Low Earth Orbit Satellite Security and Reliability: Issues, Solutions, and the Road Ahead

Pingyue Yue, *Student Member, IEEE*, Jianping An, *Senior Member, IEEE*, Jiankang Zhang, *Senior Member, IEEE*, Jia Ye, *Member, IEEE*, Gaofeng Pan, *Senior Member, IEEE*, Shuai Wang, *Member, IEEE*, Pei Xiao, *Senior Member, IEEE*, and Lajos Hanzo, *Life Fellow, IEEE*

***Abstract*—Low Earth Orbit (LEO) satellites undergo a period of rapid development driven by ever-increasing user demands, reduced costs, and technological progress. Since there is a lack of literature on the security and reliability issues of LEO Satellite Communication Systems (SCSs), we aim to fill this knowledge gap. Specifically, we critically appraise the inherent characteristics of LEO SCSs and elaborate on their security and reliability requirements. In light of this, we further discuss their vulnerabilities, including potential security attacks launched against them and reliability risks, followed by outlining the associated lessons learned. Subsequently, we discuss the corresponding security and reliability enhancement solutions, unveil a range of trade-offs, and summarize the lessons gleaned. Furthermore, we shed light on several promising future research directions for enhancing the security and reliability of LEO SCSs, such as integrated sensing and communication, computer vision aided communications, as well as challenges brought about by mega-constellation and commercialization. Finally, we summarize the lessons inferred and crystallize the take-away messages in our design guidelines.**

***Index Terms*—LEO satellite communication systems, security attacks, reliability risks, security enhancement solutions, reliability enhancement solutions, security attack prevention, security attack detection, security attack mitigation, design guidelines.**

I. Introduction

Driven by the explosive proliferation of smart devices and the escalation of data traffic, the Sixth-generation (6G) [1]–[3] concept aims for building a large-dimensional and autonomous global network capable of supporting seamless coverage and ubiquitous services. As evidenced by the literature [4], it has been proposed that future wireless networks must be able to seamlessly interface with terrestrial and satellite networks. Compared to Medium Earth Orbit (MEO) and Geostationary Earth Orbit (GEO) satellites, Low Earth Orbit (LEO) satellites [5]–[7] are closer to the Earth. Hence, they are more suitable for supporting delay-sensitive communications worldwide [8]. Additionally, rocket recovery and multi-satellite launching technologies have substantially reduced the average launch cost and deployment time. From 2012 to the second quarter of 2023, about 7824 LEO satellites have been successfully launched, as shown in Fig. 1. As a benefit, LEO Satellite Communication Systems (SCSs) have found a plethora of applications, including the Internet of Remote Things (IoRT), smart city, and emergency rescue [9]–[11].

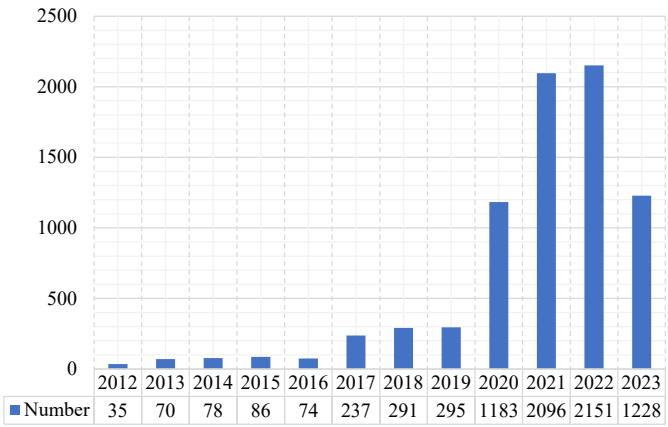


Fig. 1: Number of LEO satellites launched from 2012 to the second quarter of 2023.

Fig. 2 illustrates the application scenarios of LEO satellites. In Fig. 2(a), the LEO satellite-based IoRT concept is illustrated, where LEO satellites are deployed to support seamless wireless access to remote geographical areas [12]. Since they are closer to the earth, they have low propagation loss, which reduces the transmit power requirements of power-limited sensors. A large number of sensors deployed in mines, farms, mariculture farms, and solar power plants collect voltage, temperature, pH, and other status information and then separately upload them to LEO satellites. LEO satellites deliver these sensory data to remote operators for further analysis and processing.

In Fig. 2(b), the LEO satellite-based smart city scenario is illustrated, where they are employed in support of telemedicine, the Internet of Vehicles (IoV), smart factories, and homes for improving urban services, the city's sustainability, and

This work was supported in part by the National Key Research and Development Program of China under Grant 2021YFC3320200 and 2022YFC3331102, and in part by the National Natural Science Foundation of China under Grant 62171031.

Pingyue Yue is with the School of Information and Electronics, Beijing Institute of Technology, Beijing 100081, China (e-mails: ypy@bit.edu.cn).

Jianping An **(Corresponding author)**, Gaofeng Pan, and Shuai Wang are with the School of Cyberspace Science and Technology, Beijing Institute of Technology, Beijing 100081, China (e-mails: an@bit.edu.cn; gfpan@bit.edu.cn; swang@bit.edu.cn).

Jiankang Zhang is with the Department of Computing and Informatics, Bournemouth University, Bournemouth BH12 5BB, U.K. (e-mail: jzhang3@bournemouth.ac.uk).

Jia Ye is with the school of Electrical Engineering, Chongqing University, Chongqing, 400044, China (yejiaft@163.com)

Pei Xiao is with the 5GIC & 6GIC, Institute for Communication Systems, University of Surrey, GU2 7XH, U.K. (e-mail: p.xiao@surrey.ac.uk).

Lajos Hanzo is with the School of Electronics and Computer Science, University of Southampton, Southampton SO17 1BJ, U.K. (e-mail: lh@ecs.soton.ac.uk).

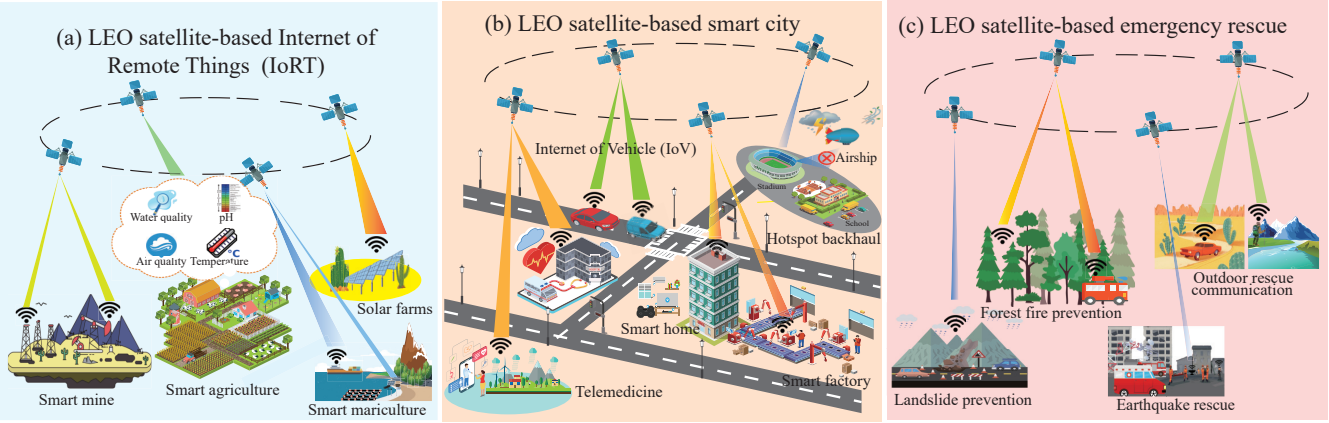


Fig. 2: The application scenarios of LEO SCSs.

the factory's production efficiency [13]. For instance, the IoV allows vehicles to communicate with the surrounding environment, such as neighboring cars and roadside infrastructure, supporting a wide range of 'on-the-go' services such as road safety, congestion control, and location-dependent services. It is imperative to leverage LEO satellites to serve vehicles anywhere and anytime by exploiting their respective advantages in terms of low latency, and seamless coverage [14]. Long-distance diagnosis, consultation, and treatment may be provided for the wounded and sick in case of emergencies. In addition, in massive connectivity scenarios at schools, sporting events, or rallies, it may be permitted to deploy airships to provide temporary access but it is difficult to establish stable wireless backhaul links due to the weather conditions, such as wind and rain. Therefore, LEO satellites constitute a promising solution for coverage extension and backhaul links since they tend to be more immune to weather conditions [15]. In Fig. 2(c), an LEO satellite-based emergency rescue scenario is portrayed [16]. People in remote mountains or deserts may use their terminals to send distress signals or even may have access to real-time voice services via LEO satellites in an emergency. Disasters, such as landslides, forest fires, and earthquakes, may cause the loss of life and property, which motivate emergency responses based on LEO satellites to support enhanced situational awareness, automated decision-making, and a whole host of other prompt responses [17].

Given the wide range of applications of LEO SCSs seen in Fig. 2, their security is also of paramount importance. For example, the data collected by sensors in mines contains confidential information, including mineral types and reserves, which attracts potential commercial competitors to exploit their satellites for eavesdropping. Butun *et al.* [18] revealed that the operational telemedicine systems lack the strong security services that prevent patient privacy from disclosure. In addition, given the ongoing deployment of dense LEO mega-constellations, the electromagnetic environment becomes more complex, which may jam or disrupt communications altogether.

II. Existing Literature and Contributions

In this section, we delve deeper into a discussion of existing literature and summarize their contributions and limitations, which has motivated our research. Subsequently, we detail our contributions. Finally, the organization of this paper is provided.

A. Existing Literature

In recent years, a range of important papers have been conceived on the security of LEO SCSs. Although these papers have played a certain role in how to safeguard LEO SCSs, they also have shortcomings. Firstly, some of them focused on the security of Space Information Networks (SIN) relying on LEO SCSs. More specifically, Li *et al.* [19] considered the security performance as their pivotal target, focused on eavesdropping security attacks, and presented a security design of the SCSs from the perspective of Physical Layer Security (PLS). Han *et al.* [20] critically appraised a secure architecture to safeguard the SIN, where relays relying on hopped beams were deployed for mitigating both the jamming attacks of the uplink and the eavesdropping attacks of the downlink. In fact, the SIN has also suffered security attacks, including user privacy and message modification, which are not covered in this paper. To address this, Bao *et al.* [21] presented blockchain techniques for dealing with user privacy and message modification. But blockchain alone cannot solve physical layer attacks like jamming. Therefore, the protection of SIN cannot depend on one technique alone, but on the collaboration of several techniques.

Secondly, substantial efforts were dedicated to integrated networks containing LEO SCSs, e.g., Space-air-ground Integrated Networks (SAGIN), and satellite-terrestrial networks. Li *et al.* [22] conceived the integration of Artificial Intelligence (AI) and blockchain for improving data security (e.g., eavesdropping and malicious message modification) in 6G. Similarly, this paper still lacked a discussion on malicious jamming and corresponding measures. Liu *et al.* [23] discussed the core issues of cross-layer design, resource management, and allocation in SAGINs, with a brief reference to PLS techniques to address eavesdropping. Lin *et al.* [24] surveyed

TABLE I: Comparison with literature

Ref.	Security and reliability issues						Security and reliability enchancement solutions					Future trends	Design guidelines
	Security attacks				Reliability risks								
	Eavesdropping	Jamming	Message modification	User privacy	CCI	Physical threats	PLS	CR	AI	QKD	Blockchain		
[19]	✓						✓					✓	
[20]	✓	✓					✓					✓	
[21]			✓	✓							✓		
[22]	✓		✓						✓		✓		
[23]	✓	✓					✓						
[24]	✓						✓					✓	
[25]	✓				✓		✓	✓				✓	
[26]	✓						✓					✓	
[27]	✓	✓	✓	✓					✓	✓	✓	✓	
[28]	✓	✓	✓	✓		✓		✓	✓	✓		✓	
[29]					✓			✓					
[30]			✓	✓					✓		✓		
[31]	✓		✓						✓	✓			
[32]			✓		✓			✓	✓			✓	
[33]	✓		✓	✓				✓				✓	
[34]		✓	✓						✓				
[35]			✓	✓					✓	✓			
[36]	✓	✓						✓					
[37]		✓	✓	✓					✓	✓		✓	
[38]	✓	✓	✓	✓	✓			✓	✓	✓		✓	
[39]	✓	✓	✓	✓			✓			✓		✓	
[40]	✓	✓	✓	✓			✓	✓	✓	✓		✓	
[41]					✓	✓		✓	✓	✓		✓	
This paper	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔

the current activities and system architecture of converged 5G and satellite networks. A novel metric, termed as an effective and achievable rate relied on the PLS technique, was conceived for quantifying the trade-off between reliability and security. However, security is mainly focused on eavesdropping. Wang *et al.* [25] highlighted the convergence of satellite and terrestrial networks, where the former was deemed to be more vulnerable to security violation risks and eavesdropping threats. Multiple Input Multiple Output (MIMO) antenna-aided PLS techniques were discussed as their solutions. Another security concern addressed in this paper is reliability degradation due to spectrum scarcity. As a remedy, the Cognitive Radio (CR) technique is adopted for dealing with this issue. But other security attacks, such as jamming and message modification, were not mentioned in this paper. Lorenzo *et al.* [26] focused their attention on PLS based on Artificial Noise(AN) as well as Reflective Intelligent Surfaces (RISs) to address eavesdropping in 6G. Nguyen *et al.* [27] focused their research on the emerging security risks, such as learning-empowered attacks and massive data breaches, caused by the plethora of devices and a suite of novel technologies emerging as part of the recent 6G. Security and privacy issues were discussed in the context of the physical, connection, and service layers. The assessments of the prospective techniques, such as PLS, Quantum Key Distribution (QKD), and distributed ledgers, were also outlined. Guo *et al.* [28] surveyed the security threats in SAGINs and divided them into four research areas, i.e. operation threats, network threats, and data threats. Furthermore, a variety of attack methodologies and their corresponding solutions were discussed. This paper discusses security issues comprehensively, especially the first-time discussion of physical threats, such as earthquakes and floods, that affect reliability. However, these threats are targeted at terrestrial networks in SAGINs and do not involve LEO satellites. Xie *et al.* [29] focused on the future development of key technologies and challenges for LEO mega-constellations for 6G global coverage. This paper introduced interference coordination techniques, such as CR, to mitigate interference between LEO satellites and terrestrial networks as well as GEO satellites. Wang *et al.* [30] presented a comprehensive survey of the family of blockchain solutions designed for SAGINs. This paper classified security attacks into data-related, identity-related, service-related, and so on, but neglected signal-related security attacks, such as eavesdropping and jamming, in wireless environments. Xu *et al.* [31] focused their attention on QKD solutions for the sake of providing ultimate security for the space, aerial, and ground nodes of the emerging SAGIN systems. Zhou *et al.* [32] presented a comprehensive survey of aerospace-integrated network innovation for 6G and discussed AI measures to deal with security attacks. In addition, Lu *et al.* [33] discussed the

reinforcement learning-based cross-layer security and privacy protection methods conceived for enhancing physical layer security and user privacy in 6G. By integrating the physical layer, media access control layer, and network layer, the paper optimized the network security decision-making mechanism using reinforcement learning, while maintaining the user experience and performance. However, Lu *et al.* only provided an overview of reinforcement learning-based security solutions for UAV communications in the Non-terrestrial Networks (NTNs) of 6G.

Thirdly, some authors have discussed security issues in specific satellite-based applications. Liu *et al.* [34] focused on the security of satellite-based Automatic Dependent Surveillance-Broadcast (ADS-B). This paper mainly discussed the employment of machine learning for dealing with malicious injection and modification attacks. Hao *et al.* [35] considered the security and privacy issues encountered in satellite-based radio spectrum monitoring and outlined the compelling benefit of blockchain in security and privacy protection dispensing with centralized authorization. Centenaro *et al.* [36] surveyed the satellite-based IoT and suggested the employment of optical Inter-satellite Links (ISLs) for mitigating jamming and eavesdropping. However, this paper lacked a discussion on the protection of data security and user privacy. Vaezi *et al.* [37] studied the most prevalent attacks targeted at the satellite-based Internet of Things (IoT), and categorized them into physical attacks, software attacks, and network attacks based on their entry point. Then a host of Deep Learning (DL) and federated learning techniques were proposed as their corresponding solutions. This paper primarily focused on the security attacks on cellular IoT, but there was relatively little content about satellite IoT. Hraishawi *et al.* [38] discussed the deployment challenges of LEO SCSs, including their coexistence with GEO SCSs and terrestrial communication systems. Both PLS techniques and QKD schemes were also introduced as the means of mitigating the associated security threats, such as eavesdropping and jamming. With the wider development of LEO SCSs, some concomitant security issues have come along. Manulis *et al.* [39] analyzed a whole host of past satellite security threats and discussed their motivations and characteristics. Moreover, they also discussed the emerging security risks posed by advanced technologies, such as Commercial Off The Shelf (COTS) components, Software Defined Radios (SDRs), and cloud computing. Tedeschi *et al.* [40] surveyed the security of SCSs, with an emphasis on PLS and cryptography. More specifically, anti-jamming strategies and anti-spoofing schemes were discussed in PLS, while authentication, key agreement, and key distribution based on emerging quantum domain techniques were also studied. However, these two papers lacked a discussion on the reliability of the continuous deployment of LEO satellites, such as the Co-channel Interference (CCI) between LEO satellites and terrestrial networks as well as GEO satellites due to the spectrum scarcity. In addition, Marko *et al.* [41] emphasized the importance of space safety for sustainable satellites and discussed hot issues of space traffic management, debris detection, and spectrum sharing of SCSs. However, this paper lacked a discussion on eavesdropping and malicious jamming as well as corresponding solutions.

Again, Table I boldly and explicitly contrasts this survey against the existing magazine and survey papers, indicating that a wider survey is provided by this literature by critically appraising as many as 23 citations [19]–[41]. Furthermore, based on these we formulated explicit lessons to prevent pitfalls and design guidelines, which are unique for this paper, along with detailed discussions on reliability enhancement solutions.

B. Motivations

Although there are some early papers on the security and reliability of LEO SCSs, in the light of recent advances, it is timely to critically appraise them.

1) Insufficient Research of Existing Papers: As seen in Table I, the existing papers have incomplete coverage of security and reliability issues. In particular, while some papers have recognized the impact of physical threats, such as space debris [34], on reliability, the existing research on this topic is limited.

Only with a deeper assessment and understanding of the existing security and reliability issues, such as the degree of damage, reversibility, awareness, collateral damage, etc., can we design potent solutions. Hence we are inspired to fill this knowledge gap in the open literature.

2) Lack of Consideration for the Inherent Characteristics of LEO SCSs: Lots of existing papers discussed LEO satellites as an important component of the future 6G or SAGINs, but only a few of them focus on the analysis of the inherent characteristics of LEO SCSs, such as being sandwiched between GEO satellites and terrestrial communication systems, their high mobility, the large number of LEO satellites, limited onboard resources, and so on. These characteristics are the key to considering the security and reliability requirements, issues, and solutions.

Given the crowded orbits and the ongoing deployments of dense LEO mega-constellations, their orbits are becoming increasingly overcrowded, which undoubtedly increases the probability of collisions. Frequent launch activities also generate space debris in LEOs, which hence threatens the safe operation of LEO satellites. In addition, the space environment is harsh. Many satellites have failed before accomplishing their missions, partly because cosmic radiation may impair the electronic devices on the satellite.

The Doppler shift caused by high mobility seriously deteriorates the performance [42]. Additionally, LEO satellites are sandwiched between MEO satellites and terrestrial communication systems. Hence the CCI due to spectrum sharing among these systems and its corresponding solutions have to be investigated in detail.

3) Lack of Design Guidelines of Secure and Reliable LEO SCSs: Existing papers show that protecting the secure and reliable operation of LEO SCSs does not rely on a specific solution alone but on the cooperation of multiple solutions. Moreover, effective security and reliability enhancement solutions may be derived by carefully characterizing the relationship between their confidentiality, integrity, and latency. For

example, due to size, memory, and power constraints, LEO satellites either have no operating system at all or can only run stripped-down versions of a sophisticated operating system. They are unsuitable for complex encryption algorithms. By contrast, usually complex encryption algorithms are used for authentication in the ground segment, given the abundant power supply and computing resources. Hence, several trade-offs must be struck in the design of secure LEO SCSs.

However, the existing literature does not integrate these advanced solutions together to safeguard LEO SCSs. Hence in this literature, design guidelines for secure and reliable LEO SCSs. Indeed, design guidelines are distilled from the characteristics of LEO SCSs, security and reliability requirements, issues, and solutions, outlining the lessons learned and the various trade-offs.

