Covert Communications in Satellite Internet: A Survey

Zewei Guo[1], Ji He[2*], Yuanyu Zhang[3*], Shuangrui Zhao[4], Yulong Shen[5], and Xiaohong Jiang[6]
[1,2,3,4,5]School of Computer Science and Technology, Xidian University, Xi'an 710071, China
[2]Guangzhou Institute of technology, Xidian University, Guangzhou, 510555, China
[1,2,3,4,5]Shaanxi Key Laboratory of Network and System Security, Xidian University, Xi'an, 710071, China
[6]School of Systems Information Science, Future University Hakodate, Hakodate, Hokkaido, 041-8655, Japan

The broadcast nature of wireless channels and broad coverage brings significant challenges to the security of Satellite Internet. Recently, a new security paradigm named covert communication aims to enhance security by hiding the transmission process and has received great research attention. Various covert transmission schemes were proposed to achieve covertness for different network scenarios. Motivated by the importance of promising security techniques, this survey provides a comprehensive overview of the recent works on covert communication in Satellite Internet for the first time. We first introduce the basic architecture and characteristics of Satellite Internet, as well as its access security challenges. Then, an in-depth overview of covert communication technologies is provided with an emphasis, which is divided into two categories, i.e., traditional ones and information theory-based ones. Finally, several key challenges and future research directions on covert communication are presented.

***Index Terms*—Satellite Internet, covert communication, spread spectrum, artificial noise, cooperative relaying.**

I. Introduction

Satellite Internet is one of the most important technologies for accelerating the development of the sixth-generation (6G) networks, which can provide seamless network coverage and real-time transmission worldwide. The satellite-terrestrial link is capable of delivering download speeds in excess of 100Mbps while transmitting latency below 50ms [1]. Satellite base stations can use multiple access technologies to provide Internet access services for a large number of users because of their vast footprints. In addition, Satellite Internet also plays a crucial role in critical communications and emergency rescue. These undeniable benefits have extensively promoted the commercial process of Satellite Internet. According to a dedicated research report by Market Research Future (MRFR), "Satellite Internet Market Statistics-2030", the global market size of Satellite Internet was valued at 2.93 billion in 2020 and is projected to reach 18.59 billion by 2030, growing at a Compound Annual Growth Rate (CAGR) of 20.4% from 2021 to 2030 [2]. Thus, the major countries and technology companies have been in deployment new large constellations to implement global connectivity ecosystem, e.g., Starlink from SpaceX, OneWeb from the UK, HongYan from China. As of Jan. 2022, SpaceX has launched 2,042 Starlink satellites, of which 1,495 are in orbit, providing Internet access to over 40,0000 subscribers [3], [4].

Due to the distinctive worldwide openness and complex network structure, Satellite Internet is more vulnerable to security threats than the terrestrial Internet. Although the existing cryptography and physical layer security (PLS) technologies have the ability to secure the content of transmitted information, malicious adversaries can still detect the communication behavior and attack transmission links, such that the destination cannot receive the message without error. Besides, frequent handover and severe attenuation of satellite-terrestrial channels would brings major challenges. To provide a strong security guarantee for wireless transmissions, covert communication, also known as low probability of detection (LPD) communication, was been widely investigated. Its main idea is to artificially create through signal technologies or utilize background noise to confuse the adversary, and then conduct covert transmission opportunely [5], [6]. By applying covert communication technology to Satellite Internet, a high level of security and privacy can be attained. In particular, using covert communication technology to ensure the covertness of Satellite Internet uplink and downlink can enable the transmission of secret information across international borders without being obstructed by network censorship.

Depending on the adopted security techniques, the existing works of covert communication in Satellite Internet can be divided into two categories, i.e., traditional and information theory-based covert communications. Traditional covert communications include time hopping, frequency hopping, and Weighted Fractional Fourier Transform (WFRFT) techniques. By designing the waveform of the transmitted signal, traditional covert communication techniques suppress the power spectral density of the transmission and complicate the time-frequency characteristics of the signal to provide both covert communication capability and anti-interference ability. Information theory-based covert communications include artificial noise assist, transmission power control and intelligent reflecting surfaces techniques. By increasing interference dynamics and reducing signal leakage, it can provide randomness of received power and a low signal-to-noise ratio for wardens. The fundamental principle of these techniques is to impair the warden's ability to discern between the transmitted signal and the noise.

In the last few years, there are excellent surveys in satellite communications, which provide comprehensive overviews and insightful comments to understand the application paradigms, technology status, and major challenges in this field. Cioni

Manuscript received September 13, 2022; revised October 31, 2022. Corresponding authors: Ji He and Yuanyu Zhang (email: garyhej1991@gmail.com; yyuzhang@xidian.edu.cn).

et al. in [7] described the potential application that satellite systems may have in mMTC services. Kodheli *et al.* discussed the state-of-the-art in satellite communications, and highlighted the promising research topics in [8]. Potential AI-based solutions for several challenges in Satellite Communication are discussed in [9]. Li *et al.* reviewed the current research progress of satellite communications in the context of PLS in [10], [11]. From the view of cyber security, Manulis *et al.* in [12] reported the motivations and characteristics of adversarial threats to the space segment, ground segment, and user segment of Satellite Internet. Recently, Tedeschi *et al.* in [13] elaborated on the application of PLS and cryptography methods on addressing the potential security issues for satellite-based communication.

The aforementioned literature has laid the foundation for understanding the development of satellite communication, however, as far as we know, there is no overview of the covert communication in Satellite Internet. Therefore, the goal of this paper is to comprehensively survey the state-of-the-art research of covert transmission, and discuss the major security challenges. First, we specify the basic architecture of Satellite Internet, including space-based network, air-based network, and terrestrial-based network, and some unique characteristics. Second, we survey the state-of-the-art of covert communication methods from two categories, i.e, traditional covert communication and information-based covert communication. Finally, we identify the potential physical-layer and upper-layer security approaches, and discuss the detection methods to counter covert communications.

We organize the remainder of this article as follows. In Section II, we present the system architecture and features of the Satellite Internet. In Section III, we introduce traditional satellite covert communication technologies. In Section IV, we introduce research on information theory-based covert communication technologies. In Section V, we provide a number of future research directions. Concluding remarks are provided in Section VI.

II. Background

In this section, we introduce the basic architecture and unique features of Satellite Internet.

