, pp. 1017–1029, 2018.

[52] H. Li, S. Zhao, Y. Li, and C. Peng, "Sum secrecy rate maximization in NOMA-based cognitive satellite-terrestrial network," *IEEE Wireless Communications Letters*, vol. 10, no. 10, pp. 2230–2234, 2021.

[53] J. Du, C. Jiang, H. Zhang, X. Wang, Y. Ren, and M. Debbah, "Secure satellite-terrestrial transmission over incumbent terrestrial networks via cooperative beamforming," *IEEE Journal on Selected Areas in Communications*, vol. 36, no. 7, pp. 1367–1382, 2018.

[54] Z. Lin, M. Lin, Y. Huang, T. De Cola, and W.-P. Zhu, "Robust multi-objective beamforming for integrated satellite and high altitude platform network with imperfect channel state information," *IEEE Transactions on Signal Processing*, vol. 67, no. 24, pp. 6384–6396, 2019.

[55] Q. Gao, M. Jia, Q. Guo, X. Gu, and L. Hanzo, "Jointly optimized beamforming and power allocation for full-duplex cell-free NOMA in space-ground integrated networks," *IEEE Transactions on Communications*, vol. 71, no. 5, pp. 2816–2830, 2023.

[56] G. Cui, Q. Zhu, L. Xu, and W. Wang, "Secure beamforming and jamming for multibeam satellite systems with correlated wiretap channels," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 10, pp. 12348–12353, 2020.

[57] Z. Lin, M. Lin, B. Champagne, W.-P. Zhu, and N. Al-Dhahir, "Secure and energy efficient transmission for RSMA-based cognitive satellite-terrestrial networks," *IEEE Wireless Communications Letters*, vol. 10, no. 2, pp. 251–255, 2021.

[58] V. Bankey and P. K. Upadhyay, "On the physical layer security for land mobile satellite systems," in *Modelling, Simulation and Intelligent Computing*, N. Goel, S. Hasan, and V. Kalaichelvi, Eds., pp. 218–226, Springer, Singapore, 2020.

[59] M. Bouabdellah and F. E. Bouanani, "A PHY layer security of a jamming-based underlay cognitive satellite-terrestrial

network," *IEEE Transactions on Cognitive Communications and Networking*, vol. 7, no. 4, pp. 1266–1279, 2021.

[60] K. Guo, K. An, B. Zhang, Y. Huang, and D. Guo, "Physical layer security for hybrid satellite terrestrial relay networks with joint relay selection and user scheduling," *IEEE Access*, vol. 6, pp. 55815–55827, 2018.

[61] V. Bankey and P. K. Upadhyay, "Physical layer security of multiuser multirelay hybrid satellite-terrestrial relay networks," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 3, pp. 2488–2501, 2019.

[62] J. Li, S. Han, X. Tai, C. Gao, and Q. Zhang, "Physical layer security enhancement for satellite communication among similar channels: relay selection and power allocation," *IEEE Systems Journal*, vol. 14, no. 1, pp. 433–444, 2020.

[63] K. Guo, X. Li, M. Alazab, R. H. Jhaveri, and K. An, "Integrated satellite multiple two-way relay networks: secrecy performance under multiple eves and vehicles with non-ideal hardware," *IEEE Transactions on Intelligent Vehicles*, vol. 8, no. 2, pp. 1307–1318, 2023.

[64] D. Wang, B. Bai, W. Zhao, and Z. Han, "A survey of optimization approaches for wireless physical layer security," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1878–1911, 2019.

[65] N. Xie, Z. Li, and H. Tan, "A survey of physical-layer authentication in wireless communications," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 1, pp. 282–310, 2021.

[66] X. Du, D. Shan, K. Zeng, and L. Huie, "Physical layer challenge-response authentication in wireless networks with relay," in *IEEE INFOCOM 2014-IEEE Conference on Computer Communications*, pp. 1276–1284, IEEE, Toronto, ON, Canada, 2014.

[67] H. Tan, N. Xie, J. Lu, and D. Niyato, "Generalized tag-based physical-layer authentication under frequency selective fading channels," *IEEE Transactions on Communications*, vol. 71, no. 5, pp. 2876–2890, 2023.

[68] L. Xiao, X. Lu, T. Xu, W. Zhuang, and H. Dai, "Reinforcement learning-based physical-layer authentication for controller area networks," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 2535–2547, 2021.

[69] N. Xie, Q. Zhang, J. Chen, and H. Tan, "Privacy-preserving physical-layer authentication for non-orthogonal multiple access systems," *IEEE Journal on Selected Areas in Communications*, vol. 40, no. 4, pp. 1371–1385, 2022.

[70] Q.-Y. Fu, Y.-H. Feng, H.-M. Wang, and P. Liu, "Initial satellite access authentication based on Doppler frequency shift," *IEEE Wireless Communications Letters*, vol. 10, no. 3, pp. 498–502, 2021.

[71] O. A. Topal and G. K. Kurt, "Physical layer authentication for LEO satellite constellations," in *2022 IEEE Wireless Communications and Networking Conference (WCNC)*, pp. 1952–1957, IEEE, Austin, TX, USA, 2022.

[72] M. Abdrabou and T. A. Gulliver, "Authentication for satellite communication systems using physical characteristics," *IEEE Open Journal of Vehicular Technology*, vol. 4, pp. 48–60, 2023.

[73] G. Oligeri, S. Sciancalepore, S. Raponi, and R. Di Pietro, "PAST-AI: physical-layer authentication of satellite transmitters via deep learning," *IEEE Transactions on Information Forensics and Security*, vol. 18, pp. 274–289, 2023.

[74] G. Oligeri, S. Sciancalepore, and R. 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*, pp. 42–52, Association for Computing Machinery, New York, NY, USA, 2020.

[75] B. Dirks, I. Ferrario, A. Le Pera et al., "GEOQKD: quantum key distribution from a geostationary satellite," *International Conference on Space Optics—ICSO 2020*, vol. 11852, Article ID 118520J, 2021.

[76] A. Ntanos, N. K. Lyras, D. Zavitsanos, G. Giannoulis, A. D. Panagopoulos, and H. Avramopoulos, "LEO satellites constellation-to-ground QKD links: Greek quantum communication infrastructure paradigm," *Photonics*, vol. 8, no. 12, Article ID 544, 2021.

[77] N. S. Agency, "Quantum key distribution and quantum cryptography," 2020, [Online]. Available: https://www.nsa.gov/Cybersecurity/Quantum-Key-Distribution-QKD-and-Quantum-Cryptography-QC.

[78] S. Xu, J. Liu, Y. Cao, J. Li, and Y. Zhang, "Intelligent reflecting surface enabled secure cooperative transmission for satellite-terrestrial integrated networks," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 2, pp. 2007–2011, 2021.

[79] Q. T. Ngo, K. T. Phan, A. Mahmood, and W. Xiang, "Physical layer security in IRS-assisted cache-enabled satellite communication networks," in *IEEE Transactions on Green Communications and Networking*, IEEE, 2023.

[80] Z. Lin, H. Niu, K. An et al., "Refracting RIS-aided hybrid satellite-terrestrial relay networks: joint beamforming design and optimization," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 58, no. 4, pp. 3717–3724, 2022.

[81] S. Jeon, J. Kwak, and J. P. Choi, "Cross-layer encryption of CFB-AES-TURBO for advanced satellite data transmission security," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 58, no. 3, pp. 2192–2205, 2022.