C. Contributions

Against this backdrop, the main contributions of this survey are summarized as follows:

- We discuss the inherent characteristics of LEO SCSs and outline their unique security and reliability challenges. Based on this, we also summarize their security and reliability requirements (Sec. III, IV).
- Relying on recent research results and the unique security and reliability challenges encountered by LEO SCSs, we review their security attacks and discuss several reliability risks, such as Single Event Upsets (SEUs) and collisions with debris. Furthermore, the characteristics and impacts of these issues are analyzed and summarized in Table VI at a glance. We also summarize several lessons learned from these issues (Sec. V).
- As a remedy, we review a rich suite of solutions and classify them into security and reliability enhancement solutions. Moreover, we further divide the family of security enhancement solutions into active and passive security enhancement solutions from the perspective of prevention, detection, and mitigation. Moreover, we discuss several trade-offs to be observed by the solutions and summarize the lessons learned from these solutions (Sec. VI).
- Our discussions concerning the lessons learned from the analysis of solutions and gleaned from the remaining technical challenges inspire several promising future research directions, such as the employment of integrated sensing and communication, Computer Vision (CV)-aided secure communications, as well as the unique challenges imposed by mega-constellations and commercialization (Sec. VII).
- Again, the analysis of the inherent characteristics, security and reliability requirements, and issues as well as solutions, allows us to outline the lessons learned, leading to our design guidelines for secure and reliable LEO SCSs (Sec. VIII).

D. Paper Organization

The organization of this paper is illustrated in Fig. 3. Section III presents the background of LEO SCSs. Section IV introduces security and reliability requirements in LEO SCSs. In Section V, the security and reliability issues encountered by LEO SCSs are categorized. Section VI describes solutions for safeguarding LEO SCSs. In Section VII, some open problems and research ideas concerning LEO SCSs are provided. Section VIII provides design guidelines for LEO SCSs. Finally, our concluding remarks for LEO SCSs are provided in Section IX. The acronyms used in this paper can be found in Table XII for convenience.

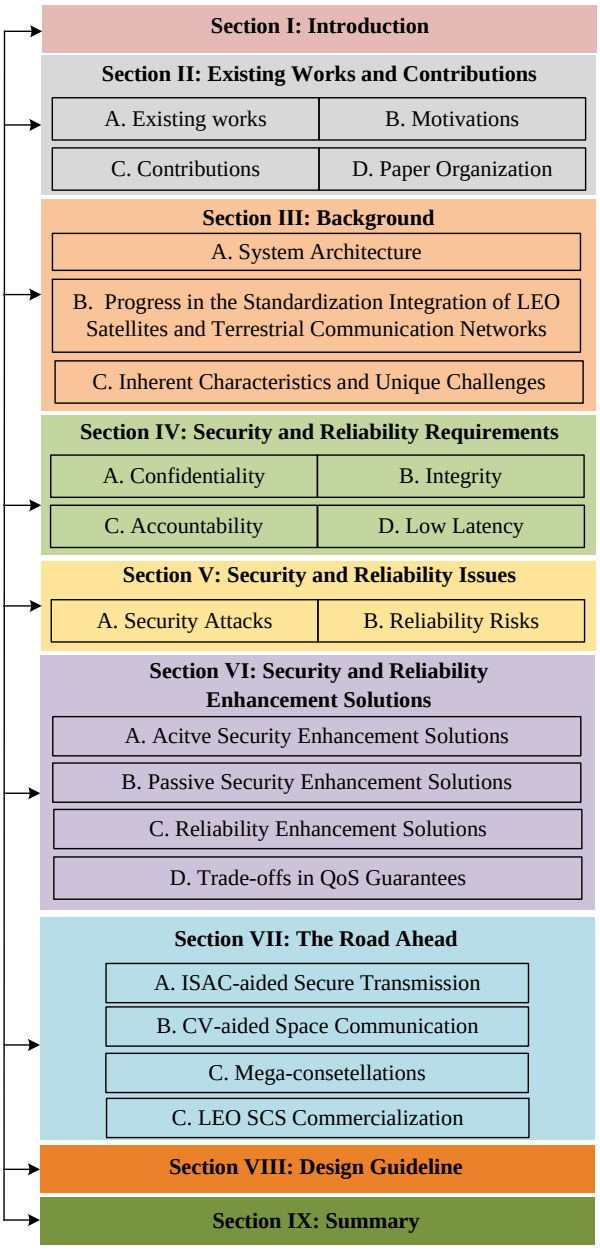


Fig. 3: Organization of this paper.

III. Background

In this section, we first outline the system architecture of LEO SCSs. Then we summarize the current developments concerning LEO constellations and the standard progress of

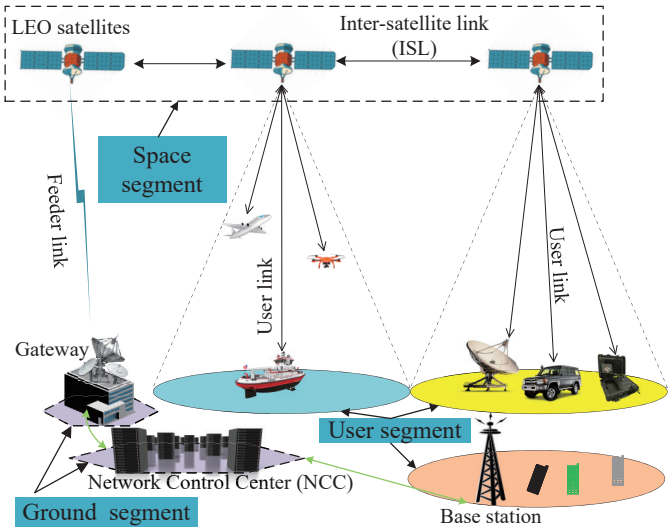


Fig. 4: The system architecture of LEO SCSs.

Non-terrestrial Networks (NTNs) represented by LEO satellites. Finally, the inherent characteristics and unique challenges of LEO SCSs are introduced.

A. System Architecture

As shown in Fig. 4, the system architecture of LEO SCSs is divided into the components of space segment, ground segment, and user segment. The space segment consists of LEO satellites and ISLs, where the LEO satellites are connected by ISLs. However, not all LEO SCSs have ISLs, a counterexample is OneWeb [43]. The ground segment is composed of the gateway and Network Control Center (NCC). The gateway sets up the feeder links for tracking LEO satellites, while the NCC is the center of operation, management, and control for the entire LEO SCS. If there are no ISLs in the space segment, then we have to build enough gateways for ensuring that each LEO satellite is indeed visible. These gateways are connected by optical fiber to jointly ensure the reliable operation of all satellites. Additionally, the NCC is also responsible for the interaction of LEO SCSs with other systems, such as terrestrial mobile communication systems and Wireless Local Area Networks (WLAN). Finally, the user segment includes a large number of terminals. These terminals access LEO satellites via the user link.

B. Progress in the Standardization Integration of LEO Satellites and Terrestrial Communication Networks

LEO satellites were first launched over 50 years ago. The concept of LEO SCSs can be traced back to the 1990s, when the Iridium [44], Globalstar [45], and Orbcomm [25] were designed to provide low-latency voice and data service. However, some of them ended up becoming bankrupt due to the high cost, immature technology, and modest communication capabilities [46]. But thanks to the development of advanced materials, sophisticated technology, and scale of economy, a new LEO SCS age has dawned. In recent years, as a benefit of the ever-increasing demands [47], reduced costs [48], and technological progress, LEO mega-constellations, such as OneWeb, Starlink, and Lightspeed, are making a renewed effort to provide services for 'the other 3 Billion' who do not as yet have access to the Internet. At the time of writing, they tend to evolve towards a converged system, as shown in Fig. 5.

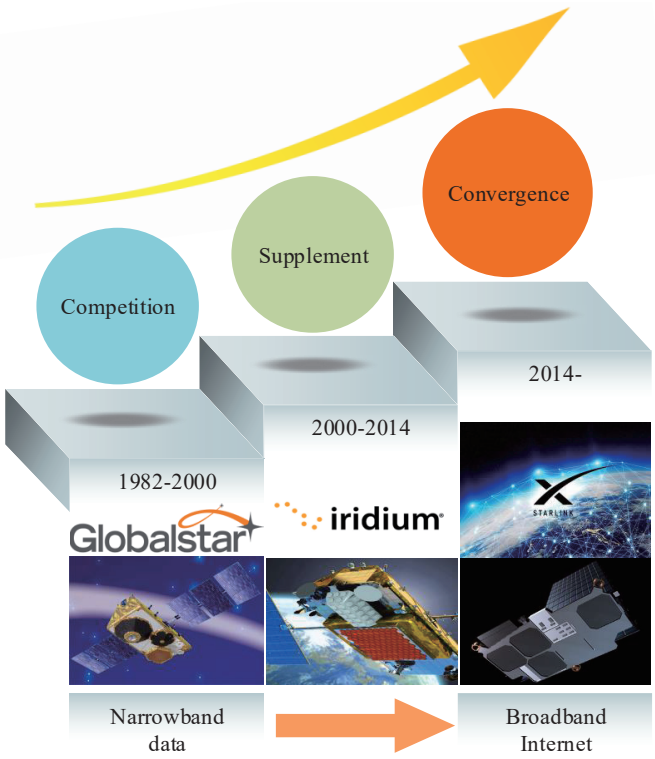


Fig. 5: Development process of LEO SCSs.

Meanwhile, 5G services have been made available to consumers having smartphones, but there is also a significant demand among network operators to offer 5G services to massive Machine Type Communication (mMTC) devices, especially in remote areas [49]. As a result, both the research focus and industrial push are shifting towards NTNs represented by LEO satellites.

The 3rd Generation Partnership Project (3GPP) is a primary international body responsible for defining technical specifications for mobile wireless networks. Enabling the 5G system to support NTNs requires a holistic and comprehensive design that spans numerous areas, primarily including Radio Access Networks (RAN) and Service Aspects (SA).

1) Radio Access Networks: The work on NTNs started in 2017 with a Study Item in Release-15 in 3GPP RAN [50] that focused on deployment scenarios and channel models for NTNs.

After completing this study, 3GPP followed up with the Release-16, which aimed for providing solutions for adapting 5G New Radio (NR) to support NTNs. The main objective of this study is to identify a set of features, including the architecture, higher-layer protocols, and physical layer components, that enable NTNs within the 5G system while minimizing the

impact on the existing 5G system. The outcome of this study is summarized in [51].

The Release-17 Work Item focused on addressing the issues left from the Release-16 study, such as the architecture, frequency synchronization, and Hybrid Automatic Repeat Request (HARQ). Specifically, two possible architectural options are discussed: transparent mode and onboard processing (regenerative) mode. Furthermore, UEs with GPS capabilities can employ their position and the NTNs' ephemeris for predicting and compensating for the Doppler frequency shift [52].

2) Service Aspects: The 3GPP SA workgroup started to discuss the use cases of satellite-based NTNs as part of the Study Item on satellite access in 5G based on Release-15. This study identified three main categories of use cases and service requirements, including serving as an access point for User Equipment (UE) and a backhaul link, guaranteeing coverage for IoT devices, and supporting mission-critical access in disaster situations [53].

Based on this, the 3GPP SA workgroup further identified the main network functions, how these functions were linked to each other, and the information they exchanged [54].

Subsequently, the scope of this work was to identify key issues and provide efficient solutions, such as mobility management, delay in satellite, and Quality of Service (QoS), which are captured in TR 28.808 [55].

Additionally, the 3GPP workgroups approved the study on 5G core network architecture [55] and the operation of IoT NTNs [56].

The deployment of LEO mega-constellations and work at 3GPP provide a potential pathway for closer integration of terrestrial networks and NTNs. At the time of writing, many researchers and commercial companies are tirelessly striving for integrating these two types of networks.

C. Inherent Characteristics and Unique Challenges

Although the development of LEO SCSs is in full swing, they tend to suffer from numerous unprecedented challenges due to their inherent characteristics. Table II summarizes the characteristics of LEO, MEO, and GEO satellites. As seen in Table II, the inherent characteristics of LEO satellites are as follows, and the consequent challenges faced by LEO SCSs can also be clarified.

The Specific Orbit of LEO Satellites Degrades Both the Security and Reliability: LEO satellites are sandwiched between terrestrial communication systems and MEO satellites, which are convenient for attackers. For example, compared to MEO and GEO satellites, ground attackers can achieve the same jamming effect at low jamming power, since LEO satellites are closer to the Earth. By contrast, MEO and GEO satellites can also act as jammers to launch malicious jamming to contaminate the downlink signals of LEO satellites. To make things worse, since the MEO or GEO satellites have a larger coverage area than LEO satellites, a single MEO or GEO satellite may affect many LEO satellites at the same time.

The spectrum crunch imposed by the scarcity of radio resources results in inevitable spectrum sharing between SCSs and terrestrial communication systems. Moreover, the specific location of LEO satellites may also lead to CCI with both GEO SCSs and terrestrial communication systems. Typically, a large number of LEO satellites are sandwiched between the terrestrial communication systems and MEO SCSs. Severe CCI may arise whenever LEO satellites pass through the Line of Sight (LoS) path of a GEO satellite in spectrum sharing scenarios [57].

The High Mobility of LEO Satellites Degrades Both the Security and Reliability: Both the high mobility and limited coverage area of each LEO satellite result in limited time spent above the horizon, hence the ground segment of LEO SCSs should be responsible for the mobility management of terminals. Moreover, in order to prevent malicious intrusion, the ground segment is usually allowed to admit users following authentication [58]. Therefore, both the mobility management and authentication of a massive number of terminals impose severe challenges on the ground segment. Additionally, if there are no ISLs in the space segment, many gateways have to be constructed to support the reliable operation of all satellites, which are prone to hacking attacks.

On a different note, the dramatic increase in the number of LEO satellites will undoubtedly increase the probability of satellite collisions. Moreover, the proliferation of launch activities has caused a surge in LEO space debris, which fly at high speeds and impose severe challenges on the reliable operation of LEO satellites.

The Large Number of LEO Satellites or Gateways Degrades the Security: LEO SCSs have to rely on a large number of gateways (transparent without ISLs, e.g., OneWeb [32]) or multiple satellites (on-board processing with ISLs, e.g., Iridium [59]) to achieve global coverage. A large number of LEO satellites or gateways creates numerous opportunities, respectively.

The Limited Resources of LEO SCSs Degrades Both the Security and Reliability: Both the LEO satellites and the terminals in LEO SCSs have limited power, storage capacity, and computation capability. On the one hand, in order to reduce both the satellite manufacturing and the launching cost, the weight of a typical Starlink satellite is only 227 kg, while the weight of a OneWeb satellite is less than 150 kg [60]. These satellites have to be equipped with small batteries as well as limited fuel and computing equipment.

Compared to the terminals deployed in urban areas, terminals operating in remote areas lack stable power supplies. These terminals have to rely either on the battery carried or on solar panels [61]. Hence, the limited computation and storage capacity of the LEO satellites makes them unsuitable for signal processing with high complexity.

Additionally, the power-limited terminals result in low transmit power, which in turn leads to a low Signal-to-Noise Ratio (SNR) for the signal arriving from LEO satellites, posing serious challenges for reliable reception. Specifically, in order to improve the detection performance of weak signals under the condition of low SNR, the receiver has to increase the coherent integration time, indicating that more data needs to be stored and processed [62].

The Production of Low-cost Satellites Degrades Both the Security and Reliability: The deployment of a large number

TABLE II: Comparison of the main characteristics between GEO, MEO, and LEO satellites

Satellite feature	GEO satellites	MEO satellites	LEO satellites
Orbital altitude	35786 km	2000-20000 km	500-2000 km
Orbital period	24 hours	2 to 8 hours	10 to 50 minutes
Path loss	High	High	Least
Propagation latency	High	High	Low
Coverage	Largest	Large	Small
Satellite life	10-15 years	10-15 years	From a few years up to 10-15 years
Satellite required	At least 3	At least 6	Depends on the design
Deployment time	Depending on the deployment strategy	Depending on the deployment strategy	Depending on the number of satellites per launch and orbit parameters

of satellites in LEO mega-constellations has stimulated the transformation of their production and testing models. Hence, a large number of low-specification components used for LEO satellites are supplied by civilian manufacturers both for cost savings and for reducing the production cycle duration by relying on COTS components. For instance, OneWeb is known to be a pioneer in the mass production of satellites, whose satellite factory in Florida is expected to produce as many as two satellites per day [48]. However, loopholes in production methods and inadequate testing may lead to potential defects in satellites.

In order to support more diverse scenarios and iterative updates of functions, LEO satellites adopt a large number of Field Programmable Gate Arrays (FPGAs), which exhibit flexibility and programmability. However, these FPGAs are also susceptible to the impact of cosmic radiation [63], which can affect the reliability of the programs and algorithms running onboard the satellites.

Quality of Service (QoS) Guarantee When Designing Security and Reliability Solutions: A certain target QoS must be guaranteed by satellite communication service providers for the satellite links. Satellite providers can use these indicators to measure and optimize the performance of their systems, ensuring that users can consistently enjoy a high-quality service experience.

In contrast to terrestrial communication systems, there are different types of services due to the wide coverage of each satellite. With the emergence of compelling services based on LEO SCSs, as seen in Fig. 2, they have to offer differentiated service capabilities. For example, smart mining only requires low-rate data transmission, but a large number of connections, while tele-medicine requires highly reliable, low-latency data transmission to support tele-consultations and remote patient monitoring.

Therefore, when designing solutions to improve security and reliability, it is also necessary to provide QoS guarantees for differentiated services.

IV. Security and Reliability Requirements

Again, the LEO SCSs suffer from both security attacks and reliability risks. The security and reliability requirements of LEO SCSs are specified for the sake of preventing both these attacks and risks, exemplified by eavesdropping, jamming, SEUs, collisions, and so on. For example, maintaining the specific target integrity say in terms of BER constitutes a pivotal security requirement, which refers to reliable reception even in the face of malicious jamming [64]. Philosophically, secure and reliable LEO SCSs should satisfy confidentiality, integrity, availability, and accountability [65], which will be discussed in deeper technical detail in this section.

A. Confidentiality

Confidentiality implies that the transmitted data or information is not disclosed to unauthorized users or groups. However, due to the broadcast nature of the wireless medium, it is vulnerable to eavesdropping, which may cause potential confidentiality violations [66]. In general, the PLS [67] philosophy has been conceived for satellite-to-Earth links, which exploits the random physical characteristics of wireless channels to protect confidentiality. To make things worse, it is necessary to deploy numerous LEO satellites for achieving seamless global coverage. The large number of satellites provides convenience for attackers. Similarly, LEO SCSs without ISLs, such as Oneweb [43], should rely on a large number of gateways for seamless global coverage, which are also tempting for attackers. The above two statements impose more serious challenges to the confidentiality of LEO SCSs.

B. Integrity

Integrity characterizes the accuracy and completeness of confidential information, which must be safeguarded during its transmission. For example, a powerful adversary may jam the wireless user's link by contaminating it with high-power white noise across the entire frequency band. Compared to GEO satellites, LEO satellites are closer to the ground, which makes it easier to contaminate legitimate signals at a lower jamming power. As a solution, the Direct Sequence Spread Spectrum (DSSS) technique may be adopted to counteract it by exploiting its inherent jamming mitigation capability [68].

Furthermore, even in the absence of jamming, the Doppler frequency shift due to the high mobility of LEO satellites also affects the integrity of LEO SCSs.

C. Accountability

Each country or institution has the responsibility to use the space sustainably. As LEO mega-constellations are proliferating, the debris of transportation tools as well as operational

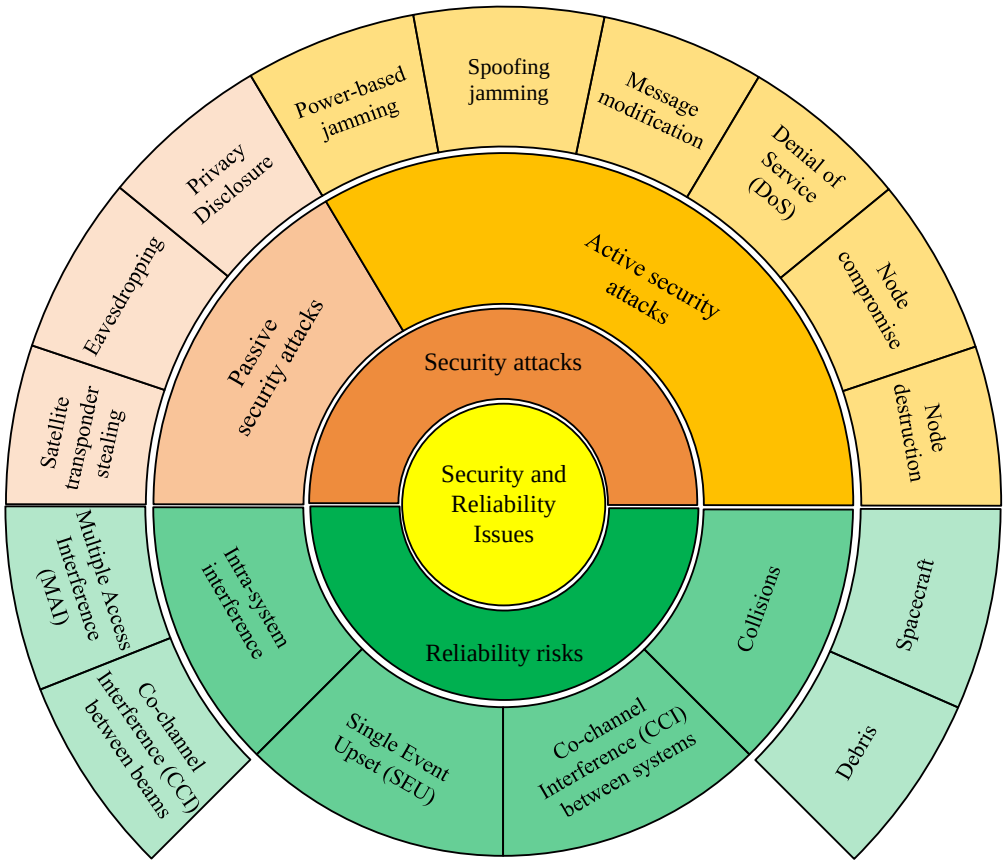


Fig. 6: Classification of security and reliability issues.

or retired satellites make the low Earth orbit increasingly crowded, thus requiring debris removal measures, for reducing the above-mentioned deleterious impact on space. Additionally, considering the scarce spectral resources, LEO SCSs and GEO SCSs have to rely on spectrum sharing according to the International Telecommunication Union (ITU) regulations [69]. In this context, LEO SCSs shall not impose excessive interference on GEO SCSs.