A. Architecture of Satellite Internet

From space to ground, the architecture of Satellite Internet mainly includes three parts, i.e., space-based networks, air-based networks, and terrestrial-based networks, as shown in Fig. 1. The space-based network is one of the most critical components of Satellite Internet, which utilizes satellite-satellite optical links and satellite-air/terrestrial microwave links to provide Internet access services worldwide. This part consists of satellites for various purposes, e.g., earth observation satellites, communication satellites, and astronomical satellites. According to the different orbital altitudes (i.e., the distance from the satellite to earth surface), these satellites can be generally divided into three categories, i.e., geostationary orbit (GEO) satellites, medium earth orbit (MEO) satellites, and low earth orbit (LEO) satellites. Their respective orbit

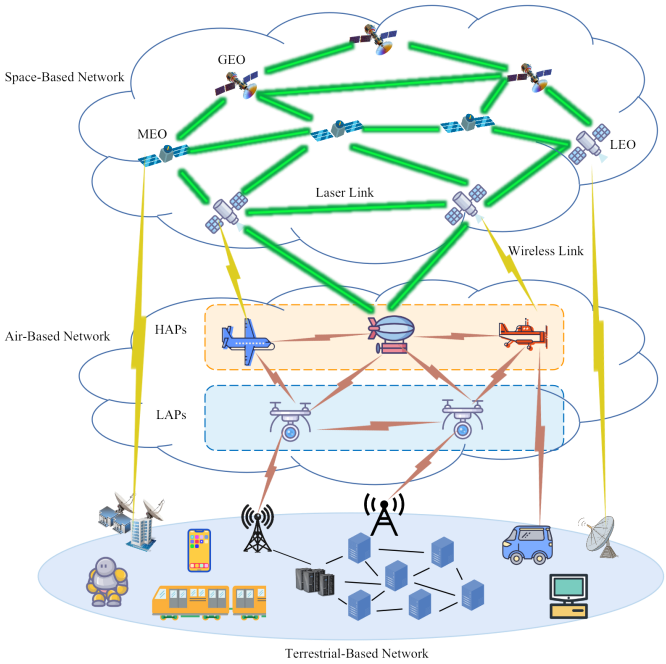


Fig. 1. Illustration of the Architecture of Satellite Internet

altitude ranges are $35,786$ km, from $2,000$ to $25,000$ km, and from 400 to $2,000$ km, respectively [10]. Their altitude ranges are directly related to the services provided by satellites in space-based networks. Particularly, the higher orbital altitude results in greater earth coverage area and higher latency. Due to the broadest earth coverage area and geostationary characteristics, GEO satellites mainly provide satellite telephone and radio broadcasting services, such as MSAT and Inmarsat systems. MEO satellites are usually used by global positioning systems (GPS) and other satellite communication systems (e.g., O3B), since they can hit a trade-off between satellite coverage and latency. LEO satellites, which have received great attention recently, are mainly adopted for mobile Internet because of the advantages of low latency, high throughput, and low cost.

Air-based networks can be regarded as an extension of the space-based network with lower latency and clearer channels. It consists of a wide variety of air platforms, which can be divided into High Altitude Platforms (HAPs) and Low Altitude Platforms (LAPs) based on the operating altitude. The HAPs are composed of airships, aircraft, and balloons located in the stratosphere between $17-22$ km [14]. Particularly, HAPs can be equipped with heterogeneous radio interferences and serve as a bond between space-based and terrestrial-based networks. On the one hand, because of the little atmosphere effect, the communication between HAPs and space-based networks can use optical links to achieve wider bandwidth. On the other hand, the communication between HAPs and terrestrial networks has a shorter path than the orbit height of satellites, thereby achieving an excellent quality of service (QoS). The LAPS is mainly composed of unmanned aerial vehicles (UAVs) with a working altitude of $0-4$ km [8]. Taking advantage of UAVs' rapid and flexible deployment,

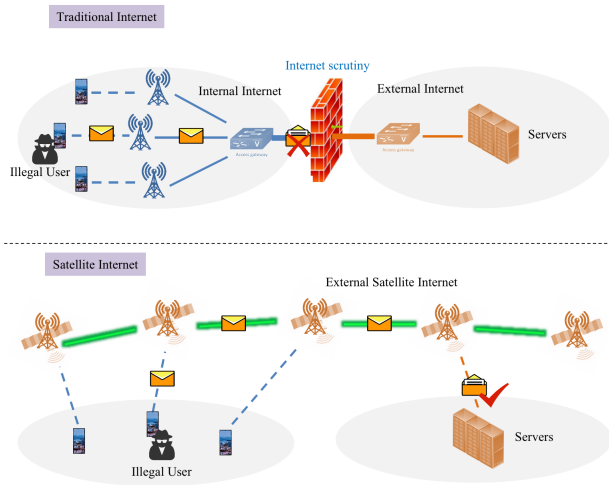


Fig. 2. Channel Openness of Satellite Internet

LAPs can provide temporary communication and network access services for the field of emergency communications.

In the terrestrial-based network, macro cells and small cells can form a heterogeneous radio access network to serve different industries, such as IIoT, smart city, automated driving, and so forth. Furthermore, the terrestrial network incorporates the space ground station system for detecting the satellite's location and receiving satellite remote sensing photos. Owing to its vast storage capacity and computer resource, the terrestrial network can process data transferred from other networks to balance the computing pressure of the entire Satellite Internet.

B. Features of Satellite Internet

Highly open channel: Compared with the traditional Internet, Satellite Internet has longer transmission distances and broader coverage. Therefore, its channel is more open and more vulnerable to network attacks such as interference, eavesdropping, and wireless intrusion, which brings significant challenges to the transmission security. Furthermore, the illegal users can utilize the satellite links to transmit sensitive information to the hostile territory without regional restriction, which breaks the traditional Internet scrutiny scheme shown as Fig. 2.

Mix-up of friend and foe in space: Due to the scarcity of orbital and spectrum resources, satellite access to these resources follows a "first-come, first-served" basis, which is contained in ITU's Radio Regulations [15]. Thus, major countries and commercial companies in the world are actively deploying large-scale low-orbit satellite constellations to seize scarce orbit and spectrum resources, resulting in the mixture of enemy and friendly satellites in space. As shown in Fig. 3, when conducting satellite communications, enemy satellites may use the satellites between the communication link or change orbits to a closer location for eavesdropping or monitoring. This will bring serious security challenges to the Satellite Internet.

Predictability of Satellite Internet Topology: Unlike terrestrial base stations, satellite base stations break geographical restrictions and fly around the earth at high speed. Thus, the

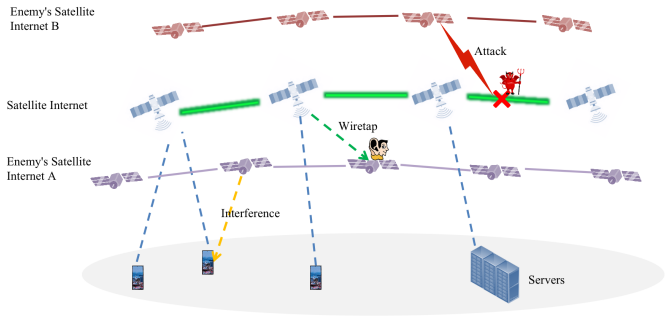


Fig. 3. Enemy and Friendly Satellites Mixed in Space

topologies of Satellite Internet change more frequently than the terrestrial Internet. However, note that before the constellation of satellites took shape, the FCC requests that the satellite operators must be mandated to some design parameters. So, the adversaries can deduce the design detail of the interconnections and predict network topology with high accuracy. In contrast, the topology of terrestrial networks is more concealed and obfuscated. This allows malicious nodes to attack critical links or satellites through predictable topologies. Furthermore, due to the fixed trajectory of satellites, malicious nodes can predict the trajectory of the satellite and prepare for attack or eavesdropping in advance as Fig. 4, which will bring serious security challenge to Satellite Internet.

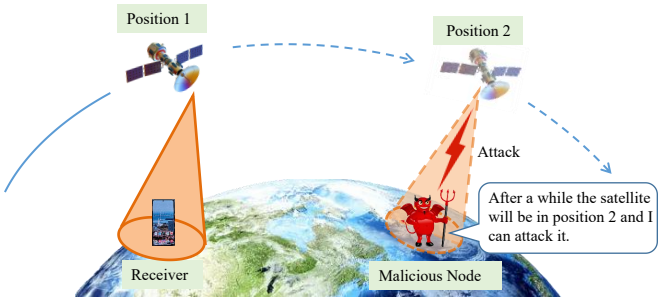


Fig. 4. Predictability of Satellite Internet Topology

These distinctive characteristics of Satellite Internet bring serious challenges to the security techniques based on traditional cryptography and PLS, which need to be tackled by utilizing innovative technology. Fortunately, the emerging covert communication technology can provide high-level security and privacy for satellite communications. It can enable a higher level of security by hiding the communication process. In the following sections, we summarize the current studies on covert communication in Satellite Internet.

III. Traditional Covert Communication Technologies in Satellite Internet

The core idea of traditional covert communication technologies is to design the waveform of the transmitted signal to reduce the intercept and the detection probability, which was first used in World War military communications [16]. According to the different waveform design transform domains, we divided these traditional technologies into the following three categories to introduce them.

A. Techniques Based on Time Domain Transformation

Time hopping spread spectrum (THSS) is the most prominent technique in the time domain of signals, which is widely utilized in time division multiple access (TDMA) communications [17]–[19]. In the THSS, the sender makes the signal jump along with the pseudo-code sequence on the time axis, and the receiver receives the signals synchronously with the same jump law. In this way, it can effectively prevent information leakage and provide an LPD capability. In 1985, Polydoros and Weber in [20] analyzed the detection performance of wideband detectors for THSS waveforms in the presence of additive white Gaussian noise (AWGN). Based on the results of [20], Bharadwaj and Townsend in [21] evaluated the covertness of the time-hopping impulse radio system under multi-radiometer detection and derived the detection probability of single- and multi-user scenarios. Moreover, Yu and Yao in [22] further investigated the low probability of intercept (LPI) performance of the time-hopping ultra-wideband system, where the single detector and multiple detectors are considered.

B. Techniques Based on Frequency Domain Transformation

The current covert communication techniques based on frequency domain transformation can be mainly divided into the frequency hopping spread spectrum (FHSS) and direct sequence spread spectrum (DSSS).

Frequency hopping spread spectrum: FHSS is one of the most commonly used spread spectrum techniques for wireless communication, which has been implemented successfully in many satellites and military communication systems [16], [23]–[26]. Its core idea is to use the pseudo-random sequence to make the carrier frequency of the transmitted signal hops randomly over a wider frequency band. Based on Neyman-Pearson detection theory, Beaulieu *et al.* proposed coherent and noncoherent interception receiver structures for FHSS signals detection, and derived formulas that relate the probability of detection and false alarm in [27]. Then, Lee *et al.* in [28] proposed a dirty-template-based detection scheme to detect fast frequency-hopping signal, which outperforms the autocorrelation-based detection scheme when the hopping period is short. To improve the covert performance of the communication signals, Ning *et al.* in [29] proposed a novel frequency-hopping sequence design scheme, which achieves the lowest probability of detection under the bit error rate constraint. In this scheme, an optimal probability vector was calculated based on the estimated bit error rate (BER) and probability of detection (PD) of each channel, and then a frequency-hopping sequence is generated by mapping the probability vector to a sequence.

Direct sequence spread spectrum: As a widely used method for military communications during World War II [30]–[34], the fundamental philosophy behind the concept of Direct Sequence Spread Spectrum (DSSS) is to spread the signal in the frequency domain to suppress the power spectral density of the transmission under the noise floor. In this way, the information is concealed in the noise and the wardens cannot detect it. To improve the LPI properties of a DSSS system under the detection of squaring detector and delay-and-multiply detector, Wik and Lindblad proposed a novel spreading codes generation method in [35]. The method generated the spreading code at a very high rate and processed it through a lowpass filter with a low cutoff frequency, so as to give the spread code multilevel amplitudes and remove the spectral lines of DSSS signals. Nowak *et al.* in [36] utilized zinc waveforms as a spreading signal to improve the transmit and covertness performance of DSSS systems, where temporal-spectral characteristics of the novel DSSS systems and the covert nature of the transmitted signal were presented. The results demonstrated that the covertness of zinc waveform signals is better than typical pseudo-noise (PN) signals.

C. Techniques Based on Time-Frequency Domain Transformation

Weighted Fractional Fourier Transform (WFRFT) is a novel time-frequency design method that was first proposed by Shih in [37]. It enables the bit energy of the modulated signal to exhibit a uniform and symmetrical distribution in the time-frequency domain and the signal constellation diagram to exhibit characteristics such as rotation and blurring under varied modulation parameters [38]. In this way, WFRFT provides covert transmission capabilities by making it harder for the warden to detect the communication behavior of the transmitter accurately. Based on the result in [37], the authors in [39]–[42] further proposed multi-fractional and multi-parameters WFRFT schemes which improve the security and transmit performance of the communication. Then, Mei *et al.* in [43] proposed a novel covert communication scheme based on waveform overlay with WFRFT signals, which boosted the capacity and security of the covert communication system without additional noise. By setting the appropriate WFRFT parameters, the constellation of modulated signals appears a quasi-Gaussian probability distribution, which makes it difficult for the wardens to detect and recognize. In order to improve the security performance and anti-interception of the satellite Multiple Input Multiple Output (MIMO) communication system, Zhai *et al.* in [44] proposed a multiple-layer WFRFT scheme in which each transmit (receive) antenna has unique WFRFT modulation (demodulation) parameters.

IV. Covert Communication Technologies Based on Information Theory in Satellite Internet

As we summarized in the previous section, traditional technologies can already realize covert communication on Satellite Internet. However, their covert communication performance, in terms of the amount of information that can be secretly transmitted under certain covert constraints, is unknown. Based on the information theory, Bash *et al.* [45] theoretically proved that the limit of covert communication under the AWGN channel obeys the Square Root Law, while using n channels, at most $\mathcal{O}(\sqrt{n})$ bits of information can be transmitted covertly. Then, the authors in [46]–[48] extend the square root law to Binary Symmetric Channel and Discrete Memoryless Channel, respectively. In [49], Goeckel *et al.* further prove that legal nodes can covertly transmit $\mathcal{O}(n)$ bits of information under

n channel used when the warden cannot obtain its own exact noise power. To obtain a positive covert rate, numerous information theory-based covert communication technologies have been investigated on this basis. Accordingly, we classify the present covert communication technologies as follows.