D. Low Latency

Having low latency and high security is also a desirable feature of 6G networks. The end-to-end latency is given by the sum of the propagation delay, the processing latency, and the queuing delay. An LEO satellite at 600 km orbit altitude has, for example, a 4 Milliseconds (ms) uplink/downlink turnaround propagation delay at the speed of light, which is perceptually unobjectionable for voice calls. However, the G.729 speech code would add 10 ms [70] processing delay at both the encoder and decoder, which may escalate further owing to the channel coding and queuing delays. Hence it is imperative to conceive low-latency security solutions for supporting secure delay-sensitive services in tele-medicine and emergency rescue.

Remarks: The QoS terminology includes numerous metrics, such as latency, traffic rate, Bit Error Rate (BER), voice and video quality, etc.

Although all the above-mentioned security and reliability requirements are of paramount importance, it is challenging to simultaneously satisfy all of them. Indeed, typically trade-offs must be struck. For example, to improve the confidentiality in the uplink without any powerful secrecy coding, the conventional approach is to reduce the terminal's transmit power. However, the system's integrity will also be reduced simultaneously. Conversely, by increasing the transmit power to improve the desired link's integrity, the probability of eavesdropping will also be inevitably increased [71]. Suffice it to say that further research is required for the multi-component Pareto-optimization of the system to determine all optimal operating points of the non-dominated set of solutions [72]. None of the metrics in these optimal solutions can be improved without degrading at least one or several of the others.

V. Security and Reliability Issues

LEO SCSs support more and more civilian and military applications, thus it is of paramount importance to eliminate their issues. In this section, we focus our discussions on the issues of LEO SCSs, which are shown in Fig. 6 at a glance. In addition to the security attacks by potential adversaries that the existing magazine and survey papers focus on [18], [28], [40], [65], [73], [74], there is a whole host of other issues, which are not due to the presence of attackers as exemplified by SEUs, collisions, and so on. To this end, the issues of LEO SCSs can be classified into security attacks and reliability risks.

These two categories also have their respective subclasses. Furthermore, based on this classification, we further analyze and infer the characteristics of these issues, such as attribution, reversibility, awareness, and collateral damage. We will continue by highlighting several lessons learned from these issues and use them as a springboard for conceiving potent security and reliability enhancements.

A. Security Attacks

LEO SCSs provide a powerful platform for military applications, which are hence prime targets for hostile attacks. Their ground segments are responsible for all interactions with other terrestrial communication systems, and these facilities create opportunities for attackers.

Considering the activity of the attack, security attacks can be further classified into passive and active security attacks, and both of them are detailed below.

1) Passive Security Attacks: The most crucial thing in passive security attacks is that the victim does not get informed about the attack. Passive security attacks may cause the loss of confidentiality. Two types of passive security attacks are eavesdropping and satellite transponder stealing.

Eavesdropping: The open nature of wireless propagation makes legitimate transmissions vulnerable to the interception and interpretation of signal or message. Eavesdropping attacks do not require high technical capabilities, only individuals or commercial competitors can deploy a number of drones to obtain an opportunity to overhear the user link due to frequent access caused by the high mobility of LEO satellites. Furthermore, the large number of LEO satellites also provide convenience for eavesdroppers. Additionally, eavesdroppers will analyze and extract useful information to create future attacks. DSSS and PLS techniques are separately used for mitigating the eavesdropping [75]–[77].

Furthermore, perturbing the normal behavior or stealing secret information may also occur during the design and during runtime due to hardware issues. To proceed one step further, given the explosive proliferation of LEO satellites, many manufacturers would prefer using COTS components to increase their production rate at a reduced cost. However, some COTS components may also open the door for attackers. For example, the authors of [78] discussed the security threats that arise from the adoption of the well-known Reduced Instruction Set Computer V microprocessor operating on board of satellites. They demonstrated how hardware trojan horses and microarchitectural side-channel attacks might compromise the overall system's operation by stealing confidential information.

Satellite Transponder Stealing: Satellites with the merits of wide coverage and free from natural disasters have attracted widespread attention. However, their high cost and advanced technology make it possible for only a few countries or institutions in the world to produce. In this case, Some criminals without satellite production capabilities exploit existing satellites to quietly complete their own transmissions. Existing satellites mainly include on-board processing, and transparent forwarding [79]. Between them, transparent forwarding satellites are more likely to be exploited by criminals seen in Fig. 7, because they do not perform any signal processing [80]. Hence, it is not possible to determine whether the received data is from a legitimate user. When attackers send their illegal signals, the satellite will still forward the signals [81].

In order to use the satellite transponder secretly, attackers need to conduct some research to obtain the specific parameters of the satellite transponder, such as operating frequency, satellite orbit information, etc. In addition, the DSSS techniques at a low Power Spectral Density (PSD) are adopted to bury themselves under the legitimate frequency band, as shown in Fig. 7. Regular replacement of satellite operating parameters, such as operating frequency, may prevent this type of attack.

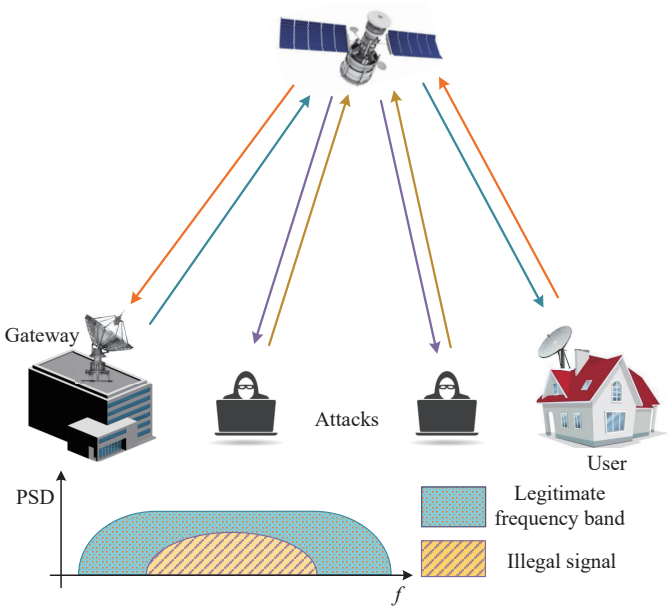


Fig. 7: Illustration of transponder stealing.

Privacy Disclosure: As mentioned in [82]–[84], compared to GEO satellites, LEO satellites have the merits of low path loss and propagation delay. Hence they are capable of supporting access to the IoRT in upcoming 6G communication systems, as shown in Fig. 2(a). However, the sharing and process of LEO satellite-based IoRT data may lead to the invasion of user privacy. Mass data of the registered User Equipments (UEs) has to rely on a large number of gateways (transparent without ISLs, e.g., OneWeb [32]) or multiple satellites (on-board processing with ISLs, e.g., Iridium [59]) to exchange worldwide. However, some of the data may contain sensitive information. For example, to reduce the delay of handover [85] among LEO satellites for achieving high-precision continuous user tracking, the location of UEs has to be shared among gateways or satellites [86]. Usually, the location of each UE can only be accessed by authorized individuals (e.g., designated service providers or insurance agents). Once this data is shared, it is beyond the owner's control and may be illegally accessed by unauthorized parties, leading to a high risk of data misuse. Moreover, once an attacker obtains access to user location information, this may trigger subsequently irreversible attacks, even potential physical destruction.

2) Active Security Attacks: For active security attacks, malicious acts are performed to disrupt or even damage the system operation. Hence the victim gets informed about these attacks. Active security attacks are dangerous to integrity as well as availability. The most common forms of active security attacks contain power-based jamming, spoofing jamming, message modification, DoS, node compromise, and node destruction. Detection-based methods are adopted for minimizing the impacts of issues and speeding remediation [87]–[89].

Power-based Jamming: A simple strategy to disrupt the legitimate signal reception by releasing the power-based jamming upon wireless user link of LEO SCSs [90]. Most of the on-orbit satellites adopt the so-called bent-pipe[1] transponder without digital signal processing, so it is easy to encounter signal power-based jamming attacks. Attackers may easily perturb the satellite's operation by transmitting high-power jamming signals [91]. If the jamming power is too high, it may at worst 'fry' the receiver front end of the satellite. There are many types of jamming signals and classification methods. Zou *et al*. [92] classified jamming based on the grade of difficulty generating them and compared the different types of jamming schemes in terms of their energy efficiency, how disruptive their interference is, their complexity, and the prior knowledge.

Due to the long open wireless link between LEO satellites and the Earth, the adversary may contaminate it by jamming at different locations, which can be divided into the types illustrated in Fig. 8. The space-based jamming is mainly released by spacecraft. This type of jamming has an extensive range over which it may disrupt the downlink transmission, but it has limited jamming time and power owing to having limited time above the horizon.

The adversary may generate air-based electronic jamming from aircraft or airships. As electronic-jamming aircraft and airships have more flexibility than their space-based counterparts, they are suitable for releasing burst-type jamming. Compared with space-based jamming, the power of air-based jamming is typically higher. Because airships are generally located between ground users and LEO satellites, they can interfere with the desired communication during both uplink and downlink transmissions.

The power of ground-based jamming is typically high, and the jamming style is diverse because ground-based jamming is maliciously released by large-scale fixed, vehicle-mounted, or ship-borne jamming stations having abundant resources and power. Ground-based jamming mainly affects the uplink transmissions. There are many types of ground-based jamming, but distance is not a dominant factor. Ground-based jamming is usually of a blocking nature, which directly blocks the satellite transponder. These three types of power-based jamming are compared in Table III. As a remedy, both temporal domains adaptive filtering [93] and transform domain adaptive filtering [94] are efficient methods for jamming mitigation.

Spoofing Jamming: Spoofing jamming is a form of more insidious electronic attack where the attacker tricks a receiver into believing in the genuine nature of a malicious signal produced by the attacker. Compared with power-based jamming, spoofing jamming is more technical. The attacker must fully understand the signal characteristics, including physical layer waveform, frame structure, etc., to forge its equivalent and confuse legitimate receivers. For example, spoofing jamming often occurs in the civilian GPS. It is easy for the adversary to release spoof GPS signals to provide false information because the format of the civilian GPS signal is known [95]. Similar to GPS, there is usually a dedicated downlink pilot channel for broadcasting channel status, user management information, call information, etc., as exemplified by Iridium [59]. Attackers can imitate the dedicated pilot channel to broadcast false information to legitimate users, causing network paralysis. Fortunately, there are some standard methods to alleviate spoofing jamming, such as energy detection, multiple antennas [96], and authentication. However, energy detection and multiple antennas increase the terminal complexity. Hence, the most effective approach is to apply authentication for LEO SCSs. The authors of [97] proposed an Unmanned Aerial Vehicle (UAV)-assisted authentication method to tackle spoofing jamming.

TABLE III: Comparison of power-based jamming

Jamming types	Space-based jamming	Air-based jamming	Ground-based jamming
Jamming power	Low	Medium	High
Jamming time	Burst	Burst	Continuous
Resources	Limited	Limited	Rich
Mobility	Poor	Strong	Poor
Sphere of action	Large	Medium	Small
Scenarios	Downlink	Downlink Uplink	Uplink

Message Modification: Message modification means that a hacker intercepts messages and changes their contents, which contains message change, message insertion, and message deletion. Message modification is more likely to occur in the ground segment, where the hacker illegally obtains the data operation permission and modifies the message. Subsequently, these modified messages may result in some wrong decisions. To combat the message modification attack, existing SCSs typically consider the employment of Intrusion Detection Systems (IDS) and encryption algorithms [98].

Denial of Service: A DoS attack is that a hacker means to shut down a device or network, making it inaccessible to its intended users. A DoS attack tends to occur in the ground segment and the space segment of LEO SCSs. There are many methods for carrying out DoS attacks. The most common method of attack occurs when a hacker floods a network server with traffic. In this type of DoS attack, the hacker sends requests to the target satellite all the time. The target satellite is busy responding to these illegal requests, resulting in authorized users being ignored. On the other hand,

[1]Many satellites send back to Earth what goes into the satellite with only amplification and a shift from uplink to downlink frequency, like a bent pipe. A bent-pipe satellite does not demodulate and decode the signal.

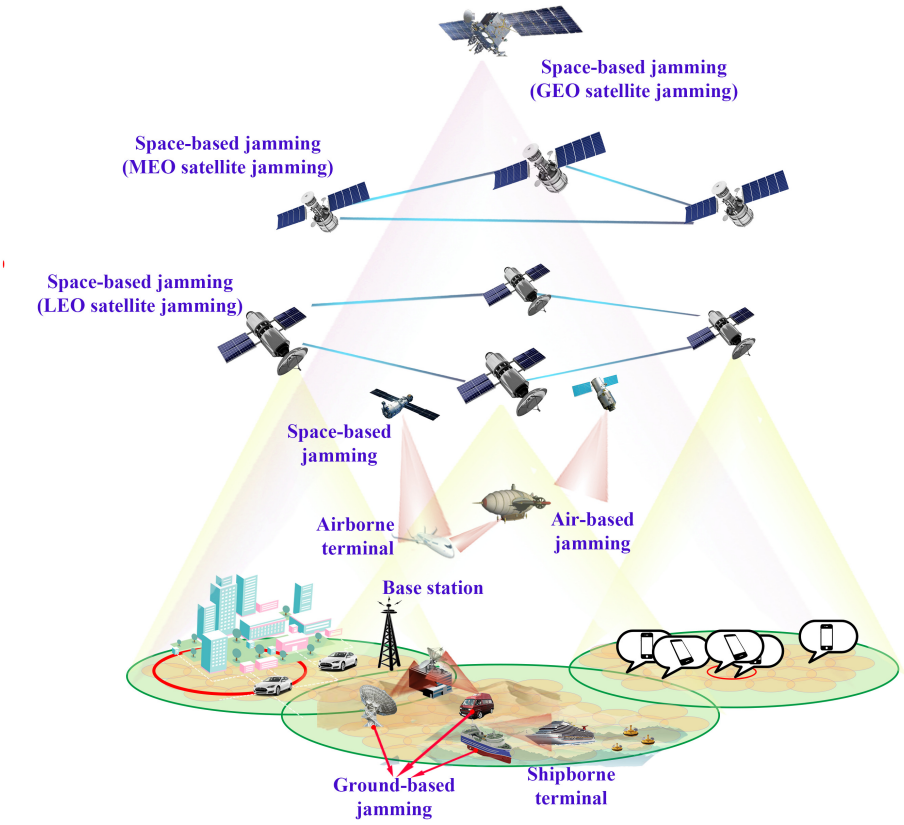


Fig. 8: Sources of power-based and spoofing jamming contaminating LEO SCSs.

the ground segment is responsible for the authentication of legitimate users. The hacker may forge a legitimate user in the ground segment to request authentication. As the junk requests are processed constantly, the ground segment is overwhelmed.

Attackers also exploit issues or device weaknesses to orchestrate a synchronized DoS attack to a single target, which is co-called Distributed DoS (DDoS). The IoT botnet in which malware source code was leaked in early 2015 is a typical paradigm of DDoS attacks [99] in terrestrial IoT networks. IoT botnets, created as hackers, infect numerous IoT devices and recruit them to launch large-scale DDoS attacks. Furthermore, with the continued proliferation of LEO mega-constellations, the large number of LEO satellites also become the potential target of DDoS attacks [100]. These attacks are difficult to detect and mitigate because they use hit-and-run tactics that originate from numerous IoT vectors distributed around the world [101].

Node Compromise: A legitimate node may be attacked by an attacker under the control of malicious algorithms, programs, or software, potentially threatening the entire network [102]. These compromised nodes may lead to some collateral damage. For example, these compromised nodes can deliberately leak confidential information to attackers. These compromised nodes may also trick other legitimate nodes into compromised nodes [103]. Moreover, an attacker may exploit a compromised node and pretend to be a legitimate user and device again to usurp system resources [104]. It is challenging to detect compromised nodes because the behaviors between these compromised nodes and legitimate nodes are hard to distinguish. Using code patches is a common method of mitigating the probabilities of these events [105].

Moreover, with limited memory and processing capacity, many satellites do not even have complicated encryption algorithms to protect themselves. To this end, some hackers may hijack a satellite as a compromised node by taking over its feeder link. For example, A group of hackers once controlled a satellite by its feeder link and further tried to change its orbit. Hackers also used the hijacked satellite for extortion [106]. Even worse, hackers could control satellites to achieve self-destruction by malicious commands, or they can use special tools to trick satellites and ultimately use them to attack other satellites or space assets.

Node Destruction: Both the space segments as well as ground segments and terminals are subject to the risk of being destroyed. In the satellite-IoT applications supported by LEO SCSs, the power-limited terminals, such as oceanic buoys, operating without advanced security protection algorithms may become captured by an adversary [107]. Additionally, LEO satellites are potential targets for anti-satellite weapons, such as missiles and high-power laser beams.

Lessons Learned: Table IV summarizes the important differences between active and passive security attacks. As mentioned in [19], passive security attacks, such as eavesdropping, typically aim for stealing confidential information, such as passwords and messages. By contrast, active security attacks [92], [105], including message modification, DoS, node

compromise, and so on, may be carried out based on the results of passive security attacks. Attackers often exploit the confidential information stolen during passive eavesdropping attacks for performing active security attacks. Moreover, active security attacks may cause severe collateral damage when hostile nodes pretend to be legitimate ones and occupy valuable resources [104].

B. Reliability Risks

Apart from security attacks, the harsh working environment, crowded orbits, and spectrum crunch result in reliability risks, which may threaten the normal operation of LEO SCSs. These threats include intra-system interference, CCI between systems, SEUs, and collisions, which will be described in detail.

1) Intra-system Interference: Intra-system interference contains MAI [108], and CCI between beams [109], which are separately caused by physical waveform selection and the scarce spectrum.

MAI: Spread Spectrum (SS) techniques are eminently suitable for LEO SCSs in military applications, which are immune to most types of interference to a certain extent. However, it is difficult to avoid the near-far effect caused by MAI. Power control and multi-user detection are common methods of mitigating these near-far effects [45]. Additionally, the careful choice of SS codes may mitigate the near-far effects. Orthogonal complementary codes have been chosen to substantially mitigate MAI [110]–[112]. However, these orthogonal codes are sensitive to frequency shifts, which must be mitigated by future research.

CCI between Beams: Multi-beam satellites reuse the available frequencies within their coverage to increase capacity. However, frequency reuse among beams may cause CCI in the overlapping areas when some beams rely on the same frequency [109], especially in adjacent beams using the same frequency. The angular side-lobes of the beam radiation patterns create interference leakage, seen in Fig. 9. The interference level is typically quantified in terms of the Carrier to Interference Ratio (CIR) [113]. Clearly, the interference limits the attainable capacity. To improve the capacity, Transmit Precoding (TPC) techniques relying on transmitter-side channel state information can be applied to mitigate the interference. A potent scheme based on hybrid wide-spot beams was designed to alleviate this source of interference in [79]. The main philosophy of this scheme is that the space-borne payload generates several fixed wide beams for providing wide-range coverage to increase the frequency reuse distance. On this basis, the space-borne payload also adopts some high-gain spot beams for enhancing the capacity in tele-traffic hot spots.

Lessons Learned: Compared to terrestrial communication systems, LEO satellites have a wider coverage area. Some public areas have higher access requirements, such as airports or railway stations. By contrast, some regions, such as deserts, oceans, etc., have a low access demand. Hence it is suboptimal to have fixed frequency reuse within each satellite. For example, although the frequency reuse pattern may be appropriately adjusted to satisfy the high access demands in hotspot areas, the associated CCI between beams also affects the regions having low access requirements. By contrast, the frequency pattern may also be adjusted for reducing CCI between beams, but then it cannot satisfy the access requirements of hotspot areas. To make things worse, LEO satellites fly over many regions, hence the resultant time-varying and unbalanced services pose a more serious challenge for the control of frequency reuse.

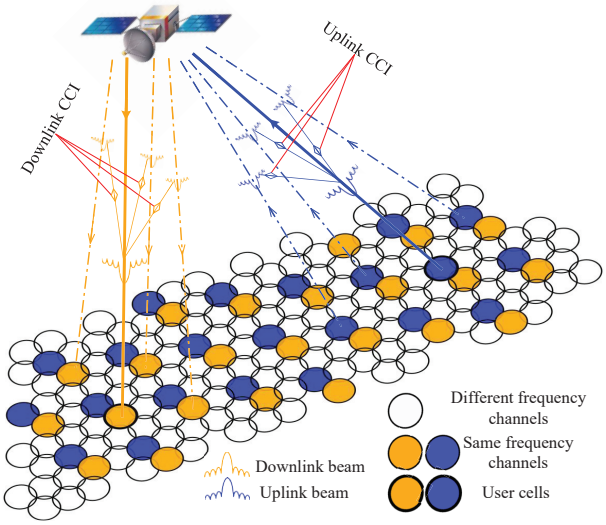


Fig. 9: Depiction of the satellite uplink and downlink CCI.