A. Increasing signal uncertainty

Artificial-noise-assist techniques: The fundamental concept of artificial-noise-assist techniques is to transmit random AN to wardens in order to increase their uncertainty. Based on the result in [49], Sobers *et al.* demonstrated that the covert communication system can remain covert with a transmit power that does not decrease with blocklength, even if the warden employs an optimal detector [50]. Then, Soltani *et al.* further proved that the covert capacity of the covert communication system, which has multiple cooperative jamming nodes, can still reach $\mathcal{O}(min\{m^{\frac{\gamma}{2}}\sqrt{n}, n\})$ when the warden can obtain the statistical information of environmental noise [51]. To create uncertainty at the warden, Shahzad *et al.* investigated a covert communication system in which covertness was achieved by the use of a full-duplex receiver [52]. In this work, the optimal choice of AN power range and the optimal transmission probability of covert information were derived. In addition, Huang *et al.* proposed a scheme that enabled a transmitter to covertly communicate with multiple receivers by sending AN signals through a friendly jammer [53]. Li *et al.* further analyzed the covert performance of the UAV jamming node-assisted cognitive radio network and proposed a model-driven generative adversarial network optimization framework to jointly optimize the UAV flight trajectory and transmit power to maximize the covert communication rate [54]. Recently, Wang *et al.* investigated the covertness performance of Beidou navigation satellite system with a terrestrial jammer [55].

Transmit power control techniques: Similar to AN-assisted technologies, the core concept underlying transmit power control techniques is to enhance the randomness of transmit power or design transmit power to reduce the probability of warden detection. Yan *et al.* first proposed the uniformly distributed random transmit power scheme to improve the covertness performance of the delay-intolerant covert communication system [56]. In order to enhance the covert communication performance of UAV systems, Zhou *et al.* proposed a jointly optimize scheme to design the UAV's trajectory and transmit power to maximize the average covert transmission rate from the UAV to the ground user [57]. Then, Tao *et al.* analyzed the covertness performance of a downlink Nonorthogonal multiple access (NOMA) system with uniformly distributed random transmit power and derived the detection error probability of warden and the connect outage probability of users [58]. Based on the result in [58], Ma *et al.* proposed a channel inversion power control scheme to facilitate the hidden of the transmitter from the warden [59]. Recently, Kang *et al.* further analyzed the covertness performance of NOMA in Satellite Internet of things with uniformly distributed random transmit power [60].

B. Weakening signal leakage

Cooperative relaying techniques: Cooperative relaying techniques can reduce the access distance of each hop in order to keep the lower transmit power, hence reducing the probability of detection by wardens. Sheikholeslami *et al.* first proposed a Multi-Hop scheme to improve the performance of covert communication, where multiple collaborating wardens were considered [61]. Based on the result in [61], Wang *et al.* proposed a multi-hop relaying strategy for a pair of terrestrial nodes to defend against the detection of a UAV warden and then optimized the throughput by carefully designing the parameters of the multi-hop network [62]. Then, Wu *et al.* proposed a two-way relay scheme to covertly exchange information between two sources [63]. Gao *et al.* [64] analyzed the covert performance of relay-assisted Internet of Things (IoT) systems with a source-destination pair, a passive warden, and multiple relays, where random selection and superior-link selection schemes were considered. In comparison with the scheme in [63], Sun *et al.* proposed a full-duplex relaying scheme to further improve the covertness performance of systems and investigated the fundamental covert rate performance, where the different relay work modes are considered, including the FD mode and the half-duplex (HD) mode [65]. Jiang *et al.* investigated the resource allocation problem of UAV network covert communication in multi-user scenarios, considering the location uncertainty of the warden, a robust resource allocation and UAV trajectory optimization problem with worst-case covertness constraint is then formulated to maximize the average covert rate [66]. To improve the covert transmission rate of UAV-aided covert communication systems, Chen *et al.* in [67] proposed a multi-antenna jammer scheme against several randomly distributed wardens on the ground. Du *et al.* in [68] investigated a jammer-aided UAV covert communication system, which aims to maximize the user's covert rate with optimized transmit and jamming power, where the UAV is equipped with multi antennas to serve multi-users simultaneously. To improve the covertness of satellite-terrestrial transmission, Wu *et al.* in [69] proposed a relay selection scheme for the integrated satellite multiple terrestrial relay network (ISMTRN), where the closed-form error detection probability and average covert communication rate are derived.

Multiple antennas techniques: Multiple-antenna techniques can reduce signal leakage through directional transmission in order to enhance the covertness performance of wireless channels. This can be accomplished via means of beamforming, which designs the phase and amplitude of the signals on each antenna such that the signal is constructively in the direction of the receiver and destructively in other directions. Zheng et al. [70] first investigated the performance of multi-antenna-aided covert communications, where centralized and distributed antenna systems (CAS/DAS) were considered. Different from [70], Yang *et al.* exploited a full-duplex (FD) multi-antenna receiver to achieve covert communication and derived the detection limit of warden [71]. Then, Shahzad *et al.* further investigated the performance of covert communication in the presence of a multi-antenna warden. Under the assumption of

quasi-static wireless fading channels, the effect of increasing the number of antennas employed at the adversary on the achievable throughput of covert communication was analyzed in this work [72]. Combined with artificial noise technology, Shmuel *et al.* proposed a multi-antenna jamming scheme to achieve covert communication between two users [73]. Jamali and Mahdavifar investigated covert communication over millimeter-wave (mmWave) frequencies [74]. In this work, the transmitter employed two independent antenna arrays, with one array forming a beam for data transmission to the receiver and the other emitting a beam toward the warden as a jamming signal. Recently, Xu *et al.* in [75] investigated the covert downlink transmission in the mmWave massive MIMO satellite system and derived the covert transmission rate in accordance with the total variance (TV) distance covert metric.

IRS-Assisted techniques: As one of the key technologies to realize the next generation of mobile communication, Intelligent Reflecting Surfaces (IRS) has developed rapidly in recent years. Its core idea is to use a smartly controlled metasurface to reshape undesirable propagation conditions that might divulge secret messages. Si *et al.* utilized IRS to realize covert communication for the first time [76]. This work formulated a joint transmit beamforming and IRS phase shift optimization problem to maximize the covert transmission rate subject to a covertness constraint. Then, Wu *et al.* jointly designed the transmit power and the IRS reflection beamforming, including both its phase shifts and amplitudes, to minimize the transmission outage probability subject to a covertness constraint [77]. Wang *et al.* further investigated the IRS-aided multi-antenna covert communications [78]. In particular, with the help of an IRS, a favorable communication environment have established via controllable intelligent signal reflection, which facilitates the covert communication between a multi-antenna transmitter and a legitimate full-duplex receiver in the existence of a watchful warden. Recently, Zhou *et al.* further examined the performance gain achieved by deploying an IRS in covert communications [79]. To enhance covert communication performance, this work jointly designed the transmit power and IRS's reflection phase shifts and amplitudes.

Despite the fact that the aforementioned information-theory-based covert communication technologies are almost considered in the terrestrial-based network, there have been some recent studies applying these techniques to air-based networks as well as space-based networks. Particularly, the authors in [53] realized covert communication in multi-user terrestrial-based networks by using artificial noise technology. In the air-based network, the authors in [66] utilized the multi-antennas UAV to covert communication with multi-users on the ground simultaneously. In the space-based network, the authors in [69] applied cooperative relay technology in ISMTRN to improve the covert communication performance of the system. We believe that these technologies can be further applied to Satellite Internet in the future.

Remark 1. *Note that there are differences between the traditional and information-theory-based covert communication technologies. Traditional covert communication technology designs signal waveforms to reduce signal detection. Information theory-based covert communication technology research focuses on modifying the transmission environment to improve the performance of covert transmission. Furthermore, their performance metrics are different. Traditional covert communication technology quantifies covertness by detection and false-alarm probabilities. Information theory-based covert communication research uses the probability of detection error, which is the sum of false alarm and miss detection probability, as performance metrics.*

V. Challenges and Future Research Directions

Although the process of realizing the satellite covert communication has been witnessed in the last few years, there are still numerous outstanding questions that require additional investigation. In this section, we discuss the new opportunities and problems in the evolving Satellite Internet, and provide a list of interesting future research directions.

A. Satellite Uplink and Downlink Covert Communication

Since communication between the satellites is envisaged as via laser satellite links (named inter-satellite links, ISLs), secret information cannot be detected as it travels between satellites. On the other side, since the satellite ground link transmission must traverse the atmosphere, it is essential to investigate the impact of the atmospheric environment on covert communication in Satellite Internet. To the best knowledge of the authors, we only find one analytical work on the influence of atmospheric environment on the performance of satellite covert communications, which is [80]. This work examined the potential impact of evaporative ducting on the intercept vulnerability of covert communication systems. Thus, more general atmospheric environment impact problems on covert communication in Satellite Internet needs to be investigated in the future.

B. Cross-Layer Security Scheme

Due to the openness of Satellite Internet, it is important to investigate a robust security system to safeguard the vast number of sensitive data spread over numerous networks from eavesdroppers and wardens. To make security schemes more robust and protect against eavesdropping and detection, a collaborative security strategy is necessary, such as combining upper-layer encryption and physical-layer covert communication techniques. Consequently, the development of hybrid security solutions that offer many levels of protection would be a prospective and fruitful research direction.

C. Defending Against a Joint Attack

As shown in Fig. 3, the Satellite Internet is extremely vulnerable to different attacks simultaneously from neighboring enemy satellites, e.g., interference, detection, and wiretap. Thus, it is necessary to study the related defending against scheme, because this joint attack seriously threatens the security of the Satellite Internet. In UAV networks, some research efforts have proposed a security transmission scheme to defend against the joint attack [81]. However, neither the design of

a joint assault-resistant method suitable for Satellite Internet nor the transmission performance under joint attack have been researched.

D. Covert Communication Detection in Satellite Internet

Enemy and friendly satellites mixed in space allow enemy spies to communicate secret information through enemy satellites to escape interception or restriction by our firewalls, as shown in Fig. 2. Therefore, the demand for covert communication detection in Satellite Internet is very urgent, as shown in Fig. 5. For the past decades, the identification of specific communication emitter has enjoyed the most attention in the area of electronic counter measure activities [82]. Wu *et al.* proposed the identification of specific transmitters of satellite communications by using probabilistic neural networks (PNN) to reach the goal of target recognition [83]. With the rapid development of artificial intelligence (AI) technology, it has been widely used in signal processing and other directions. Thus, using AI to detect covert communication is an important research direction for covert transmission detection in the future.

E. Migration of Covert Communication Technology in Satellite Internet

Although it is theoretically possible to migrate covert communication techniques from terrestrial networks to Satellite Internet, different characteristics, e.g., relative motion, Doppler shift, rain attenuation, make the covert transmission scheme of the terrestrial network cannot be completely migrated to Satellite Internet. Therefore, the future research directions can be based on the design idea of covert communication in terrestrial network and combined with the characteristics of Satellite Internet to design the covert transmission schemes suitable for satellite network. In particular, using the predictability of the trajectory and topology of Satellite Internet, it is possible to gather future information such as the weather and the relative speed between the satellite and the earth. At the ground receiving end, we can execute operations such as Doppler frequency shift correction and channel state information estimation, which bridges the gap between the terrestrial network and Satellite Internet.

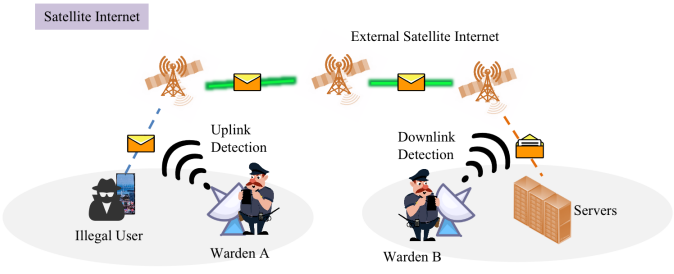


Fig. 5. Satellite Covert Communication Detection

VI. Conclusion

In this article, we provided a comprehensive survey on covert communication in Satellite Internet. We categorized the existing covert communication technologies into two categories: traditional and information theory-based covert communication technologies. Moreover, we divided the traditional covert communication technologies into three sub-categories: time domain, frequency domain, and time-frequency domain techniques. We also divided the information theory-based covert communication technologies into two sub-categories: increasing signal uncertainty and weakening signal leakage techniques. Finally, we introduce a number of research directions of Satellite Internet covert communication.

VII. Acknowledgment

This work was supported in part by the National Key R&D Program of China (Grant No. 2018YFE0207600), the Natural Science Foundation of China under Grant 61972308, 62202354, 62202355, the Natural Science Basic Research Program of Shaanxi (Grant No. 2019JC-17), and the Basic and Applied Basic Research Fund of Guangdong Province (Grant No.2021A1515111017).

References

[1] J. Fomon. (March 2022) Starlink hits 100+ Mbps download speed in 15 countries during Q4 2021. Ookla. [Online]. Available: https://www.ookla.com/articles/starlink-hughesnet-viasat-performance-q4-2021

[2] V. K. Shadaab Khan, Pramod Borasi. (2021) Satellite internet market by band type (C-band, X-band, L-band, K-band, and others) and end user (commercial users and individual): Global opportunity analysis and industry forecast, 2020–2030. [Online]. Available: https://www.alliedmarketresearch.com/satellite-internet-market-A12472

[3] J. Foust. (January 2022) SpaceX passes 2,000 starlink satellites launched. Spacenews. [Online]. Available: https://spacenews.com/spacex-passes-2000-starlink-satellites-launched/

[4] M. Sheetz. (May 2022) SpaceX's starlink satellite internet surpasses 400,000 subscribers globally. CNBC. [Online]. Available: https://www.cnbc.com/2022/05/25/spacexs-starlink-surpasses-400000-subscribers-globally.html

[5] B. A. Bash, D. Goeckel, D. Towsley, and S. Guha, "Hiding information in noise: Fundamental limits of covert wireless communication," *IEEE Commun. Mag.*, vol. 53, no. 12, pp. 26–31, 2015.