2) CCI between Systems: CCI between systems is essentially spectrum sharing between LEO SCSs and other systems, such as GEO SCSs and terrestrial mobile communication systems. An increasing number of LEO satellites has been deployed over the last few years, but the available radio spectrum remains limited. So LEO SCSs require high spectral efficiency to address the spectrum scarcity problem. Furthermore, GEO SCSs have to coexist within the same spectrum to achieve this objective. Consequently, the high-level CCI between LEO and GEO SCSs is unavoidable. When LEO satellites [114] approach the equator, they tend to inflict increased interference upon GEO satellites operating within the same frequency band, as shown in Fig. 10. According to current ITU regulations [69], it is mandated to consider the spectrum sharing between GEO and LEO SCSs. LEO SCSs shall not impose unacceptable interference on GEO SCSs. In other words, GEO SCSs are regarded as the Primary User (PU), while LEO SCSs are regarded as the Secondary User (SU). Thus interference coordination is imperative for mitigating the interference.

Lessons Learned: The impact of CCI encountered by LEO SCSs is set to become more serious in the future, since the next-generation networks will provide ubiquitous connectivity through the convergence of terrestrial systems, LEO SCSs, and GEO SCSs [115]. However, the coexistence of LEO SCSs and GEO SCSs has to be carefully planned. Adding terrestrial systems to the mix makes an already complicated picture more complex.

Since the GEO SCSs [116] and the terrestrial mobile communication systems [117] have higher priority access to the existing spectrum, LEO SCSs having lower priority have to

TABLE IV: The differences between the active and passive security attacks

Characteristics	Passive security attacks	Active security attacks
Awareness	Not be aware	Aware
Against on	Confidentiality	Integrity as well as availability
Impact on system	There is no any harm to system	System is damaged, its degree of damage depends on the type of active attacks
Countermeasure	Prevention and mitigation	Detection and mitigation
Technical capacity	Simple to implement	Requires sophisticated technical capacities
Degree of difficulty to deal with	Easy to mitigate compared with active attacks	Tough to restrict

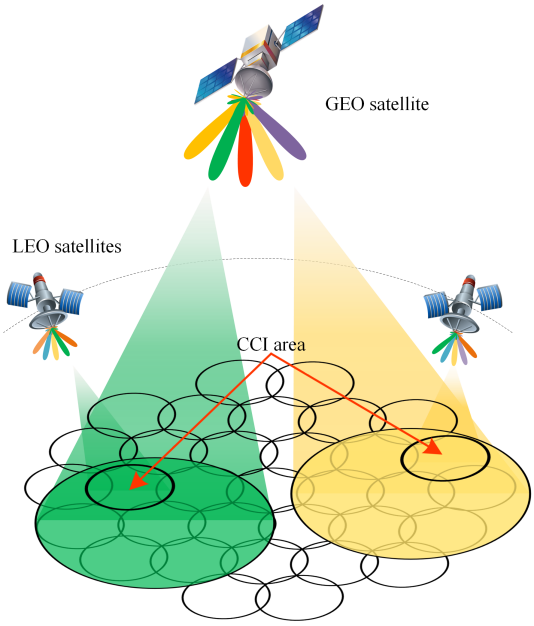


Fig. 10: CCI between LEO and GEO SCSs.

do their best to mitigate the CCI. The evolution of 6G systems stimulates the explosive proliferation of LEO satellites [118], which undoubtedly increases the probability of CCI between LEO SCSs. Therefore, it will continue to attract wide attention.

3) Single Event Upsets: The particles existing in cosmic radiation generate a large number of electrons and holes in the incident path by ionization. Electronic devices like FPGAs collect these charges, which may cause transient faults. If the charge exceeds the maximum level that the device can withstand without SEUs, the logic state of the circuit will be inverted. However, the circuit can be restored to its original working state by rewriting or resetting. Hence, SEUs constitute reversible soft errors [119].

The probability of SEUs is related to the orbit altitude and orbit inclination[2]. The authors of [121] investigated their effects on SEUs, and the results showed that at altitudes below 2000 km, the higher the orbit altitude, the higher the probability of SEUs occurrence. On the other hand, the closer the orbit inclination is to 90°, the higher the probability of SEUs occurrence.

[2]Orbital inclination measures the tilt of an object's orbit around a celestial body. It is expressed as the angle between a reference plane, and the orbit plane or axis of direction of the orbiting object [120].

The nature of SEUs is hardware-dependent. Compared to FPGAs, Application Specific Integrated Circuits (ASICs) exhibit better resistance to SEUs, but they lack flexibility. Therefore, FPGAs are widely used in LEO satellites as a benefit of their high performance and flexibility. To ensure the reliable operation of FPGAs in-orbit, it is necessary to employ SEUs prevention measures, such as Triple Module Redundancy (TMR) technique and periodical refreshing.

4) Collisions: In recent years, the launch activities have been increasing for LEO, MEO, and GEO satellites. The different orbit regions are unevenly populated. It is seen from Fig. 11 that the LEO orbits between 800 and 1400 km constitute the most crowded space fuelled by the miniaturization of satellites and the deployment of mega-constellations. Crowded space in LEOs increases the risk of collisions, threatening the regular operation of satellites or spacecraft. Even worse, LEO satellites or spacecraft move around the planet at about 7 km/s, and their relative speed may be 10 km/s or higher. At this speed, even a tiny piece of debris presents a serious hazard for satellites or spacecraft. Hence, it is clear that LEO has to be treated with a special interest. Collisions occur not only between spacecraft but also between spacecraft and space debris. Table V summarizes the publicly reported collision avoidance and collision accidents in LEOs in the past 20 years.

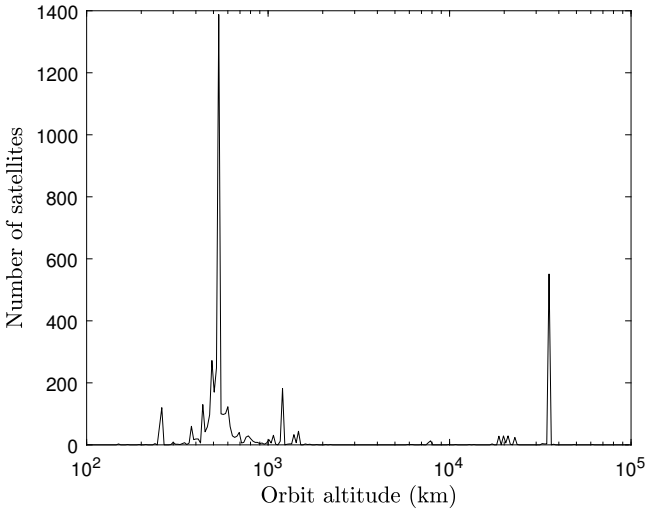


Fig. 11: Launch of satellites in different orbits during Jan. 2012 and Dec. 2022 [122].

TABLE V: Publicly reported collision avoidances and collision accidents in LEOs

2007	Orbital debris completely penetrated one of the radiator panels of the shuttle Endeavour [123].
2009	The active Iridium 33 and the derelict Russian military Kosmos 2251 collided above Siberia [124].
2013	Russian Satellite called BLITS crashed with the derelict Chinese Fengyun 1C satellite [125].
2013	Ecuador's NEE-01 Pegaso collided with Argentina's CubeBug-1 [126].
2013	A tiny Ecuadoran satellite collided in space with the remains of a Soviet rocket [127].
2015	A millimeter-sized debris hit a solar panel on the ESA Sentinel-1A satellite [128].
2016	A piece of space debris chipped one of the International Space Station's huge windows [129].
2019	Aeolus satellite belong to ESA performed a maneuver to avoid a potential approach to the Starlink 44 [130].
2021	Yunhai-1 02 collided with the debris from the Zenit-2 rocket body launched Tselina-2 in 1996 [127].
2021	China Space Station has successfully conducted two evasive maneuvers to avoid potential collisions with Starlink separately in July and October [131].
2021	The Arirang-1 satellite raised its orbit to avoid collision with debris [132].
2021	The Canadarm2 robot arm on the International Space Station was struck by space debris [133].

Collisions with Spacecraft: Given so many spacecraft belonging to different agencies entering LEOs, it is difficult to manage them collaboratively. Even worse, the orbits are constantly changing under the action of non-sphericity of the earth, ocean tides, and atmospheric damping, which results in the spacecraft deviating from their pre-set orbits. As a matter of fact, in 2009, the Iridium 33 satellite collided with the scrapped Russian Cosmos over Siberia, producing at least thousands of debris [124]. This space debris was fixed only a few months later, distributed between 500 km and 1300 km. As a remedy, collision avoidance control has to be carried out to reduce the risk of collisions with LEO satellites. On Sep. 2, 2019, the European Space Agency (ESA) made an emergency steering of the Aeolus satellite, successfully avoiding a space 'car accident' with Starlink-44 [130]. As reported by United Nation Office for Outer Space Affairs, the China Space Station has successfully conducted two evasive maneuvers to avoid potential collisions with the Starlink-1095 satellite on Jul. 1, 2021, and the Starlink-2305 satellite on Oct. 21, 2021, respectively [131].

Collisions with Debris: Again, such frequent deployment activities have also led to a surge in space debris. Most orbit debris is human-generated objects, such as pieces of spacecraft, tiny flecks of paint from a spacecraft, parts of rockets, and decayed satellites. According to the ESA, there are approximately 1036500 debris objects larger than 1 cm estimated by statistical models to be in orbit [134]. There are close to 6000 tons of materials in LEOs. Most 'space debris' moves fast, reaching speeds of 18000 miles per hour, almost seven times that of bullets. They expose LEO satellites to the Kessler phenomenon[3]. Specifically, the density of space debris in LEO is high enough to cause cascade collisions, which adversely affects space exploration. With the advent of standardized production, the satellite development cycle and constellation deployment cycle have been substantially shortened, but there are also satellite failures, potentially requiring replacements during the deployment. Hence, Kessler's hypothesis is becoming a reality.

As a matter of fact, collisions with debris at LEO orbits have already occurred [123], [128], [133], [136]. Explicitly, ESA has showcased the solar cells retrieved from the Hubble Space Telescope, which have been damaged by various collisions with space debris. In 2007, orbit debris completely penetrated one of the radiator panels of the shuttle Endeavour. On Aug. 23, 2015, ESA engineers discovered that a solar panel on the Sentinel-1A satellite was hit by a piece of millimeter-sized debris, according to space-borne cameras. Fortunately, this satellite still remained capable of operating normally. A piece of space debris struck the International Space Station's Canadarm2 robot arm, which was spotted on May 12, 2021.

Because of these incidents, it is routine for operators of satellites in dense orbits to spend time tracking the collision risk. When the probability of collision exceeds a specific limit, debris avoidance maneuvers have to be planned. For example, Indian Space Research Organisation (ISRO) reported that they monitored 7600 satellite collision threats in 2021 and avoided 60 since 2015 [137]. Moreover, the International Space Station has carried out as many as 29 debris avoidance maneuvers since 1999 [138]. However, due to its excessive fuel consumption, the technical solutions in [138] are not suitable for low-cost LEO satellites with limited energy. Debris tracking [139]–[141], space probe [142], [143], debris removal [144] are separately efficient methods for detecting and preventing collisions.

Lessons Learned: Table VI summarizes, classifies, and compares the issues encountered by LEO SCSs in terms of their types, damaged locations, security and reliability requirements, and so on. In summary, the critical lessons learned from the in-depth review of the issues are as follows.

The authors of [74] discussed the specific characteristics of attackers, while the authors of [28], [40], [65] classified the related issues. Indeed, the identity and technical capabilities of attackers determine the type of security attacks, and different types of security attacks result in different levels of damage. Since eavesdropping attacks inflict no harm upon the entire system, only those malicious individuals, who know the target satellite's operating frequency and orbit information, can have the opportunity to steal confidential information, for example,

[3]The Kessler phenomenon, proposed by National Aeronautics and Space Administration (NASA) scientist Donald J. Kessler in 1978, is a chain reaction in which the resulting space debris would destroy other satellites and so on, with the result that LEO would become unusable [135].

TABLE VI: Analysis, classification, and comparison of issues

Issue types	Damaged location	Damaged type	Security&reliability requirements	Reversibility	Apparency	Intended solutions	Collateral damage
Eavesdropping	Wireless link	Security	Confidentiality	Reversible	Inapparent	Prevention Mitigation	Could create active attacks
Satellite transponder stealing	Wireless link	Security	Confidentiality	Reversible	Inapparent	Prevention	None
Power-based jamming	Wireless link	Security	Integrity	Depending on the attackers	Apparent	Mitigation	Could leave target disabled
Spoofing jamming	User segment Space segment	Security	Availability	Reversible	Apparent	Detection Mitigation	Could leave target disabled
Message modification	Ground segment	Security	Integrity	Reversible	Apparent	Detection Mitigation	Could lead to wrong decisions
DoS	Ground segment Space segment	Security	Availability	Reversible	Apparent	Detection Mitigation	Could leave target disabled
Node compromise	User segment Space segment	Security	Availability	Irreversible	Apparent	Detection Mitigation	Could leave target disabled
Node destruction	User segment Space segment	Security	Availability	Irreversible	Apparent	Detection Mitigation	Could generate more space debris
MAI	Ground segment Space segment	Security	Integrity Availability	Reversible	Apparent	Mitigation	None
CCI between beams	Ground segment Space segment	Security	Integrity Availability	Reversible	Apparent	Mitigation	None
SEU	Space segment	Reliability	Integrity	Reversible	Apparent	Prevention Mitigation	Could lead to wrong decisions
CCI between systems	Ground segment Space segment	Security	Integrity Availability	Reversible	Apparent	Mitigation	None
Collisions with spacecraft	Space segment	Reliability	Availability	Irreversible	Apparent	Detection Mitigation	Could generate more space debris
Collisions with space debris	Space segment	Reliability	Availability	Irreversible	Apparent	Detection Mitigation	Could generate more space debris

by launching eavesdropping drones [145]. Suffice it to say that irreversible damage may be inflicted upon satellites by anti-satellite weapons owned by a national army, for example, because individuals normally do not have the capability of manufacturing weapons.

Compared to the ground segment and the user segment, the security of the space segment is more critical. As detailed in [146], the power, storage, and computing capability of LEO satellites is severely limited, rendering the specific class of security algorithms having high complexity and storage requirements inapplicable. Moreover, it is inconvenient to modify a satellite for incorporating security enhancements from an operational perspective. Additionally, owing to their harsh environment, LEO satellites tend to suffer from the risk of both SEUs as well as collisions, and the consequences of collisions are irreversible. To make things worse, debris generated by collisions could potentially cause further collisions [147].

Proficient orbit selection is extremely critical. Specifically, in order to reduce the risks of SEUs and collisions, orbits having only a few satellites on their adjacent orbits should be preferentially picked, as shown in Fig. 10. The authors of [121] provided the evidence that the higher the orbit altitude, the higher the probability of SEUs occurrence in LEOs. Therefore, it is difficult to find a beneficial orbit altitude that guarantees both low collision and low SEUs probability. Having an orbit altitude chosen for reducing the probability of collisions has a higher priority than that reducing the probability of SEUs. Given that the damages caused by collisions are irreversible [128], it is difficult to conceive solutions to repair the damaged satellites. In addition, the closer the orbit inclination is to 90°, the more seamless the global coverage becomes [148], but the probability of SEUs is also increased.

VI. Security and Reliability Enhancement Solutions

In this section, *prevention*, *detection*, and *mitigation* constitute essential principles closely linked to both security and reliability enhancement solutions [18].

- **Prevention**: Prevention focuses on protecting LEO SCSs from issues before they are exposed to LEO SCSs. The employment of Terahertz (THz) and laser techniques is capable of coping with CCI by avoiding frequency-reuse in the immediate vicinity [149]. Moreover, deploying firewalls and antivirus software and applying patches for the issues identified can dramatically reduce the probability of successful attacks. Additionally, prevention is also vitally critical concerning 'fatal' issues, such as

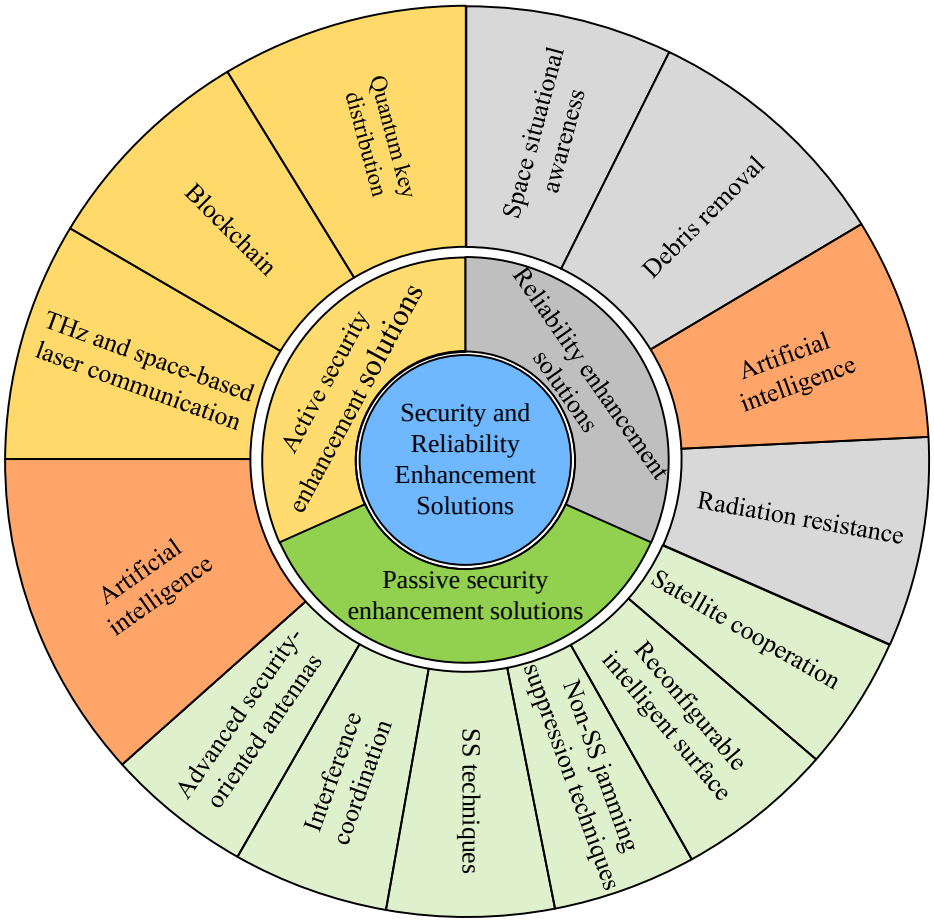


Fig. 12: Classification of solutions dealing with security and reliability in LEO SCSs.

collisions, because the resultant damage is clearly irreversible. Although prevention is desired to avoid potential security incidents, it is not always feasible.

- **Detection**: Prevention usually aims for improving its existing defense mechanism. However, once an attacker succeeds in circumventing the existing preventative solutions, this must be detected to minimize its impact. Usually, IDS is adopted for detecting the attacks and for mitigating the damage inflicted [150].
- **Mitigation**: Mitigation refers to the specific solutions put in place to help prevent issues as well as limit the extent of damage when security attacks do happen. Again, SS techniques are still popular due to their immunity to jamming and eavesdropping [151].

In light of this, we further classify solutions into active and passive solutions. Active solutions include the functions of prevention and detection, thus making LEO SCSs more proactive in the face of issues. By contrast, passive solutions must directly face these issues and reduce or eliminate their impact as far as possible. To this end, a series of security and reliability enhancement solutions are presented in Fig. 12. In addition, several trade-offs and the critical lessons learned from these solutions are also summarized.

A. Active Security Enhancement Solutions

Active security enhancement solutions, including QKD, blockchain, THz, space-based laser communications, and AI, aim for preventing or actively detecting impending deleterious issues. Among them, QKD constitutes a symmetric secret key negotiation protocol capable of maintaining information-theoretic security, and it has evolved from academic research to off-the-shelf commercialization [152]. Furthermore, blockchain is capable of satisfying the security requirement of decentralization, making LEO SCSs more robust. As a further advance, the progress of THz and laser-based communications is conducive to dealing with the CCI caused by the spectrum crunch. Finally, intelligent data-driven model-based AI-aided solutions are suitable for traffic prediction, telemetry-based data mining, and anomaly detection.

1) Quantum Key Distribution: The conceptually simplest encryption method relies on generating a pseudo-random secret key and then taking the modulo-two function of the key and the information to be encrypted, which is termed as plain text. Naturally, the key has to be as long as the data sequence is transmitted, which implies imposing an overhead of 100%.