[6] S. Yan, X. Zhou, J. Hu, and S. V. Hanly, "Low probability of detection communication: Opportunities and challenges," *IEEE Wireless Commun.*, vol. 26, no. 5, pp. 19–25, 2019.

[7] S. Cioni, R. De Gaudenzi, O. D. R. Herrero, and N. Girault, "On the satellite role in the era of 5G massive machine type communications," *IEEE Netw.*, vol. 32, no. 5, pp. 54–61, 2018.

[8] O. Kodheli, E. Lagunas, N. Maturo, S. K. Sharma, B. Shankar, J. F. M. Montoya, J. C. M. Duncan, D. Spano, S. Chatzinotas, S. Kisseleff *et al.*, "Satellite communications in the new space era: A survey and future challenges," *IEEE Commun. Surveys Tuts.*, vol. 23, no. 1, pp. 70–109, 2020.

[9] F. Fourati and M.-S. Alouini, "Artificial intelligence for satellite communication: A review," *Intelligent and Converged Netw.*, vol. 2, no. 3, pp. 213–243, 2021.

[10] B. Li, Z. Fei, C. Zhou, and Y. Zhang, "Physical-layer security in space information networks: A survey," *IEEE Internet Things J.*, vol. 7, no. 1, pp. 33–52, 2019.

[11] S. Han, J. Li, W. Meng, M. Guizani, and S. Sun, "Challenges of physical layer security in a satellite-terrestrial network," *IEEE Netw.*, 2022.

[12] M. Manulis, C. P. Bridges, R. Harrison, V. Sekar, and A. Davis, "Cyber security in new space," *Int. J. Inf. Secur.*, vol. 20, no. 3, pp. 287–311, 2021.

[13] P. Tedeschi, S. Sciancalepore, and R. Di Pietro, "Satellite-based communications security: A survey on threats, solutions, and research challenges," *arXiv preprint arXiv:2112.11324*, 2021.

[14] S. Karapantazis and F. Pavlidou, "Broadband communications via high-altitude platforms: A survey," *IEEE Commun. Surveys Tuts.*, vol. 7, no. 1, pp. 2–31, 2005.

[15] A. L. Allison, *The ITU and managing satellite orbital and spectrum resources in the 21st century*. Springer Science & Business, 2014.

[16] R. Scholtz, "The origins of spread-spectrum communications," *IEEE Trans. Commun.*, vol. 30, no. 5, pp. 822–854, 1982.

[17] R. Huiltberg, F. H. Jean, and M. E. Jones, "Time division access for military communications satellites," *IEEE Trans. Aerosp. Electron. Syst.*, no. 3, pp. 272–282, 1965.

[18] T. Sekimoto and J. Puente, "A satellite time-division multiple-access experiment," *IEEE Trans. Commun. Technol.*, vol. 16, no. 4, pp. 581–588, 1968.

[19] O. Gabbard, "Design of a satellite time-division multiple-access burst synchronizer," *IEEE Trans. Commun. Technol.*, vol. 16, no. 4, pp. 589–596, 1968.

[20] A. Polydoros and C. Weber, "Detection performance considerations for direct-sequence and time-hopping LPI waveforms," *IEEE J. Sel. Areas Commun.*, vol. 3, no. 5, pp. 727–744, 1985.

[21] A. Bharadwaj and J. K. Townsend, "Evaluation of the covertness of time-hopping impulse radio using a multi-radiometer detection," in *Proc. IEEE MILCOM*, vol. 1, 2001, pp. 128–134.

[22] J. Yu and Y. Yao, "Detection performance of time-hopping ultra-wideband lpi waveforms," in *Proc. IEEE/Sarnoff Symp. on Advances in Wired and Wireless Commun.*, 2005, pp. 137–140.

[23] M. Pursley, "Frequency-hop transmission for satellite packet switching and terrestrial packet radio networks," *IEEE Trans. Inf. Theory*, vol. 32, no. 5, pp. 652–667, 1986.

[24] P. Lal, V. Palsule, and K. Ravi, "Applications of frequency hopping spread spectrum techniques: an overview," *IETE Technical Review*, vol. 3, no. 5, pp. 210–220, 1986.

[25] K. M. Dostert, "Frequency-hopping spread-spectrum modulation for digital communications over electrical power lines," *IEEE J. Sel. Areas Commun.*, vol. 8, no. 4, pp. 700–710, 1990.

[26] L. Rong and L. Ruimin, "An anti-jamming improvement strategy for satellite frequency-hopping communication," in *Proc. IEEE Int. Conf. on Wireless Commun. & Signal Processing*, 2009, pp. 1–5.

[27] N. C. Beaulieu, W. L. Hopkins, and P. J. McLane, "Interception of frequency-hopped spread-spectrum signals," *IEEE J. Sel. Areas Commun.*, vol. 8, no. 5, pp. 853–870, 1990.

[28] K. Lee and S. Oh, "Detection of fast frequency-hopping signals using dirty template in the frequency domain," *IEEE Wireless Commun. Lett.*, vol. 8, no. 1, pp. 281–284, 2018.

[29] B. Ning, L. Guan, and H. Huang, "A novel frequency-hopping sequence for covert communication," *IEEE Access*, vol. 5, pp. 20 157–20 163, 2017.

[30] D. Borth and M. Pursley, "Analysis of direct-sequence spread-spectrum multiple-access communication over rician fading channels," *IEEE Trans. Commun.*, vol. 27, no. 10, pp. 1566–1577, 1979.

[31] R. Pickholtz, D. Schilling, and L. Milstein, "Theory of spread-spectrum communications-a tutorial," *IEEE Trans. Commun.*, vol. 30, no. 5, pp. 855–884, 1982.

[32] E. Chandler and G. Cooper, "Low probability of intercept performance bounds for spread-spectrum systems," *IEEE J. Sel. Areas Commun.*, vol. 3, no. 5, pp. 706–713, 1985.

[33] R. D. Van Nee, H. S. Misser, and R. Prasad, "Direct-sequence spread spectrum in a shadowed rician fading and land-mobile satellite channel," *IEEE J. Sel. Areas Commun.*, vol. 10, no. 2, pp. 350–357, 1992.

[34] M. Simon, J. Omura, R. Scholtz, and B. Levitt, *Spread spectrum communications handbook*. McGraw-Hill Education, 2002.

[35] A. M. Wik and A. L. Lindblad, "A novel LPI concept using filtered spreading codes," in *Proc. IEEE Military Commun. Conf. (MILCOM)*, vol. 1, McLean, VA, USA, 1996, pp. 90–94.

[36] M. S. Nowak, J. LoCicero, and D. Ucci, "Bandlimited covert data communications using zinc waveforms," in *Proc. IEEE Military Commun. Conf. (MILCOM)*, vol. 2, Anaheim, CA, USA, 2002, pp. 1018–1023.

[37] C. Shih, "Fractionalization of fourier transform," *Opt. Commun.*, vol. 118, no. 5-6, pp. 495–498, 1995.

[38] L. Mei, X. Sha, and N. Zhang, "The approach to carrier scheme convergence based on 4-weighted fractional fourier transform," *IEEE Commun. Lett.*, vol. 14, no. 6, pp. 503–505, 2010.