Then the resultant so-called ciphertext may be transmitted from the source to the destination over a public channel. Given the knowledge of the secret key, the receiver can recover the original plaintext using the secret key. Since the key must

TABLE VII: Major achievements in the implementation of QKD

2017	1200 km satellite-to-ground QKD at 1.1 kbit/s [153]
2017	1000 km satellite-to-ground entanglement-based QKD at 3.5 bit/s [154]
2018	7600 km apart ground gateways with satellite relay QKD and encryption demonstration at key volume 100 kB [155]
2019	Continuous-variable QKD over 100 km fiber link at 0.14 kbit/s based on a photonic integrated quantum system [156]
2020	Point-to-point discrete-variable QKD over 509 km fiber link at 0.1 bit/s [157]
2020	First wavelength division multiplexing of 194 continuous-variable QKD at 172.6 Mbit/s over 25 km [158]
2020	Point-to-point continuous-variable QKD over 13 km fiber link at 0.88 Mbit/s [159]
2020	Point-to-point continuous-variable QKD over 202.81 km fiber link at 6.214 bit/s [160]
2020	Discrete-variable QKD over 1200 km free space optical link at 31 bit/s using Micius [153]
2020	Continuous-variable QKD over 180 km fiber link at 31 bit/s based on a photonic integrated quantum system [154]
2020	1120 km apart ground stations entanglement-based QKD at 0.12 kbit/s [161]
2021	4600 km apart ground stations entanglement-based QKD at 47.8 kbit/s [162]

remain confidential for the communications of the two parties, it must be shared between them over a secure channel.

The family of legacy cryptography schemes was conceived under the assumption that it would require an excessive amount of time, even upon using the most powerful computers by the eavesdropper to infer the key. However, given the threat of powerful quantum computers, it is no longer safe to rely on the above-mentioned antiquated assumption.

Similarly, simple principles may be used in QKD systems for the encryption/decryption process, but the negotiation of the secret key relies on a quantum channel as well as on an insecure public channel plus an authenticated public channel. The family of satellite-based QKD systems was richly characterized in [163], along with diverse satellite channels using detailed examples.

The transmission medium of QKD-based key negotiation typically relies on optical fibers and free space. Optical fiber has a low loss of about 0.3 dB/km and a high stability, hence it is more suitable for transmitting quantum signals. In recent years, numerous theoretical and experimental QKD designs have been proposed for improving the achievable secret-key rate vs distance trade-off [156]–[160].

There has also been substantial progress in QKD experiments relying on free-space optical links, culminating in the launch of the world's first quantum satellite-based QKD experiment in 2016, as reported in [153]–[155], [161], [162]. The significant milestones achieved in the implementation of QKD systems are chronologically arranged in Table VII.

Additionally, many other countries or organizations, such as the ESA and Canada, are also aiming for providing their satellite-based QKD services.

However, as the terminology suggests, QKD remains a key negotiation and distribution protocol, where the secret key is used by classical systems. By contrast, Quantum Secure Direct Communications (QSDC) [164] is a fully-fledged quantum communication protocol, in which confidential messages are transmitted directly over a quantum channel without requiring a secret key. It has hence enjoyed a rapid evolution, as documented in [165]–[172].

Lessons Learned: QKD has already found numerous commercial applications [173], such as finance and healthcare. But it still has numerous open challenges. Specifically, the operational QKD networks only tend to provide point-to-point key distribution or short-distance network services by relying on optical switches and routers. Explicitly, their distance is limited, since the quantum-domain signal must not be amplified. Otherwise, it collapses back into the classical domain. Continued focus in this area is required to facilitate large-scale deployments. Moreover, in the FSO-based QKD and QSDC scenarios [163], the clouds may affect QKD and QSDC transmission owing to dispersion imposed by atmospheric eddies. Specifically, the water molecules in the cloud layer cause scattering and absorption of optical signals, whereas the attenuation of optical signals by the cloud causes signal strength reduction. Furthermore, free-space QKD and QSDC usually require the precise alignment of telescopes. When there are clouds, the transmission of visible light and infrared light is limited, hence the telescope cannot be accurately aligned. This affects the stability of the QKD and QSDC systems. Even worse, the high mobility of LEO satellites exacerbates the above challenges.

2) Blockchain: Given the increasing number of LEO satellites and users supported by LEO SCSs, managing their security becomes a new challenge. As a remedy, the blockchain technique becomes a promising solution for the secure decentralized management of LEO SCSs. Briefly, the blockchain technique [174] is a structure that stores transactional records in several databases, known as the 'block', in a peer-to-peer network constituted by connected nodes, known as the 'chain'. Typically, this storage is referred to as a digital ledger.

The blockchain technique satisfies several of the above-mentioned security and reliability requirements, namely confidentiality, accountability, and decentralization. By relying on an encrypted database, users must have the correct key to read information from this database or write to it. Moreover, once the information is updated, all the related information is updated together as a block and appended to the previous version, thereby creating an immutable tamper-proof record. The premise is that the majority of participants check and verify this information. Otherwise, the information cannot be updated on the blockchain.

Additionally, decentralization is another compelling feature of the blockchain technique. If a failure occurs on one or several nodes of a blockchain network, the other nodes still

retain their data, and the network continues to function. Hence, a blockchain is often referred to as a distributed ledger because the information resides on multiple devices in a peer-to-peer network, where each device replicates and holds an identical copy of the ledger and updates it independently.

Given these benefits, many researchers have harnessed the blockchain technique for dealing with security attacks. Han *et al.* [175] exploited the blockchain technique to share and verify location information in a UAV network to detect spoofing jamming. By contrast, the blockchain technique is adopted in [176], [177] for protecting information from modification in resource-constrained IoT devices. Briefly, Chen *et al.* [176] conceived a stochastic blockchain scheme for protecting the integrity of IoT data. A fraction of the nodes were randomly selected for broadcasting their IoT data, which led to uncertainty for the attacker. As a further development, Yuan *et al.* [177] exploited the characteristics of the Physical Unclonable Functions (PUF) as part of the key agreement without storing sensitive keys in their lightweight broadcast authentication protocol in the blockchain.

As a benefit of its distributed ledgers and consensus operations, the blockchain technique is immune to both the DoS and the DDoS attacks [30]. For example, Georgios *et al.* [178] employed lightweight agents for exchanging outbound traffic information governed by blockchain to identify possible victims of DDoS attacks, which ensured the integrity of both the procedure and information exchanged.

For instance, to detect a compromised node in the DoS attack scenario, Kumar *et al.* [179] proposed a blockchain-based deterministic en-route report filtering scheme, which is capable of dropping false reports. As a further benefit, their scheme did not require any critical exchange between sensor nodes for data endorsement or authentication, thus reducing both the associated key storage overhead and communication overhead.

Lessons Learned: As evidenced by the literature, LEO SCSs empowered by the blockchain exhibit high robustness and fault tolerance even in the context of high-mobility LEO satellites. Since blockchain-based security services usually require substantial storage space and computing power, their employment in resource-constrained terminals and LEO satellites requires radical innovation.

Again, LEO SCSs have to share the user's sensitive information among multiple gateways or LEO satellites. In this case, the users' sensitive information may become exposed, hence potential security risks and data misuse issues may occur without user awareness. Therefore, during the blockchain implementation process, the protection of user privacy also has to be carefully considered.

3) THz and Space-based Laser Communication: The frequency allocations of several commercial LEO satellite constellations are shown in Fig. 13. Observe that many LEO satellites operate in the decimeter wave and centimeter wave bands such as Iridium and Globalstar. At the time of writing, the Millimeter Wave (MmWave) band is attracting research attention as a benefit of its rich spectral resources [180]. Many LEO satellite manufacturers such as Boeing, Starlink, and OneWeb sought permission to launch satellites operating in the 50.2-52.4 Gigahertz (GHz) bands [181]–[183]. However, these frequency resources are becoming congested. A potential solution is to increase the operating frequency to the THz or even optical bands. Thanks to the development of device and communication technology, these emerging bands are gradually entering commercialization [184], [185].

The THz band has a vast amount of available bandwidth, which has to be further explored. Radio frequencies above 100 GHz are largely untapped for specific applications by the ITU. Hence they might become available for SCSs. In the presence of water vapor molecules and other propagation effects, the THz band suffers a limitation in transmission distance, which is not suitable for the satellite-Earth link [186]. Hence, the employment of THz communications for ISLs [187], [188], which operates above the Earth's atmosphere, could be an attractive alternative. According to [189], THz transmitters and receivers could be designed to circumvent the disadvantages of microwave bands. Although the attenuation of the THz band is high, this may potentially be compensated by large-scale antennas used for Beamforming (BF) on a space-borne payload. The beam width of the large-scale antennas in the THz band is narrower than that of common microwave ISLs, which enhances their ability to resist eavesdropping.

However, observe that the longest communication distance was 21 km at 140 GHz [190], which is insufficient for ISLs. Therefore, a large antenna array and high-power devices operating in the THz band should be developed to overcome the extremely high propagation loss and power limitations of the space-borne transceivers in harsh operating environments.

The laser band is far above the electromagnetic spectrum. Thus it has a strong anti-interference capability. Laser communications cannot be detected by spectrum analyzers or RF meters since the laser beam is highly directional, which makes it a strong candidate for ISLs and cross-layer links [191]. Additionally, laser offers several advantages over microwave communications in terms of size, weight, and power dissipation compared to the MmWave band under the same data rate conditions [192], [193].

Many research institutions across the world have conducted numerous experiments, which are summarized in Table VIII at a glance. Additionally, Starlink tested 'space lasers' between two satellites, relaying hundreds of Gbytes of data in Sep. 2020. At the time of writing, Starlink is engaged in rolling out further laser cross-links amongst their satellites to minimize the number of ground facilities and to extend the coverage to remote areas [194], [195].

Lessons Learned: Since the THz and laser beam are highly directional, they have a limited coverage area. This imposes serious challenges for signal alignment (acquisition and tracking) in the context of high-mobility LEO satellites. In the existing satellite-Earth communication experiments, the experiments in Table VIII were conducted between satellites and an Optical Ground Station (OGS). The OGS exploits its own position and the position of the satellites to assist with signal alignment. However, the Doppler shift still has to be mitigated with the aid of sophisticated processing algorithms to eliminate their adverse effects.

Furthermore, signal alignment is more challenging for ISLs

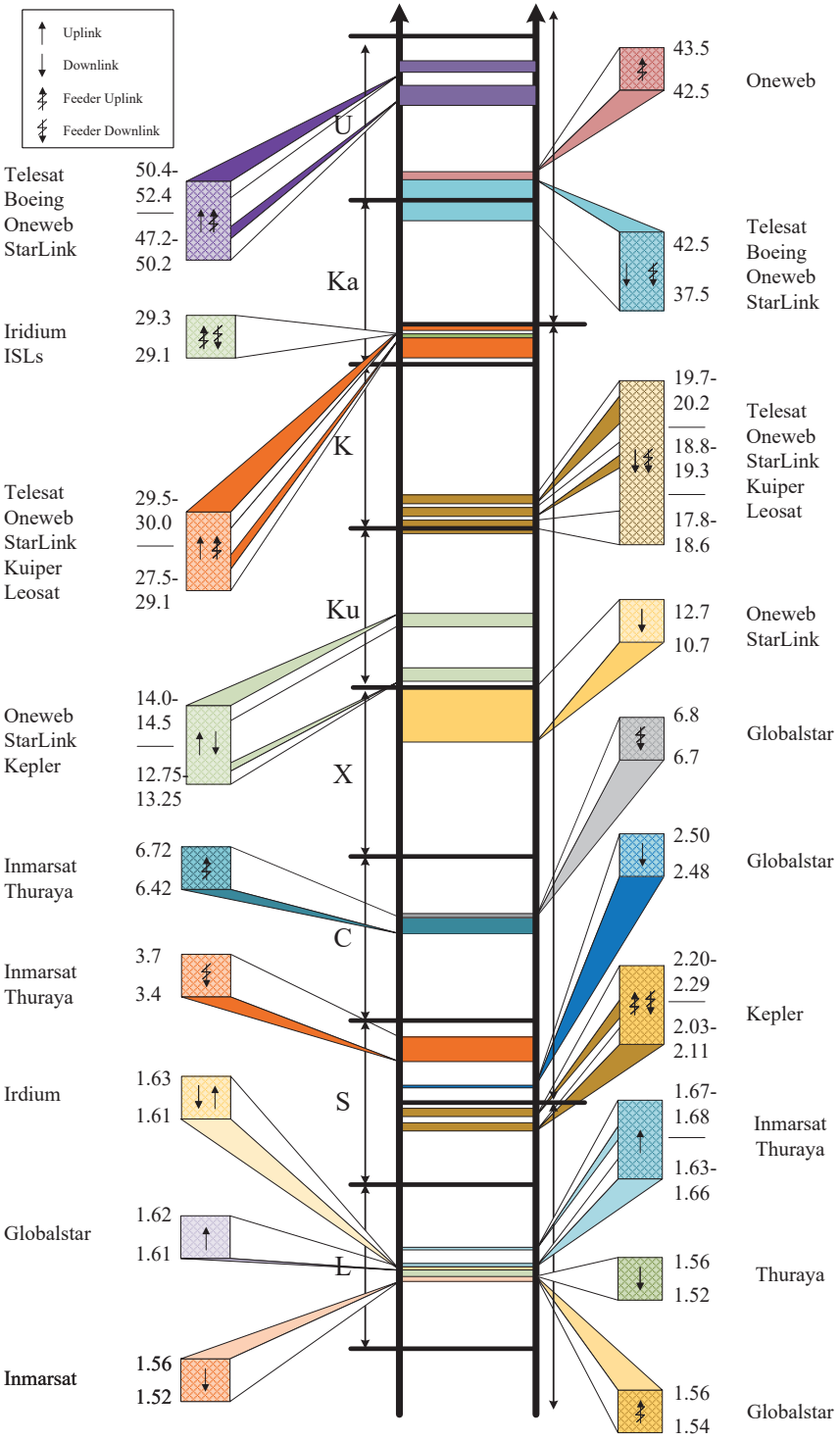


Fig. 13: Frequency allocations of several commercial constellations between 1 and 60 GHz.

TABLE VIII: The evolution of space-based laser communications

Year	Project	Type	Country/Region	Data rate (Mbps)	Modulation	Distance (km)	Ref.
2001	SILEX	GEO-LEO	Europe	50	IMDD	45000	[196]
2006	OICETS	LEO-OGS	Japan	50	IMDD	610	[197]
2010	TerraSAR	LEO-OGS LEO-LEO	Europe	5625	BPSK	500-1000 1000-5000	[198]
2011	BTLS	LEO-OGS	Russia	125	IMDD	400	[199]
2013	LLCD	Lunar-OGS	US	622	PPM	400000	[200]
2013	Alphasat	GEO-LEO	Europe	1800	BPSK	45000	[201]
2014	OPALS	LEO-OGS	US	50	IMDD	400	[202]
2014	SOTA	LEO-OGS	Japan	10	OOK/IMDD	642	[203]
2016	MICIUS	LEO-OGS	China	5120	DPSK	1500	[204]
2016	OCSD	LEO-OGS	US	200	IMDD	450	[205]
2017	VSOTA	LEO-OGS	Japan	10	——	1000	[206]
2017	SJ-13	GEO-OGS	China	4800	IMDD	36000	[207]
2020	EDRS-C	GEO-LEO	Europe	1800	BPSK	45000	[208]
2020	SJ-20	GEO-OGS	China	10000	OOK/BPSK/QPSK	36000	[209]
2023	CubeSOTA	GEO-LEO LEO-OGS	Japan	10000	DPSK	39693 1103	[210]
2025	EDRS-D	GEO-GEO	Europe	3600-10000	BPSK	80000	[207], [211]
2025	ScyLight	GEO-LEO LEO-OGS	Europe	100000	——	—— 80000	[212]

in LEO SCSs. The high velocity and the jitter of the space-borne payload [213] make the accurate alignment of the beam a challenge. Furthermore, even higher Doppler frequency shifts may be observed for the space-borne laser terminals in the 'reverse seam' [59], where the adjacent satellites move in opposite directions. The authors of [214] analyzed the Doppler frequency shift of LEO SCSs relying on laser links. Inadequate Doppler frequency shift compensation results in a loss of frequency synchronization at the receiver, ultimately resulting in data loss.

4) Aritificial Intelligence: In recent years, the success achieved by AI in terrestrial wireless communication systems has also pervaded the family of LEO SCSs. Among the AI techniques, Machine Learning (ML) has matured and emerged as a valuable tool capable of learning empirical models and tracking changes in data patterns during space missions [215]. This aspect of ML proves particularly advantageous in the context of security solutions since it enables the analysis of various types of data from different perspectives.

Tele-traffic Data: Accurate processing of tele-traffic in LEO SCSs holds paramount significance. Predicted traffic patterns play a critical role in optimizing routing paths and pre-scheduling networking resources, hence mitigating the CCI and minimizing both transmission outages and the probability of congestion. Moreover, early detection of abnormal traffic generated by malicious attackers can proactively prevent congestion from occurring. The authors of [216], [217] adopted the extreme learning machine (ELM), a neural network having a simple structure and high computation speed in accurately characterizing the traffic load of LEO satellites. As a further development, an accurate long-short-term memory (LSTM) prediction model based on a deep recurrent neural network was proposed in [218], [219]. LSTM constitutes an ideal ML method for handling multi-variate time-series data since it is capable of modeling the complex interactions of a system. However, the LSTM prediction model imposes a high computational burden. To circumvent this, Li *et al.* developed a Gated Recurrent Unit (GRU) based neural traffic prediction algorithm having a reduced gate structure [220], whose training efficiency and accuracy can be substantially improved by cooperating with the powerful techniques of transfer learning and online training.

Housekeeping Data: The housekeeping data collected from satellites consists of numerous measurements and readings that reflect the status of the satellite and its surrounding environment. By analyzing the abnormalties within the housekeeping data, potential failures and imminent alerts can be inferred, allowing the satellite to intelligently make proactive decisions for mitigating the risk of failure. In this context, Fuertes *et al.* developed a Support Vector Machine (SVM)-based anomaly detection algorithm [221], which is capable of recognizing anomalies with high detection sensitivity, but comes at the price of a high false alarm rate. The properties of housekeeping data are summarized in [222], including their high dimensionality, multi-modality, and heterogeneity, which lays the foundations for ML-based detection relying on probabilistic clustering. LSTM still represents a significant leap forward in efficiently processing historical data for future prediction and anomaly detection [223]–[226]. In [223], the LSTM method is combined with the Gaussian model of the training errors for the sake of detecting anomalies. Notably, this solution mitigates the probability of false alarms resulting from misconstrued anomalies, unknown incidents, and sparse samples using the Deviation Divide Mean over Neighbors method. Additionally, the authors of [226] propose exploiting the causality of time series to construct a causal network, which exhibits plausible interpretability, robustness, and adaptability. Comprehensive comparisons among different ML techniques, including the Recurrent Neural Network (RNN), LSTM, and GRU, used for the prediction of the LEO satellite

data are conducted in [227]. The evaluation of prediction accuracy using battery temperature, power bus voltage, and load current data shows that LSTM achieves the highest accuracy, while GRU exhibits the shortest running time. More recently, the temporal convolution network also raised much attention for time series prediction with favorable parallel processing ability and temporal characterization [228], which shows superior operational efficiency compared to LSTM. The predicted telemetry data based on the aforementioned prediction techniques can then be further analyzed to detect any potential future failure. A common approach is to compare the prediction error to a predefined or automatically adjusted threshold to detect which data is anomalous [224], [225], [228].

Attack Data: Furthermore, the interconnected nature of LEO satellite networks results in vulnerabilities to cyber threats and malicious satellites because of the poor network security of inter-satellite networks. It was thus important to detect cyber-attacks from satellite networks while preserving data privacy. More recently, the distributed LSTM technique was utilized in [229] for identifying cyber-attacks in each smart satellite network, such as reconnaissance, fuzzes, and denial of service attacks. The results were then further processed by a federated learning architecture to form a more private and secure intrusion detection system.

Power System Data: Power system data plays a critical role in maintaining the safe and stable operation of a specific mission. However, the structure of the power system is complex, where faults may occur in cables, solar arrays, batteries, power distribution switches, power controllers, and so on. Quantifying the correlation between different fault types and the causality between faults and the corresponding fault predictions is challenging. Fortunately, a large amount of power system data can be gathered, which allows ML methods to build an accurate fault classification model for characterizing the relationship between abnormal data and fault association [230]. In particular, the LSTM method discussed above can also be utilized for predicting the parameters and for performing anomaly detection in the satellite's power system [231], [232]. In [233], the authors specifically focus on detecting faults in solar arrays, which have the highest failure rate among all components in orbit. Similar to [221], an SVM-based regression is utilized in [234] for detecting potential threats in a generic spacecraft power system. This system exhibits excellent learning and prediction capabilities.

Spectrum Data: ML tools are crucial for processing spectrum data in satellite communication systems to detect anomalies and interference. Similarly to other time-dependent telemetry data, the spectrum data can be utilized in an LSTM-based prediction model for intelligently managing future signal spectrum as well as for detecting anomalies and interference [235]–[237]. Furthermore, the features of interference can be leveraged for interference classification to identify and avoid interfering sources. For example, in [236], the authors utilize an intelligent LSTM interference classifier that harnesses four features, including the magnitude and phase of the temporal and frequency domain signals. The ML classifier model developed in [238] consists of a backbone network, neck network, and head network, which characterize interference based on its type, bandwidth, intensity, and frequency. These features are classified into six interference patterns: single-frequency interference, frequency-hopping interference, single-frequency sweeping interference, round-trip frequency sweeping interference, low interference, and other interference. The experiments conducted demonstrated nearly 100% accuracy in spectrum detection, enabling accurate satellite interference management.

In summary, the most popular ML techniques for conducting prediction, anomaly detection, and classification on satellite data are neural networks. Again, a representative technique is LSTM, which is a kind of neural network associated with recurrent connections. These connections allow the network to retain valuable information in internal memory. GRU is similar to LSTM in terms of having recurrent connections and memory, but with a simpler structure and less information-flows within the network compared to LSTM. Both LSTM and GRU constitute specialized variants of the traditional RNN, where each neuron receives its input from the previous time step and passes the output to the next time step. On the other hand, ELM, as adopted in [216], [217], is a feed-forward neural network without any recurrent connections. In other words, ELM does not have explicit memory to store past information, but it is known for its fast training. Fig. 14 illustrates the entire process of the ML-based security solutions conceived for satellite data reviewed in this paper.

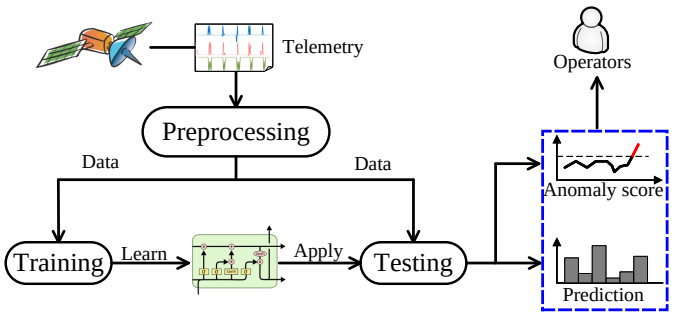


Fig. 14: The entire process of the ML-based security solutions for satellite data.

When it comes to ML techniques, one of the key bottlenecks in implementation is the availability of datasets. However, most of the existing literature does not make the associated datasets gleaned from real satellites publicly available [220], [222]–[225], [227], [230], [237]. Hence some authors resorted to simulated artificial data generated from software [217], [218], [231], [238]. Since accessing real satellite data is challenging, some of the literature utilizes data generated on the ground as a substitute. For example, traffic [239], [240], housekeeping [241], [242], and attack [243], [244] data on the ground were used for representing satellite data in the above papers. Additionally, the authors of [216] mentoioned an avaliable internet network traffic dataset :http://ita.ee.lbl.gov/index.html, which provides a collection of data related to network traffic, including packet-level information, network flow statistics, and other measurements. Although the data traces available on the website were last

updated in April 2018, they still serve as valuable resources for studying network dynamics, usage characteristics, and growth patterns.

B. Passive Security Enhancement Solutions

Passive security enhancement solutions tend to rely on advanced security-oriented antennas, interference coordination, SS techniques, Non-SS jamming suppression techniques, reconfigurable intelligent surfaces, satellite cooperation, and AI tools, which are adopted for mitigating eavesdropping, CCI between systems, and malicious power-based jamming. These solutions are discussed in the following.

1) Advanced Security-oriented Antennas: Advanced security-oriented antennas combining PLS and multiple-antenna-aided techniques can effectively mitigate eavesdropping and power-based jamming, which are detailed below.

Eavesdropping Mitigation: There are recent studies on advanced security-oriented antennas for secure transmissions since they are capable of reinforcing the radiation pattern in the direction of the desired receiver while suppressing the pattern in most of the other directions. However, an eavesdropper equipped with a sensitive receiver may still be capable of intercepting the communication link via a side lobe. To tackle this problem, side-lobe randomization [245] may be used for alleviating side-lobe information leakage. The advanced security-oriented antennas employ BF, and Artificial Noise (AN) [246] in the downlink to transmit AN in the direction of eavesdroppers for actively suppressing eavesdropping [246]–[248].

However, eavesdroppers may be able to penetrate the main-lobe direction anywhere between the LEO satellite and the Earth. It may frequently occur in LEO SCSs, because LEO satellites are always orbiting overhead, inevitably making eavesdroppers fall within the main-lobe direction. In this scenario, the Phased Array (PA) no longer works, as its beams are only angle-dependent. The Frequency Diverse Array (FDA) [249] can be employed to address this problem.

The authors of [250] introduced a Linear Frequency Diverse Array (LFDA) that can generate a beam pattern depending on both the angle and the distance by linearly shifting the carrier frequencies across different antennas. However, the length and direction of the beam pattern generated are coupled. Hence it may still be possible for the eavesdropper to intercept the message of the legitimate user at certain positions. To tackle this problem, several kinds of non-Linear frequency offset schemes, including logarithmic offset, exponential offset, and random offset, are proposed for decoupling distance and direction of the beam pattern [251]–[253]. Fig. 15 shows the beam pattern of PA, LFDA, and logarithmic FDA. Explicitly, recall from Fig. 15 that the peak position of the PA is independent of distance. While the peak position of the LFDA and the logarithmic FDA is related to both the direction and the distance. Between them, the peak positions of LFDA are distributed as an 'S' shape due to the coupling of distance and direction. Its beam is periodic, and the period is determined by the frequency offset Δf. But the logarithmic FDA can form a spot beam owing to its enabling distance and angle decoupling. Both of their detailed derivations are contained in [250], [251]. Although the FDA is capable of providing additional security in the distance dimension, its beam pattern is time-variant, which limits its field of application [254].

Jamming Mitigation: The advanced security-oriented antennas also allow the beam pattern to be adjusted in response to power-based jamming conditions. Explicitly, the beam pattern can be adjusted in azimuth to minimize the jamming impinging from the left or right of an antenna or in elevation [255]–[257].

2) Reconfigurable Intelligent Surfaces: The above techniques mainly rely on specifically designing the signals to prevent eavesdropping and mitigate interference. At the time of writing, the innovative technology of RISs has generated excitement in the wireless community, which is capable of beneficially ameliorating the wireless communication environment. Specifically, a RIS is capable of manipulating the phase and even the amplitude of advanced reflecting elements. This property allows the system to mitigate the blockage of the LoS component in satellite communication systems. Additionally, RISs can also mitigate security and interference problems.

Security Safeguards: The preliminary contributions in the field of RIS-assisted secure satellite communications appeared in [258], where the authors used a RIS to reflect the terrestrial interference signals to the eavesdroppers on the ground, who aimed for overhearing the satellite downlink transmission. The transmit beamformer weights of the terrestrial BS and the reflection coefficients of RIS are thus jointly designed to ensure that the interference generated can be tolerated by the satellite user while guaranteeing reliable satellite communication. As a benefit, the proposed RIS-assisted cooperative jamming strategy achieves lower SINR at the eavesdroppers than the conventional one operating without a RIS. This allows the RIS to enhance security. The authors also showed that the RIS having reflecting elements imposes increased jamming power on the eavesdroppers, thereby improving security. In addition to safeguarding the conventional satellite downlink, the authors of [259] proposed deploying a RIS in a full-duplex relaying aided satellite communication system.

However, a terrestrial RIS cannot get close to the eavesdroppers and to objects flying in the air, thus it has eroded gains. Owing to the lightweight and conformal geometry of the RIS, a HAP carrying a RIS is proposed in [260] for securing the communication link between an LEO satellite and a UAV receiver in the presence of a UAV eavesdropper. Even without the CSI knowledge of the eavesdropper, the legitimate user can still have a secure system by increasing the number of reflecting elements of the RIS in a hostile environment by simply maximizing the received signal power.

Additionally, the authors conceived a RIS optimization strategy to maintain a higher level of security, when either the statistical or the perfect CSI is known. The importance of a suitable RIS design is highlighted by characterizing a system at serious risk, namely when the RIS coefficients are random. The authors of [260] also reveal the impact of the phase quantization at the RIS on the secrecy performance. Explicitly, they demonstrated that 3 bits are sufficient to avoid substantial secrecy degradation.

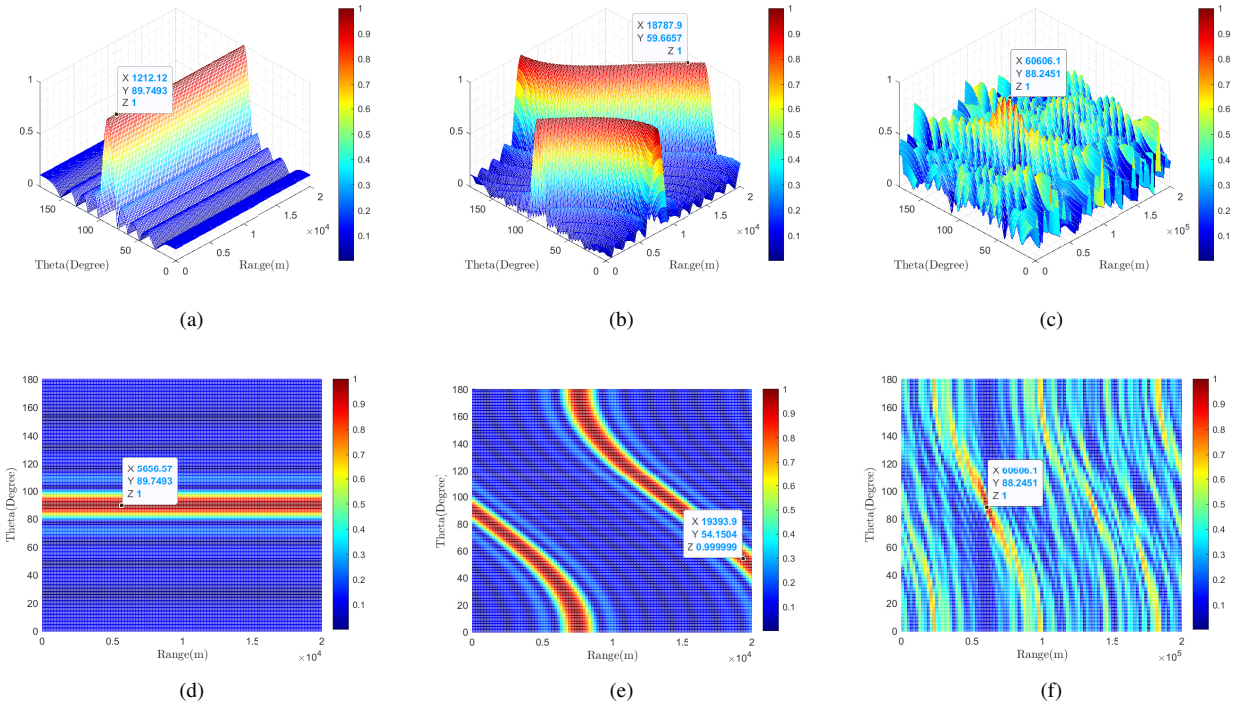


Fig. 15: The beam patterns of PA, LFDA, and logarithmic FDA. (a), (b), and (c) separately present the 3D beam pattern when $t = 0$. While (d), (e), and (f) show the projection of their beam pattern on the distance-direction plane when $t = 0$. The simulation parameters are as follows. The operating frequency f_c and the antenna interval d are given by 10 GHz and 0.15 m, respectively. The number of the array is 9. The Δf of LFDA and logarithmic FDA is 20 kHz.

As we mentioned before, the amplitude of reflected elements can be adjusted. However, this kind of RIS does not work in a passive manner, since it consumes additional power to bring about additional amplitude gain. It is therefore termed as an active RIS. Another difference with respect to the passive RIS is that the active one inevitably introduces thermal noise, which is also amplified along with the incident signal. The investigation of an active RIS in terms of securing satellite communication was conducted in [261], where a cooperative jamming strategy similar to that in [258] is adopted to allow the terrestrial network to secure the legitimate satellite downlink transmission under the assistance of an active RIS. However, the impact of an active RIS on the secrecy performance is not fully revealed in [261]. The authors of [262] showed that a well-designed active RIS outperforms its passive counterpart when it comes to the secrecy energy efficiency of the conventional satellite downlink overheard by terrestrial eavesdroppers. However, it is still an open question, whether the security is enhanced by an active RIS. Moreover, the authors of [262] considered a GEO satellite without considering the unique mobility-induced propagation properties of LEO satellites. But again, the benefits of the active RIS over the passive one in securing LEO satellite systems, as well as the impact of the amplification power budget, are still awaiting further investigation.

Interference Mitigation: Similar to protecting legitimate signals from eavesdroppers, RISs can also be utilized for mitigating both intra-system interference and CCI. The authors of [263] reveal the benefit of RIS in terms of improving the sum rate of LEO satellite systems, which is directly related to the SINR at the receivers. The superiority of the RIS in spectrum-sharing-based integrated terrestrial-LEO satellite networks was investigated by Dong *et al.* in [264]–[266]. The improvement of the received SINR becomes more pronounced upon increasing the number of RISs, the number of reflecting elements, and the phase shift resolution. The benefits of RIS were also observed in [267] where instead of a terrestrial network, a HAP-aided scenario was considered, where the SINR was the constraint rather than the optimization objective in the design of the RIS. This paper emphasized that both the channel estimation error and the multipath effect should be carefully addressed when designing the reflecting elements. The interference reduction capability of RIS was investigated in [268] for a UAV-mounted RIS (U-RIS). The U-RIS is shown to have the ability to enhance signal transmission within the terrestrial network, while mitigating the interference generated by the uplink signals transmitted from the ground stations to the satellite, thereby improving the SINR at the intended terrestrial users.

Lessons Learned: The literature reviewed above has been summarized in Fig. 16. Observe that there is a paucity of literature on the security of LEO SCSs relying on RISs. Moreover, most of the existing literature where the RIS acts as the security safeguard or operates as the interference canceller either does not specify the type of the satellite at all or only targets GEO satellites. Hence, they ignore the effect

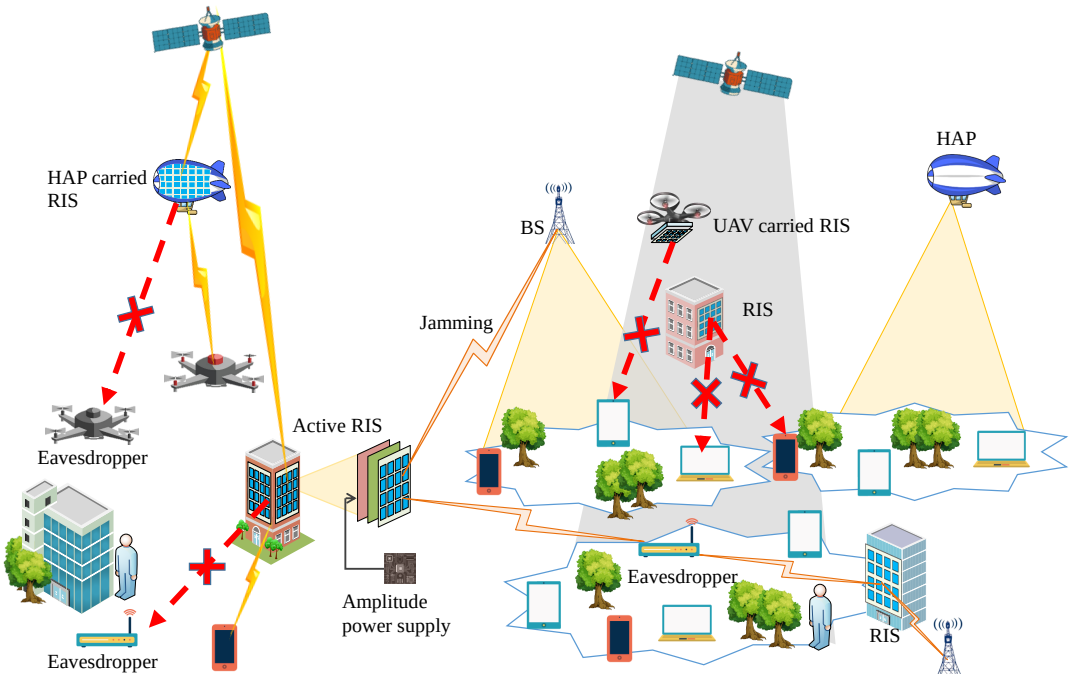


Fig. 16: Application scenarios for RIS-enabled passive security enhancement solutions.

of the limited above-the-horizon communication period, the frequent handovers, and the high Doppler shifts. Nonetheless, some of the above-mentioned contributions do allude to LEO satellites but do not accurately reflect their unique propagation properties, such as the time-variant received SNR, Doppler frequency shifts, and delay. The corresponding influence of these phenomena on the RIS design and on the performance achieved has not been investigated. Hence the employment of RIS-aided solutions in practical LEO systems requires substantial further research. Furthermore, security threats exist not only in satellite-terrestrial systems but also in satellite-satellite networks.

Considering the high mobility and limited access time of LEO satellites, the working time of RISs deployed on the Earth or UAVs is also limited. Similar to RISs deployed on UAVs, it can also be considered to install RISs on LEO satellites, which undoubtedly increases the weight of the satellite and launch costs. Additionally, the hash space environment, such as intense temperature changes and cosmic rays, has to be considered. In a nutshell, the security of RIS-aided LEO satellites requires further exploration.

3) Interference Coordination: Interference coordination is a promising technique for mitigating the CCI between systems caused by the spectrum crunch. It typically mitigates interference by power control, beam drifting, cognitive radio techniques, etc., while improving spectral efficiency and meeting the ever-increasing capacity demands. Its evolution is chronologically arranged in Table IX.

The ITU specifies that GEO SCSs have priority over LEO SCSs with regard to frequency usage. Consequently, accurate power control is required in LEO SCSs to satisfy the interference constraints imposed by GEO SCSs. However, the power control also directly affects the throughput of LEO SCSs [117], [269]. As a remedy, the authors of [273] modeled this power control problem as an optimization problem aiming to maximize the sum rate of the LEO SCSs. Then, the popular fractional programming technique was employed to transform this nonconvex problem into a tractable form. By contrast, the authors of [116] conceived a joint multi-beam power control algorithm for optimizing the transmit power of LEO and GEO satellite beams. On the premise of ensuring the signal quality of GEO SCSs. This algorithm judiciously reduced the transmission power of GEO beams, thereby maximizing the throughput of LEO SCSs.

Some schemes rely on so-called beam drifting in LEO SCSs, which force the LEO satellite users into the adjacent beam even before interference actually occurs [79], [271], [272], [274]. The authors of [272] conceived a sophisticated strategy for reducing the downlink interference inflicted by LEO satellites on GEO satellite users. The authors of [271] mitigated the interference between LEO and GEO satellites by appropriately tilting the transmission direction of the PA-based antennas of LEO satellites by solving a nonlinear programming problem used for finding the optimal direction. OneWeb adopted the method of [274] for LEO SCSs to avoid the risk of interference with GEO SCSs operating at the same frequency. Specifically, when an interference event occurs, some beams are briefly turned off as they cross the equator. Subsequently, when the LEO SCSs exit the GEO SCSs exclusion zone, the specific beams which were turned off are turned back on again. In the context of a hybrid-beam coverage scheme[4], the authors of [79] also proposed a so-called coverage-extension method

[4]There is a wide beam providing coverage for the whole service area and several spot beams for tracking users in each LEO satellite. The gain of a spot beam is designed to be much higher than that of a wide beam. Hence the spot beam is provided for supporting data transmission, while the wide beam is fixed and is suitable for control signals.

TABLE IX: The evolution of interference coordination

Year	Ref.	Target Problem	Ways	Proposed algorithm/scheme	Results
2015	[269]	CCI between LEO SCSs and terrestrial systems	Power control	Presents three different efficient power control methods	Strikes a clear trade-off between channel state information and rates.
2016	[117]	CCI between LEO SCSs and terrestrial systems	Power control	Investigates optimization approaches to solve the power and rate allocation problems	Formulates a multi-objective optimization problem and provides a Pareto-optimal solution
2017	[270]	CCI between LEO SCSs and GEO SCSs	Modulation coding	Presents a method combining modulation and coding based on power control	Improves the throughput of LEO SCSs compared with traditional power control method
2018	[271]	CCI between LEO SCSs and GEO SCSs	Beam drifting	Presents an optimal method by tilting the direction of PA of LEO satellite	Guarantees the signal level of LEO satellite with a simple method
2018	[272]	CCI between LEO SCSs and GEO SCSs	Beam drifting	Proposes an exclusive angle strategy for CCI mitigation	Reduces the CCI level sacrificing the coverage of LEO satellites
2019	[79]	CCI between LEO SCSs and GEO SCSs	Beam drifting	Turns off the current beam and expands its adjacent beam to take place	Ensures the throughput of LEO SCSs as well as CCI mitigation
2019	[273]	CCI between LEO SCSs and GEO SCSs	Power control	Proposes an adaptive beam power control method based on optimization	Maximizes the throughput of LEO SCSs under the premise of that the signal quality of GEO SCSs.
2019	[274]	CCI between LEO SCSs and GEO SCSs	Beam drifting	Adjusts the angle of the spot beams or even turns off some spot beams of LEO satellites	Reduces the CCI level with the limited throughput of LEO SCSs
2019	[275]	CCI between LEO SCSs and GEO SCSs	Cognitive radio	proposes detailed spectrum strategies to detect the presence of the GEO SCSs	Adjusts the transmit power of LEO SCSs according to the signal power level of GEO SCSs
2020	[276]	CCI between LEO SCSs and terrestrial systems	Cognitive radio	Integrates a distributed cooperative sensing network with satellite terrestrial network	Strikes a trade-off between the average throughput and the average energy consumption
2020	[277]	CCI between LEO SCSs and GEO SCSs	Cognitive radio power control	Proposes an optimal method by combining spectrum sensing and power allocation	Maximizes the throughput of LEO SCSs with power allocation after optimizing the sensing time and the sensing interval
2020	[278]	CCI between LEO SCSs and GEO SCSs	Deep learning	Proposes a DL aided spectrum prediction method	Adjusts the operating frequency of LEO SCSs to avoid the CCI by diging the historical spectrum data of the GEO SCSs
2021	[279]	CCI between LEO SCSs and GEO SCSs	Beam hopping power control	Proposes a joint beam hopping and power control scheme	Maximizes the throughput of LEO SCSs under the premise of ensuring the signal quality of GEO SCSs
2021	[116]	CCI between LEO SCSs and GEO SCSs	Power control	Jointly optimizes the transmit power of LEO and GEO satellite beams	Maximizes the throughput of LEO SCSs under the premise of ensuring the signal quality of GEO SCSs
2021	[280]	CCI between LEO SCSs and GEO SCSs	Cognitive radio	Proposes a low-complexity cognitive radio technique for CCI mitigation	Enhances the throughput of LEO SCSs under the premise of ensuring the signal quality of GEO SCSs

for beam drifting, which relies on expanding the wide beam to cover the serving areas of adjacent satellites. When the coverage area of an LEO satellite is overlapped with that of the adjacent satellites, one of them can be turned off to avoid potential interference.