[39] S. Liu, J. Zhang, and Y. Zhang, "Properties of the fractionalization of a fourier transform," *Opt. Commun.*, vol. 133, no. 1-6, pp. 50–54, 1997.

[40] D. S. Yeung, Q. Ran, E. C. Tsang, and K. L. Teo, "Complete way to fractionalize fourier transform," *Opt. Commun.*, vol. 230, no. 1-3, pp. 55–57, 2004.

[41] Q. Ran, D. S. Yeung, E. C. Tsang, and Q. Wang, "General multifractional fourier transform method based on the generalized permutation matrix group," *IEEE Trans. Signal Process.*, vol. 53, no. 1, pp. 83–98, 2004.

[42] Z. Wang, L. Mei, X. Wang, and N. Zhang, "WFRFT precoding for generalized frequency division multiplexing," in *Proc. IEEE WCNC*, Doha, Qatar, 2016, pp. 1–6.

[43] L. Mei, X. Sha, and N. Zhang, "Covert communication based on waveform overlay with weighted fractional fourier transform signals," in *Proc. IEEE Int. Conf. on Wireless Commun., Netw. and Information Security*, 2010, pp. 472–475.

[44] D. Zhai, X. Da, H. Hu, Y. Liang, R. Xu, and L. Ni, "Satellite anti-interception communication system based on WFRFT and MIMO," in *Proc. IEEE Int. Conf. Commun. Soft. and Netw. (ICCSN)*, Chengdu, China, 2018, pp. 305–310.

[45] B. A. Bash, D. Goeckel, and D. Towsley, "Limits of reliable communication with low probability of detection on AWGN channels," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1921–1930, 2013.

[46] P. H. Che, S. Kadhe, M. Bakshi, C. Chan, S. Jaggi, and A. Sprintson, "Reliable, deniable and hidable communication: A quick survey," in *Proc. IEEE Information Theory Workshop (ITW)*, Hobart, TAS, Australia, 2014, pp. 227–231.

[47] P. H. Che, M. Bakshi, C. Chan, and S. Jaggi, "Reliable, deniable and hidable communication," in *Proc. Information Theory and Applications (ITA)*, San Diego, CA, USA, 2014, pp. 1–10.

[48] M. Bloch, "A channel resolvability perspective on stealth communications," in *Proc. IEEE Int. Symp. on Information theory (ISIT)*, Hong Kong, China, 2015, pp. 2535–2539.

[49] D. Goeckel, B. Bash, S. Guha, and D. Towsley, "Covert communications when the warden does not know the background noise power," *IEEE Commun. Lett.*, vol. 20, no. 2, pp. 236–239, 2015.

[50] T. V. Sobers, B. A. Bash, S. Guha, D. Towsley, and D. Goeckel, "Covert communication in the presence of an uninformed jammer," *IEEE Trans. Wireless Commun.*, vol. 16, no. 9, pp. 6193–6206, 2017.

[51] R. Soltani, D. Goeckel, D. Towsley, B. A. Bash, and S. Guha, "Covert wireless communication with artificial noise generation," *IEEE Trans. Wireless Commun.*, vol. 17, no. 11, pp. 7252–7267, 2018.

[52] K. Shahzad, X. Zhou, S. Yan, J. Hu, F. Shu, and J. Li, "Achieving covert wireless communications using a full-duplex receiver," *IEEE Trans. Wireless Commun.*, vol. 17, no. 12, pp. 8517–8530, 2018.

[53] K. Huang, H. Deng, and H. Wang, "Jamming aided covert communication with multiple receivers," *IEEE Trans. Wireless Commun.*, vol. 20, no. 7, pp. 4480–4494, 2021.

[54] Z. Li, X. Liao, J. Shi, L. Li, and P. Xiao, "MD-GAN based UAV trajectory and power optimization for cognitive covert communications," *IEEE Internet Things J.*, 2021.

[55] M. Wang, W. Yang, L. Xu, X. Lv, Y. Chen, Q. Wu, and B. Liu, "Covert wireless communication on beidou short message communication," in *China Satellite Navigation Conference*. Springer, 2022, pp. 310–320.

[56] S. Yan, B. He, X. Zhou, Y. Cong, and A. L. Swindlehurst, "Delay-intolerant covert communications with either fixed or random transmit power," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 1, pp. 129–140, 2018.

[57] X. Zhou, S. Yan, J. Hu, J. Sun, J. Li, and F. Shu, "Joint optimization of a UAV's trajectory and transmit power for covert communications," *IEEE Trans. Signal Process.*, vol. 67, no. 16, pp. 4276–4290, 2019.

[58] L. Tao, W. Yang, S. Yan, D. Wu, X. Guan, and D. Chen, "Covert communication in downlink noma systems with random transmit power," *IEEE Wireless Commun. Lett.*, vol. 9, no. 11, pp. 2000–2004, 2020.

[59] R. Ma, X. Yang, G. Pan, X. Guan, Y. Zhang, and W. Yang, "Covert communications with channel inversion power control in the finite blocklength regime," *IEEE Wireless Commun. Lett.*, vol. 10, no. 4, pp. 835–839, 2020.

[60] B. Kang, N. Ye, and B. Qi, "Comparisons on covert performances of noma in satellite internet of things," in *Proc. IEEE Comput., Commun. and IoT Appl. (ComComAp)*, Shenzhen, China.

[61] A. Sheikholeslami, M. Ghaderi, D. Towsley, B. A. Bash, S. Guha, and D. Goeckel, "Multi-hop routing in covert wireless networks," *IEEE Trans. Wireless Commun.*, vol. 17, no. 6, pp. 3656–3669, 2018.

[62] H. Wang, Y. Zhang, X. Zhang, and Z. Li, "Secrecy and covert communications against UAV surveillance via multi-hop networks," *IEEE Trans. Commun.*, vol. 68, no. 1, pp. 389–401, 2019.

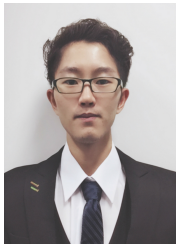
[63] H. Wu, Y. Zhang, X. Liao, Y. Shen, and X. Jiang, "On covert throughput performance of two-way relay covert wireless communications," *Wirel. Netw.*, vol. 26, no. 5, pp. 3275–3289, 2020.

[64] C. Gao, B. Yang, X. Jiang, H. Inamura, and M. Fukushi, "Covert communication in relay-assisted IoT systems," *IEEE Internet Things J.*, vol. 8, no. 8, pp. 6313–6323, 2021.

[65] R. Sun, B. Yang, S. Ma, Y. Shen, and X. Jiang, "Covert rate maximization in wireless full-duplex relaying systems with power control," *IEEE Trans. Commun.*, vol. 69, no. 9, pp. 6198–6212, 2021.