Given the ever-increasing deployment density of LEO mega-constellations, a spectrum crunch is imminent. Cognitive radio [281]–[283] techniques are capable of mitigating this problem. In cognitive radio networks, PUs have a higher priority or legacy rights on the usage of a specific spectrum. SUs, which have a lower priority, should not cause interference with PUs. Hence SUs must have cognitive radio capabilities for adapting their communications channel access to the dynamic environments in which they operate. Explicitly, cognitive radio devices can sense, detect, and monitor the surrounding opportunities, including spectrum, time, geographical space, code, as well as angle [284] and reconfigure the operating characteristics to best match those opportunities.

Cognitive radios are capable of making autonomous real-time decisions for mitigating the spectrum scarcity problem in SAGINs. The authors of [275] proposed a spectrum sensing scheme for LEO SCSs capable of mitigating the inter-system interference between GEO and LEO SCSs. Upon identifying the specific power level utilized by the GEO SCSs after differentiating the GEO signal from the interfering LEO signal and noise, the authors of [280] conceived a cognitive radio technique for improving the throughput of LEO SCSs, while guaranteeing that the signal quality of GEO SCSs can be satisfied. By applying sophisticated relaxation and approximation schemes, they significantly reduced the complexity of the related optimization problem. The authors of [276] proposed a cognitive satellite-terrestrial network relying on a distributed cooperative spectrum sensing technique by striking a trade-off between the average throughput and the average energy consumption under specific interference constraints.

Additionally, the authors of [277] conceived a two-stage spectrum-sharing framework by combining the advantages of cognitive radio and power control techniques. This framework jointly optimizes the spectrum sensing time and the LEO SCSs transmit power with the objective of enhancing spectral efficiency and seamless coexistence. The authors of [279] proposed a joint beam hopping and power control scheme for maximizing the throughput of LEO SCSs, while preserving the signal quality of GEO SCSs. A DL-aided spectrum prediction method was proposed in [278] for mitigating the inter-system interference. A sophisticated combination of a convolutional neural network and a carefully dimensioned bespoke memory was harnessed for data mining from the historical spectrum usage of the GEO SCSs. This technique was used for predicting future spectral occupancy. Furthermore, an adaptive modulation and coding method was adopted in [270] for interference mitigation. Specifically, this method adopted the angle between LEO and GEO satellites for controlling the specific choice of modulation and coding scheme, with the objective of improving the spectral efficiency of LEO SCS, while limiting the interference inflicted upon the GEO SCSs to the maximum tolerable limit.

Lessons Learned: Considering the high mobility and limited over-the-horizon time of LEO satellites, the active operating duration of RISs deployed on the Earth or UAVs is also limited. Similar to RISs deployed on UAVs, it may also be feasible to install RISs on LEO satellites, which undoubtedly increases the weight of the satellite and launch costs. Additionally, the hash space environment exhibiting intense temperature changes and cosmic rays has to be considered. In a nutshell, the security of RIS-aided LEO satellites requires

further exploration.

In fact, the establishment of standards at regional and global levels facilitates the efficient and economical use of the spectrum and the development of radio services. Hence the ITU provides a regional framework that allows sovereign nations to submit and discuss their spectrum requirements in different regions (Regions 1, 2, and 3). There are regional and sometimes country-specific differences in the way that spectrum band plans and radio system techniques are deployed. Because of the fixed orbital position of GEO satellites, GEO satellites can clearly be dealt with on a regional or country-by-country basis. Additionally, interference issues are generally related to fixed entities and are reasonably easy to manage.

By contrast, LEO satellites fly over many regions and countries, requiring them to comply with many different regulatory regimes to allow them to provide services to users. Furthermore, they have to implement sophisticated interference coordination solutions relying on power control, CR, and beam drifting for mitigating CCI imposed on terrestrial communication systems and GEO SCSs, as required by ITU regulations.

However, with the continued proliferation of LEO mega-constellations, such as SpaceX, OneWeb, and Lightspeed, the CCI between these different constellations jostling for room in LEOs also has to be addressed, and even the interference between different orbital layers within the same constellation has to be given cognizance.

AI is eminently suitable for analyzing the frequency usage in various regions by relying on spectrum sensing and combining the results of satellite flight trajectory prediction to assist interference coordination, making it a topic worth investigating.

4) SS Techniques: SS techniques have been routinely adopted as one of the secure techniques in military communications for more than 70 years [285], where the transmitted signal is spread to a much wide bandwidth than the information bandwidth. The common SS techniques include DSSS, Frequency Hopping Spread Spectrum (FHSS), and Multi-Carrier Direct Sequence Spread Spectrum (MC-DSSS). Unless the eavesdropper steals the random Frequency Hopping (FH) pattern or spreading code, it fails to detect the confidential information [286].

Again, DSSS has been widely used in satellite communications [287]. DSSS technique can prevent eavesdropping, thus guaranteeing confidentiality. Typically, the PSD of DSSS signal is low, and the received signal may be submerged in noise when arriving at the receiver, making it difficult for adversaries to eavesdrop. On the other hand, the DSSS technique is also immune to jamming to a certain extent. Whenever jamming contaminates the legitimate signal, the receiver correlator spreads the jamming to the entire bandwidth after despreading because the jamming and the local pseudo-noise code are uncorrelated. By contrast, the legitimate signal is despread back to its original narrower bandwidth. The Signal to Noise Ratio (SNR) of the baseband data increases after despreading by a factor of the Processing Gain (PG). By contrast, the PSD of jamming remains low in the baseband. Hence, the anti-jamming ability also depends on the PG. However, the payload rate is given by the ratio of the bandwidth and the spreading factor, which explicitly indicates the traffic rate versus anti-jamming capabilities trade-off in LEO SCSs. More specifically, when the jamming is strong, the DSSS sequence length should be increased to improve the anti-jamming capability controlled by its PG, hence leading to throughput reduction and $vice\ versa$.

Furthermore, FHSS constitutes another popular anti-jamming technique. In contrast to DSSS, the FHSS transceiver continuously jumps from one sub-carrier frequency to another during transmission according to the SS code. Hence, the FHSS signal bandwidth may be composed of discontinuous frequency bands, and it is often combined with cognitive radio techniques to avoid jamming at locations subject to severe jamming whilst relying on adaptive frequency hopping.

Hopping across multiple frequencies within a single symbol leads to the concept of Fast Frequency Hopping Spread Spectrum (FFHSS). More explicitly, the dwell time of each hop is shorter than the symbol duration, and multiple frequency hops are completed within a single symbol duration, leading to strong anti-jamming capability. FFHSS may rely on low-complexity non-coherent dehopping and demodulation methods, but this results in a substantial loss of SNR [288], [289]. By contrast, the coherent reception of FFHSS exhibits better performance [290], at a substantially increased complexity.

Compared to DSSS, the MC-DSSS receiver employs spectrum sensing to monitor and analyze the current operating frequency in real-time, identifying the available frequency bands (left side of Fig. 17) as well as occupied frequency bands (right side of Fig. 17), and flexibly devising sub-carrier allocation schemes. The MC-DSSS receiver can choose to avoid the existing signals to improve integrity by allocating each sub-carrier to available frequency bands. However, these signals are also easily eavesdropped by attackers, resulting in decreased confidentiality. By contrast, these sub-carriers could also be actively hidden in some of the existing signals to improve confidentiality. Specifically, the operating frequency of each sub-carrier can be set to the same as the existing signal. However, legitimate signals are also contaminated by existing signals, which undoubtedly degrades integrity. Fig. 17 shows the MC-DSSS waveform with 8 sub-carriers, where four sub-carriers are allocated to the available frequency band and the other four sub-carriers are actively hidden in the existing signals. The SNR of each sub-carrier is $E_s/N_0 = 10$ dB, and the Interference-to-Signal Ratio (ISR) of three existing signals (ES_1,ES_2,ES_3 in Fig. 17) with each subcarrier interference signal is 18, 38.5, and 25 dB, respectively.

To further illustrate this trade-off, we simulated the Bit Error Rate (BER) of MC-DSSS shown in Fig. 17. Taking the simulation conditions of the 8 sub-carriers in Fig. 17 as an example, we tested the BER with 0 to 4 sub-carriers actively hidden in the existing signals, and the BER is plotted in Fig. 18. As shown in Fig. 18, the BER degrades as the fraction of the total frequency band concealed in the existing signals from 12.5 % to 50 %.

5) Non-SS Jamming Suppression Techniques: When the jamming power exceeds the maximum tolerance level of the SS receiver, the SS system has to employ dedicated jamming

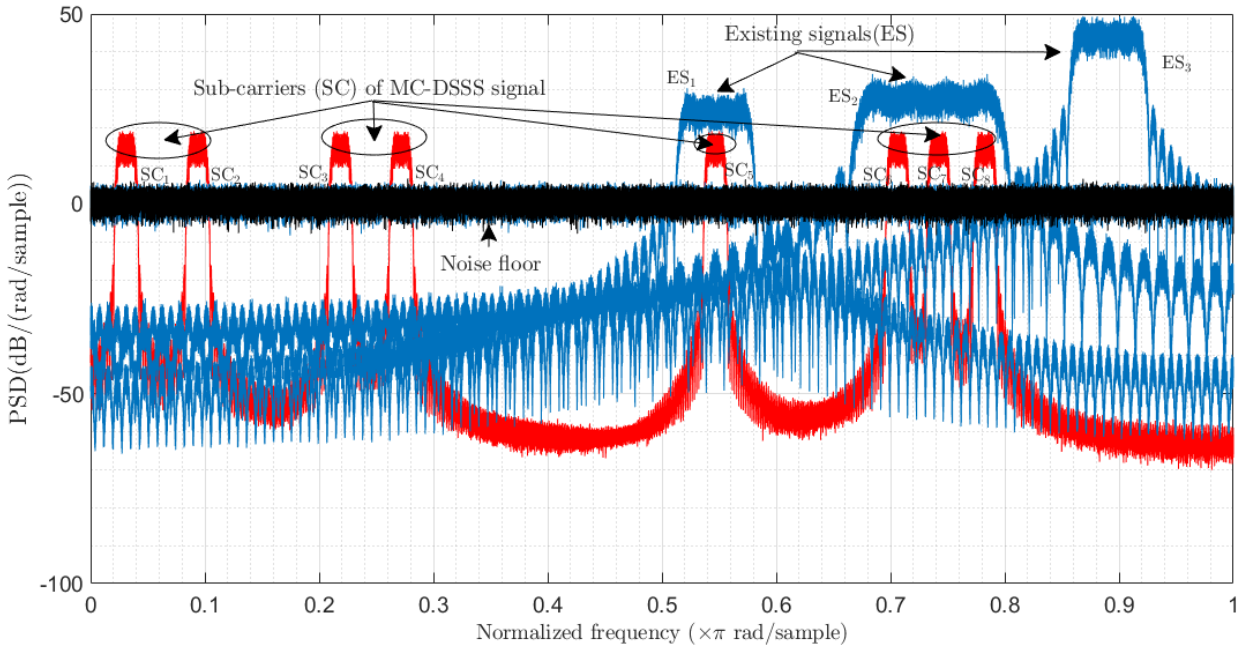


Fig. 17: The trade-off between confidentiality and integrity in MC-DSSS systems.

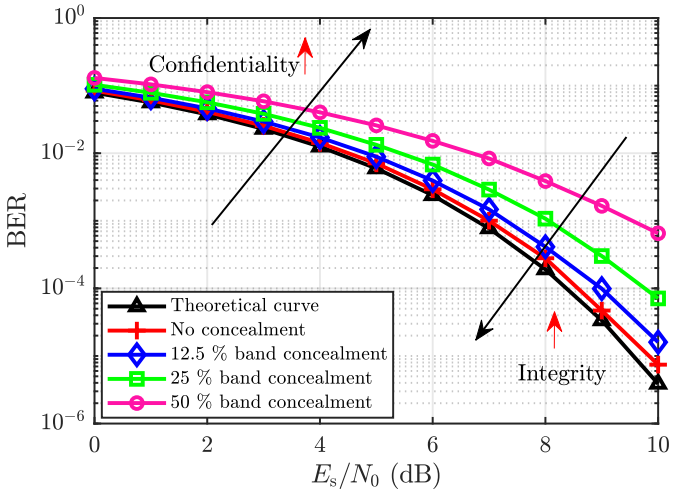


Fig. 18: The variation of BER with band concealed in existing signals.

suppression algorithms, such as temporal domain adaptive filtering [93] and transform domain adaptive filtering [94].

Temporal domain adaptive filtering algorithms are suitable for narrowband jamming suppression. The Least Mean Square (LMS) [93], [291] algorithm is a popular design option due to its low complexity. The basic idea behind the LMS algorithm is to mimic a causal Wiener filter by updating the filter weights until the least mean square of the error signal is approached. It is a stochastic gradient descent method, which means that the filter weights are only adapted based on the error at the current symbol instant. For a standard LMS algorithm, the convergence speed is determined by the step size parameter (μ), which may be gradually reduced upon approaching convergence to the minimum.

On the one hand, the higher the value of μ, the faster the weights converge. Hence, we can promptly track and mitigate the fluctuating jamming. On the other hand, the higher μ, the higher the variance of the weights will be, which affects the performance of jamming mitigation. Therefore, the realization of the LMS algorithm requires a trade-off, as seen in Fig. 19.

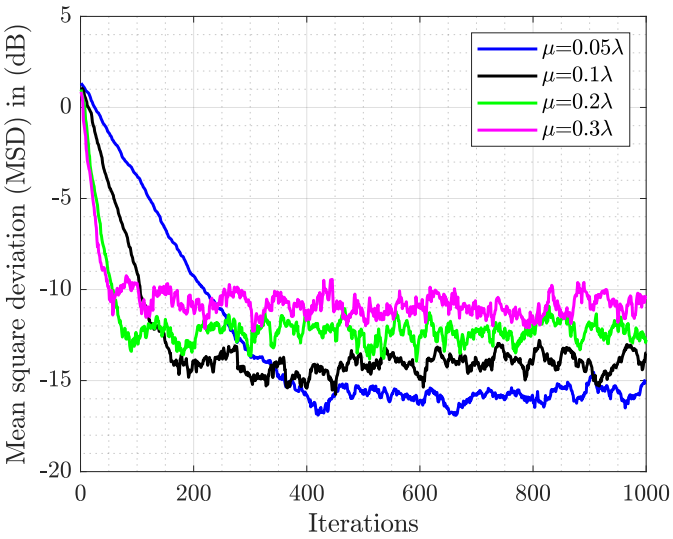


Fig. 19: The convergence performance of weights. The number of taps is 4. μ is given as $0 < \mu < \frac{2}{\lambda}$, where λ is the greatest eigenvalue of the autocorrelation matrix $R = E\{X(n)X^H(n)\}$.

By contrast, transform domain adaptive filtering is capable of promptly tracking the fluctuation of narrowband jamming

without an iterative process [292], [293]. Transform domain adaptive filtering processes the received signal in the frequency domain. Briefly, it identifies the jamming and carries out the band-pass filtering before transforming the signal back to the temporal domain.

6) Satellite Cooperation: With the explosive proliferation of connected terminals and the emergence of diverse applications, a single satellite can hardly satisfy the confidentiality and integrity requirements simultaneously, especially for LEO satellites having limited onboard resources.

Again, the open nature of wireless propagation makes legitimate transmissions vulnerable to eavesdropping, as seen in Fig. 20(a). The source transmits its signal to D, while E is capable of overhearing the legitimate transmissions if it is located in the coverage area of S.

Specifically, to improve the confidentiality of S, a common strategy is to reduce its transmit power. However, the system's integrity will also be reduced simultaneously. Conversely, by increasing the transmit power to improve the legitimate link's integrity, the probability of eavesdropping will also be inevitably increased [71]. This indicates a clear trade-off between confidentiality and integrity, which has been a long-term challenge for satellite communication researchers.

With the continuous deployment of LEO mega-constellations, such as Starlink [294], the number of satellites in space is increasing. Most locations on Earth's surface can be simultaneously covered by multiple satellites in these LEO mega-constellations, where a terminal can be covered by multiple satellites at the same time, as seen in Fig. 20(b). By beneficially combining the signals received from each satellite, the integrity of the combined signal can be maintained while allowing the terminal to transmit at lower power, thereby successfully tackling the previous trade-off between confidentiality and integrity. However, before combining, the delay, Doppler frequency shift, and phase offset of the signal received from each satellite have to be compensated.

Typically, each satellite can exploit the location information of the terminal to predict and compensate for the delay and Doppler frequency shift. However, due to the differences in satellite oscillators and startup times, estimation is the only way to deal with the phase offsets among these satellites. A modified SUMPLE [295] algorithm based on correlating the received signals was proposed in [296] to estimate and compensate the phase offsets, which is capable of coherently combining the DSSS signals received at different satellites. The authors of [296] also mentioned some promising future research directions, such as the exploration of cooperative detection and localization.

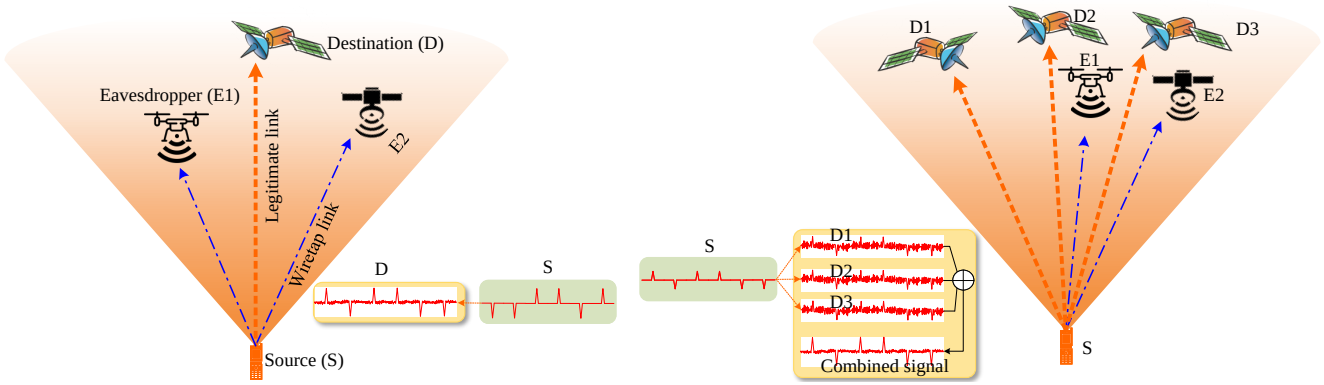
There are a number of LEO satellite cooperation research works that are based on the compensation of Doppler frequency shift, delay, and phase offset. In particular, the signals transmitted by several visible satellites to the target terminal can be combined through a specific combining scheme for reducing the jamming signal power [297], for enhancing the sensing accuracy [298], and for improving the overall performance [296]. Specifically, the authors of [297] proposed to combine all user-satellite links, where the transmit power of the user terminal targeted at each satellite was jointly optimized for maximizing the total data rate. The experimental results of [297] demonstrated that the deleterious effects of jamming can be mitigated when at least 3 satellites are available. This demonstrated the benefits of cooperation diversity against jamming.

Furthermore, due to the uneven distribution of users over the world, some LEO satellites do not have sufficient resources to serve the users in their coverage, while some other satellites may have unused resources. As the number of satellites has proliferated, the concept of satellite collaboration has attracted research attention in the interest of resource-sharing.