[66] X. Jiang, Z. Yang, N. Zhao, Y. Chen, Z. Ding, and X. Wang, "Resource allocation and trajectory optimization for UAV-Enabled multi-user covert communications," *IEEE Trans. Veh. Technol.*, vol. 70, no. 2, pp. 1989–1994, 2021.
[67] X. Chen, Z. Chang, J. Tang, N. Zhao, and D. Niyato, "UAV-aided multi-antenna covert communication against multiple wardens," in *Proc. IEEE International Conference on Communications (ICC)*, Montreal, QC, Canada, 2021, pp. 1–6.
[68] H. Du, D. Niyato, Y. Xie, Y. Cheng, J. Kang, and D. I. Kim, "Performance analysis and optimization for jammer-aided multi-antenna UAV covert communication," *arXiv preprint arXiv:2202.00973*, 2022.
[69] Z. Wu, R. Liu, H. Shuai, S. Zhu, and C. Li, "Covert performance for integrated satellite multiple terrestrial relay networks with partial relay selection," *Sensors*, vol. 22, no. 15, p. 5524, 2022.
[70] T. Zheng, H. Wang, D. W. K. Ng, and J. Yuan, "Multi-antenna covert communications in random wireless networks," *IEEE Trans. Wireless Commun.*, vol. 18, no. 3, pp. 1974–1987, 2019.
[71] L. Yang, W. Yang, S. Xu, L. Tang, and Z. He, "Achieving covert wireless communications using a full-duplex multi-antenna receiver," in *Proc. IEEE Int. Conf. on Compu. and Commun. (ICCC)*, 2019, pp. 912–916.
[72] K. Shahzad, X. Zhou, and S. Yan, "Covert wireless communication in presence of a multi-antenna adversary and delay constraints," *IEEE Trans. Veh. Technol.*, vol. 68, no. 12, pp. 12 432–12 436, 2019.
[73] O. Shmuel, A. Cohen, and O. Gurewitz, "Multi-antenna jamming in covert communication," *IEEE Trans. Commun.*, vol. 69, no. 7, pp. 4644–4658, 2021.
[74] M. V. Jamali and H. Mahdavifar, "Covert millimeter-wave communication: Design strategies and performance analysis," *IEEE Trans. Wireless Commun.*, 2021.
[75] J. Xu, L. Bai, L. Zhou, D. Liu, J. Wang, and Y. Shi, "Covert downlink mmwave communication for massive MIMO LEO satellite," in *Proc. China Conference on Command and Control*. Singapore: Springer, 2022, pp. 653–664.
[76] J. Si, Z. Li, Y. Zhao, J. Cheng, L. Guan, J. Shi, and N. Al-Dhahir, "Covert transmission assisted by intelligent reflecting surface," *IEEE Trans. Commun.*, vol. 69, no. 8, pp. 5394–5408, 2021.
[77] C. Wu, S. Yan, X. Zhou, R. Chen, and J. Sun, "Intelligent reflecting surface (IRS)-aided covert communication with warden's statistical CSI," *IEEE Wireless Commun. Lett.*, vol. 10, no. 7, pp. 1449–1453, 2021.
[78] C. Wang, Z. Li, J. Shi, and D. W. K. Ng, "Intelligent reflecting surface-assisted multi-antenna covert communications: Joint active and passive beamforming optimization," *IEEE Trans. Commun.*, vol. 69, no. 6, pp. 3984–4000, 2021.
[79] X. Zhou, S. Yan, Q. Wu, F. Shu, and D. W. K. Ng, "Intelligent reflecting surface (IRS)-aided covert wireless communications with delay constraint," *IEEE Trans. Wireless Commun.*, vol. 21, no. 1, pp. 532–547, 2022.
[80] J. R. Hampton, "The impact of evaporative ducting on covert communications," in *Proc. IEEE MILCOM*, Orlando, FL, USA, 2007, pp. 1–7.
[81] J. Liu and W. Yang, "Secure uav communication against cooperative adaptive eavesdroppers," *Wirel. Netw.*, vol. 28, no. 3, pp. 1113–1128, 2022.
[82] R. M. Clark, "Perspectives on intelligence collection," *J. of US Intelligence Collection*, vol. 20, pp. 47–52, 2013.
[83] X. Wu, Y. Shi, W. Meng, X. Ma, and N. Fang, "Specific emitter identification for satellite communication using probabilistic neural networks," *Int. J. Satell. Co. Netw.*, vol. 37, no. 3, pp. 283–291, 2019.

Zewei Guo received the B.S. degree in software engineering from Shanxi University, Taiyuan, China, in 2015 and the M.S. degree in computer technology from Xidian University, Xi'an, China, in 2019. He is currently pursuing the Ph.D. degree with the School of Systems Information Science, Future University Hakodate, Japan. His research interest focuses on the covert communication in Satellite Internet.



Ji He (Member, IEEE) received the B.S. and M.S. degrees from Xidian University, Xi'an, Shaanxi, China, in 2014 and 2018, respectively, and the Ph.D. degree from Future University Hakodate, Hakodate, Hokkaido, Japan, in 2020. He is currently a Lecturer with the School of Computer Science and Technology, Xidian University. His research interests include satellite internet, wireless security. He received the 2020 IEEE Sapporo Section Encouragement Award.

Yuanyu zhang (Member, IEEE) received the B.S. and M.S. degrees from Xidian University, Xi'an, China, in 2011 and 2014, respectively, and the Ph.D. degree from Future University Hakodate, Hakodate, Hokkaido, Japan, in 2017. He is currently an Associate Professor with the School of Computer Science and Technology, Xidian University, Xi'an, Shaanxi, China. Prior to joining Xidian University, he was an Assistant Professor with the Graduate School of Science and Technology, Nara Institute of Science and Technology, Ikoma, Japan. His research interests include physical layer security and satellite network security and IoT security.

Shuangrui Zhao (Member, IEEE) received the B.S. degree and Ph.D. degree from Xidian University in 2015 and 2021, respectively. He is currently a lecturer with the School of Computer Science and Technology, Xidian University. His research interests include physical layer security of wireless communications and optimal control.

Yulong Shen received the B.S. and M.S. degrees in computer science and Ph.D. degree in cryptography from Xidian University, Xi'an, China, in 2002, 2005, and 2008, respectively. He is currently a Professor with the School of Computer Science and Technology, Xidian University, where he is also an Associate Director of the Shaanxi Key Laboratory of Network and System Security. His research interests include wireless network security and cloud computing security. He has also served on the technical program committees of several international conferences, including ICEBE, INCoS, CIS, and SOWN.

Xiaohong Jiang (Senior Member, IEEE) received the B.S., M.S., and Ph.D. degrees from Xidian University, China, in 1989, 1992, and 1999, respectively. He was an Associate Professor with Tohoku University, from 2005 to 2010. He is currently a Full Professor with Future University Hakodate, Japan. His research interests include wireless networks and optical networks, network security, and routers/switches design. He has published over 300 technical papers, which include over 70 papers published in the top IEEE journals and top IEEE conferences, like the IEEE/ACM Transactions on Networking, the IEEE Journal of Selected Areas on Communications, the IEEE Transactions on Parallel and Distributed Systems, and the IEEE INFOCOM. He received the Best Paper Award at the IEEE HPCC 2014, IEEE WCNC 2012, IEEE ICC 2005-Optical Networking Symposium, and IEEE/IEICE HPSR 2002.