In general, cooperation among satellites is supported by information transmission among satellites through ISLs. For instance, in [299], the CSI estimated at each satellite is shared with others in the same constellation, which has the advantage of increasing the equivalent aperture of the satellite antenna. This sophisticated measure is capable of reducing the correlation between the legitimate channel and the wiretap channel, which has a positive impact on the PLS. In this context, the LEO satellites investigated in [300] served as a trusted relay to cooperatively realize QKD transmission between intercontinental ground stations. It was demonstrated that satellites deployed in different orbits were beneficial while placing more satellites in the same orbit did not introduce substantial security performance gains. The benefits of relaying satellites were also investigated in [301], where an LEO satellite forwarded its task to another collaborative satellite or ground gateway via a GEO satellite to achieve load balancing among LEO satellites. The task offloading, communication, and computing resource allocation were jointly optimized for minimizing the task processing latency by a bespoke deep reinforcement learning solution in support of confidential delay-sensitive services.

Additionally, the routing mechanism of satellite networks composed of a multitude of satellites also needs cooperation among satellites and the construction of ISLs. The cooperation mechanism of satellites should be carefully designed to ensure secure routing while taking both their dynamic topologies, constrained resources, and large coverage area into consideration. In the existing literature, routing is mainly secured by cryptography, and by some trust mechanism. More explicitly, typically encryption is utilized to ensure that the routing information transmitted among nodes achieves the required degree of confidentiality. Specifically, in [302], hop-by-hop encryption is proposed for securing the multicast routing within a three-layer satellite network composed of both LEO, highly elliptic orbit (HEO), and GEO satellites. Briefly, each intermediate satellite node encrypts the routing packets with the aid of its own private key, which can be decrypted through its public key. In this case, the transmitted packets are safeguarded from malicious nodes, since the latter cannot access the routing information without the right key.

From a trust mechanism perspective, the trust concerning a specific routing path is determined by the degree of trust attributed to the network nodes, which is typically inferred from their previous behavior. In general, the node having a higher degree of trust has a higher probability of being selected,



(a) The scenario of single satellite

(b) The scenario of multiple satellite cooperation

Fig. 20: The concept of satellite cooperation.

while a node associated with a low degree of trust might be removed from the network. In fact, different satellite networks calculate the degree of trust based on various standards. For instance, Yu *et al.* [303] monitor both the packet forwarding rate and that of abnormal behaviors to evaluate the degree of trust in a cluster-based multi-layer satellite network. They also demonstrated the robustness of their technique against DoS and disruption attacks. The so-called signature mechanism, which is one of the cryptography algorithms, is utilized in the routing process to prevent packets from being tampered with or imitated. By contrast, the degree of trust in a micro-nano satellite node was evaluated by another metric, namely by observing the attacking behavior, and the residual energy [304]. To improve the robustness of the trust mechanism, the estimated degree of trust having a value lower than a certain threshold can be re-evaluated by a different node relying on the same evaluation standards. The degree of trust evaluated in a centralized manner in [305] is based on the average estimated by the neighbors of each node according to the previous behaviors. Although this method requires more computations, it has a higher attack identification capability. Additionally, a load-balancing strategy is adopted in [305] when performing path selection, which aims for preventing high-trust nodes from becoming congested, while others remain idle. However, both the cryptography-based and trust-based routing reviewed above relies on single-path routing, hence suffering from a high path failure risk. As a remedy, multi-path routing is proposed in [306] for reducing the risk by transmitting redundant data copies along multiple paths at the same time, which outperforms its single-path counterpart by avoiding re-routing.

In a nutshell, satellite cooperation generally outperforms stand-alone satellite operations, but there are numerous open problems awaiting further exploration.

Lessons Learned: As it transpires from the literature, the important prerequisites of LEO satellite cooperation are the compensation of Doppler frequency shift, delay, and phase offset, which requires the synchronization of multiple satellites. However, the dimensionality of these tasks grows exponentially with the number of satellites. To make things worse, the high mobility of LEO satellites lead to an excessive range of Doppler frequency shift. Therefore, both the range and dimensionality of these tasks constitute severe challenges for the synchronization of multiple satellites. However, based on the existing solutions, the satellite exploits the known terminal location to predict and compensate for both the Doppler frequency shift and the delay, thus avoiding the explicit direct estimation of these two parameters. However, the user terminal location constitutes an important aspect of user privacy. Hence the synchronization of multiple satellites is worth exploring.

7) Artificial Intelligence: Although the above-mentioned passive security enhancement solutions are indeed capable of enhancing the security of LEO SCSs, they often lead to challenging non-convex optimization problems under strict performance constraints, and to optimization objectives involving coupled variables. Hence only a near-optimal performance can be obtained at the cost of high computational complexity. Many of the existing strategies are difficult to implement in practice, especially when considering that LEO satellites have limited energy resources and computational capability. In the face of uncertainty, AI-aided active security enhancement solutions may be harnessed for prediction and detection. They can also be invoked as an efficient passive security solution for solving complex optimization problems.

One of the representative application fields of AI is found in solving the beam-hopping problems of LEO SCSs, with the objective of minimizing the impact of harmful interference. Xu *et al.* investigated deep reinforcement learning aided dynamic beam hopping in multiple-beam satellite systems [307]–[310]. Specifically, in order to cope with the randomly fluctuating traffic demands and time-variant wireless channel conditions, deep reinforcement learning was combined with simulated annealing in [308]. As a further development, multi-objective deep reinforcement learning techniques were developed in [307], [309]. Furthermore, a multi-agent deep reinforcement learning method was proposed in [310], where each beam acted as an agent but operated cooperatively. The objectives and constraints of the beam-hopping optimization problem formulated are typically related to the SINR, which is directly influenced by the co-channel interference encountered.

In order to mitigate the CCI between adjacent beams, the intelligent method developed in [310] estimated the received signal strengths in the overlapping areas and arranged the spatial relationship of the beams for ensuring that the adjacent beams do not adopt the same frequency resources.

In [263], interference-related sum-rate maximization problems have been formulated with the objective of optimizing the passive beamforming vector at the RIS, which were solved by graph attention networks belonging to the family of unsupervised offline learning techniques. They were shown to be capable of capturing the dynamic RIS-assisted LEO SCSs network topology at a low online complexity. Moreover, the authors of [259] adopted a DL framework to find the optimal RIS coefficients in a secrecy capacity maximization problem, which achieved desired long-term goals at a high convergence efficiency and sample efficiency.

On the other hand, intelligent passive security enhancement solutions can be utilized to prevent LEO SCSs from jamming attacks. As the wireless networks become smarter, so do the jamming attacks. For example, jamming actions may have the capability of learning and reasoning. The SCS associated with cyclic visibility and fixed orbit is exposed to these intelligent jamming attacks, potentially leading to congestion. The traditional anti-jamming methods, such as DSSS, FHSS, multi-beam antennas, and self-adaptive routing, cannot reliably handle these smart jamming attacks. A suite of intelligent anti-jamming designs has been conceived for SCSs by Han *et al.*. Specifically, in [311], they formulated a hierarchical anti-jamming Stackelberg game to demonstrate the interactions between smart jammers and satellite users. They also proposed a two-stage anti-jamming scheme, where the first stage uses deep reinforcement learning to reduce the routing decision space. By contrast, the second stage relies on Q-learning to promptly accomplish anti-jamming routing. In the follow-up work [312], the authors developed a distributed dynamic anti-jamming for a satellite-assisted military IoT network, which cut energy consumption without substantially eroding the performance. The jamming attacks were analyzed and they were counteracted by deep reinforcement learning-based anti-jamming policies. However, since their method relied on analyzing the confrontational interaction between jammers and legitimate users, the anti-jamming performance was inevitably influenced by the accuracy of detecting the existence of jamming attacks. More recently, the authors of [313] proposed a cross-layer anti-jamming method involving both the link layer and the network layer, which performs better than a single-layer anti-jamming technique. The link layer handled the particular channel jamming by harnessing sophisticated Q-learning, while the network layer tackled the inter-satellite link jamming by finding new routing paths with the aid of a deep Q network algorithm. However, this algorithm only fits the jamming problems associated with a low-dimensional scenario, bearing with the limited processing capability, and energy cost, which leaves numerous open problems for further investigation.

Lessons Learned: AI has made substantial progress in safeguarding LEO SCSs in the face of both active and passive information domain perspectives. Both the specific features and evolutionary trends of the traffic can be accurately predicted by AI tools, which helps avoid future congestion and high CCI. Moreover, AI can act as a near-optimal solver for complex non-convex optimization problems encountered by hybrid satellite communication systems in beam-hopping solutions, RISs, anti-jamming techniques, and so on. However, the success of AI applications in LEO SCSs hinges on having a sufficiently large amount of training data, which might be inaccessible in practical communication scenarios.

C. Reliability Enhancement Solutions

Reliability solutions, including Space Situational Awareness (SSA), debris removal, and radiation resistance, are capable of supporting the stable operation of LEO satellites. Therein SSA employs lots of ground-based facilities or space-borne facilities and novel algorithms to detect and track debris. Moreover, debris removal is an effective means of cleaning up existing debris, thereby substantially reducing the risk of collision. In addition, radiation resistance can not only detect the occurrence of SEUs but also correct it.

1) Space Situational Awareness: The number of Resident Space Objects (RSO), including satellites, spacecraft, and space debris, orbiting the Earth has dramatically increased, hence posing a severe risk to space-based activities. To this end, governments, armed forces, and space agencies have set up SSA programs for collision warnings, and debris removal [314]. SSA is based on accurate knowledge of the space environment, allowing the detection and tracking of the location of RSO at any time [315]. Table X summarizes existing studies on SSA in terms of debris detection and tracking.

SSA programs exploit a whole suite of sensors, including ground-based radar, optical telescopes, and space-based radar, for inferring the orbital features of objects with the inspiration of their classification and recognition [326]. In this context, ground-based radars and optical telescopes are eminently suitable for the observation of RSO. For example, the Tracking and Imaging Radar (TIRA) of [327] was demonstrated to be capable of debris detection in LEO. The Herstmonceux telescope [328] having a small aperture also operated in good weather conditions. However, both ground-based radars and optical telescopes have their pros and cons. Ground-based radars can operate all the time free from weather conditions, but one of their problems is related to their high costs due to their high transmitter power. Additionally, the ground-based radar can not accurately observe debris in LEO scenarios with a diameter smaller than 10 cm [320] because of their large aperture. By contrast, optical telescopes have high sensitivity for observation, but their observation time is limited by weather conditions [326].

As a remedy, the idea of exploiting either Space-borne Radar (SBR) or Space-borne Cameras (SBC) [325] was conceived for debris detection and tracking. They are closer to the target, hence they require lower transmit power. Numerous scholars have subsequently proposed a variety of SBRs and SBCs [316], [318], [320], [321], [325]. Specifically, the coordination of multiple satellites carrying cameras was adopted in [316], [318] for space debris detection and tracking. The

TABLE X: The evolution of SSA

Year	Ref.	Target	Proposed algorithm/scheme	Results
2011	[316]	Tracking	A multiple satellite cooperation method to obtain the 3D debris information	Adjusts the satellite's orbit to maintain camera concentrating on target debris during tracking
2017	[317]	Tracking	The CDEKF as a variable discretization resolution	Exploits discretization and linearization of CDEKF to improve the tracking performance
2017	[318]	Detection	A satellite formation control algorithm to detect and track debris cooperatively	Calculates and adjusts actions of satellites to focus each the sensor carried on common debris
2017	[319]	Tracking	A consensus LMB filtering for distributed debris tracking	Solves the problems of debris tracking and its dataa incest
2018	[320]	Detection	A Space-borne THz Radar at 340 GHz	Provides high-resolution 3D imaging of spinning space debris
2018	[321]	Detection	A Space-borne MmWave Radar at 94 GHz	Employs COTS components and GaN solid-state technology to demonstrate a space-borne radar
2019	[322]	Tracking	A novel Lie-group based parameterization method	Derives an iterated EKF on Lie groups to track a cluster of debris
2019	[323]	Detection Tracking	A deep convolutional neural network based space debris saliency detection method	Improves the detection performance by deep convolutional neural network
2020	[324]	Detection	A feature learning of candidate regions method for space debris in optical image	Removes hot pixels, ficker noise, and nonuniform background for improving detection performance
2020	[314]	Tracking	A ML-based approach for improving orbit prediction in LEOs	Achieves at least 50% accuracy improvement of debris tracking
2021	[325]	Detection Tracking	A Space-borne Ka-band Radar at 35.5 GHz	Employs Filter Banks to combat Doppler shift for improving the capabilities of detection and tracking

estimated 3D position of the debris may be determined from two 2D images of cameras aboard the satellites flying in a formation [316]. A two-stage asymptotically stable nonlinear robust tracking controller was adopted in the formation reported in [316] for maintaining the target debris within the cameras' fields of view. A network of distributed space-borne optical sensors was shown to be able to detect and track debris in [318]. Torres *et al.* [321] presented further technological developments for a space-based radar prototype operating at 94 GHz for detecting centimeter-sized debris. Maffei *et al.* proposed a novel SBR payload architecture relying on the Ka-band. Moreover, a filter bank associated with a group of Doppler frequency shifts was also designed in [325] for improving the Doppler tolerance. Bayesian inference was adopted for precisely tracking the trajectory of a piece of debris for several hundreds of milliseconds. Yang *et al.* [320] designed a solid-state THz SBR operating at 340 GHz by relying on the so-called inverse synthetic aperture technique and obtained a high-resolution 3D image of spinning debris.

Both Kalman filtering [329] algorithms and Bernoulli filtering [330] algorithms have been used for debris tracking. Specifically, Dhondea *et al.* [317] discussed the Continuous-discrete Extended Kalman Filtering (CDEKF) technique of debris tracking. For tracking a cluster of debris sufficiently close to each other, Labsir *et al.* [322] formulated the problem as a filtering problem constructed over Lie groups [331] and derived an iterated extended Kalman filtering for the tracking of debris. As a further advance, a consensus-based Labeled Multi-Bernoulli (LMB) filtering method was adopted in [319] for estimating the state of debris. Wei *et al.* [332] proposed a multi-sensor-based space debris tracking algorithm relying on δ generalized LMB filtering. This algorithm was also used for identifying unknown debris by involving a measurement-based 'birth' model.

Lessons Learned: The capabilities of space-borne solutions relying on THz radars should be further improved. As detailed in [187], the space-borne systems are potentially capable of safeguarding the information carried among LEO satellites by THz-based ISLs. As a benefit, they can also detect space debris for protecting the satellite with the aid of THz-based radar [320]. However, the maximum attainable transmission power of space-borne THz equipment severely limits both the communication distance [190] and the radar detection distance, which calls for the conception of large-scale space-borne antenna arrays and high-power devices as part of future research.

2) Debris Removal: In practice, the LEO orbits are the most densely contaminated by space debris among all orbits. Therefore LEO satellites are at the most significant risk of being hit by debris. The accurate debris detection, tracking, and removal planning supported by the AI, sensors, and filtering algorithms introduced above have laid the foundations for our ensuing discussions on debris removal. Anecdotally, researchers in Japan are even experimenting with wooden spacecraft to minimize the amount of space debris [333]. At the time of writing, many institutes are contributing to the clean-up of space debris by harnessing the following techniques.

Nets and Harpoons: The most famous initiative is that of European research institutions employing dedicated spacecraft to snare debris by firing harpoons and nets at them [334]. These space fishing nets are thousands of meters in diameter and are made of extremely fine wires that are woven together and strong enough to withstand the impact of space debris. The mesh is launched aboard a satellite to be deployed into space, and then it travels along Earth's orbit to sweep up space debris as it passes. Due to the gravitation of the Earth, it finally

falls into the atmosphere and burns up. On September 16th, 2018, the RemoveDEBRIS satellite captured a nearby target probe that the vehicle had released a few seconds earlier, which verified the feasibility of this method [335].

Another alternative is to use space harpoons for 'hunting' satellites. Specifically, such hunting satellites employ a lidar-based guidance system to locate space debris, and a pneumatic device is designed to control the harpoon while catching moving targets. The hunting satellites could also carry tiny sub-satellites that would push the debris into the atmosphere to burn it up.

Laser 'Scavengers': A new way to deal with space debris has been proposed by Australian scientists based on adopting firing lasers from the Earth to break up space debris [147]. There are two main ways of using lasers to clean up space debris. For tiny debris, high-power laser light can be used to melt and vaporize it. Larger pieces of debris can be hit at a point, generating a backlash like a rocket jet. Thus, its course changes accordingly, and then it will drop into the Earth's atmosphere and burn up.

Robotic Arms: Japan's Aerospace Exploration Agency has also developed a robotic 'cleaner' that can use a robotic arm to firmly grasp large pieces of space debris, e.g., dead satellites, and collect them for hurling into the atmosphere to burn them up. The robot, which weighs about 140 kg, has a robotic arm equipped with powerful magnets that can be used for slowing down space debris orbiting the Earth. However, the characteristics of most space debris are not precisely known beforehand, which results in measurement errors concerning the relative motion between the robotic arm and space debris. This makes capturing space debris complicated [336].

Giant Balloons: It is generally possible for a satellite to fire up its engines at the end of its life and head towards the Earth to burn up in the atmosphere, which would require extra fuel and eventually increase the cost of launch. The new cheaper solution is to carry a folding balloon from launch filled with helium or other gases. Once the satellite exhausted its lifespan, it could blow helium bubbles to increase its drag through the atmosphere [337]. It takes only a year for a 37-meter-diameter balloon to drag a 1200 kg satellite out of its initial 830 km orbit and to crash it into the Earth's atmosphere to burn it up.

'Suicide' Satellites: The aforementioned methods of removing space debris, like using nets, harpoons, robotic arms, or lasers, are costly. Scientists in the UK developed a low-cost device called Cubic Sail to clean up space debris [338]. CubeSail is a 'suicide' micro-satellite, weighing just 3 kg, that can be launched into space. Once locked on to its target, it would deploy its kite-like solar sail, attach itself to space debris and slow its flight. Eventually, they will perish.

Table XI compares the advantages and disadvantages of these debris removal techniques. However, these solutions are currently in the design or experimental phase, and more engineering efforts are required to put these ideas into practice.

3) Artificial Intelligence: The AI family, especially ML, and DL, also find wide-ranging applications in collision avoidance and debris identification as well as removal planning.

Collision Avoidance: The rapidly escalating number of mega-constellations inevitably increases the risk of collision, especially in the LEO orbit, which has numerous objects traveling at high speed in an uncontrolled manner, including rocket body parts, dead satellites, shrapnels, and debris. In fact, collisions could generate additional orbiting debris that, in turn, produce further collisions and thereby trigger an avalanche-like debris growth chain reaction, which prompts space institutions and agencies to intensify their collision avoidance actions. The release of real-world datasets in the form of messages containing information about collision times and risks of near-miss events lays the foundation for the utilization of ML tools to avoid collisions [339], [340]. Specifically, the authors of [339] described an open-source Python package named Kessler to predict the evolution of conjunction events in a reliable manner by relying on Bayesian neural networks. A milestone in solving space collision challenges was achieved by the European Space Agency [340], by organizing an ML competition based on a large curated dataset to inspire competing teams to find the best collision risk estimation model. The competition results demonstrated the difficulties in finding a generic training set and highlighted the benefits of ML techniques in this research field.

Debris Identification and Removal Planning: Although the amount of debris can be reduced by adopting effective collision avoidance strategies, the LEO orbits are still contaminated by space debris that comes from explosions, impacting other space objects or launch activities. As Wyler, the founder of OneWeb, said: "My epitaph should say 'Connect the World' instead of 'Making Orbital Garbage'." To exploit the space debris and effectively exploit the LEO for future exploration, we must make concerted, collaborative efforts to both prevent the generation of future debris and eliminate existing space debris. The above reliability enhancement solutions, such as robotic arms, are capable of pushing the failing or inoperative spacecraft into Earth's atmosphere and burning them down. This is an effective means of mitigating the generation of space debris. However, given the dynamically time-varying factors in the space environment, the practical operational feasibility of the above reliability enhancement solutions should be carefully verified before any action in the face of the associated uncertainties. This requires substantial online or offline computing capability to identify targets, as well as to plan and track their trajectories before capturing moving targets [341].

In this context, the first step, namely space debris detection, is associated with a considerable challenge, since debris appears as a blob without visual features. Moreover, the reflectivity of debris is weak both due to its mobility and owing to the noise in the cosmic space due to the cluttered starry background. This leads to extremely low SNR. By exploiting the strong pattern recognition capability of DL, the authors of [323], [342] constructed neural networks to detect space debris. The input of the convolutional neural network proposed in [323] was a local contrast map derived from the space-based surveillance video. The spatiotemporal saliency information captured from a local contrast map enhanced the robustness when facing time-varying noisy background. To increase the detection speed, the authors of [342] split the space image captured into small tiles of the same size, where a binary label was assigned to each tile to show whether there

TABLE XI: A table comparison of debris removal techniques

Project	Advantages	Disadvantages
Nets and harpoons	Able to handle irregular and spinning debris compared to a robotic arm	Nets is not able to be reused
	Nets prevent further debris generation	Smashing large space debris by harpoons may generate further debris
Laser 'scavengers'	Effective for small space debris	May burn up the debris causing extra debris
	Able to dexterously handle tumbling debris	Large amount of beam energy, because it is hard to generate a small beam at a long distance
	Able to be reused	Sophisticated target detection and acquisition system
Robotic arms	Able to grasp space debris firmly	Sophisticated control
	Able to be reused	Easily penetrated by debris, especially sharp debris
Giant Balloons	Effective large space debris such as failing or inoperative spacecraft	Easily penetrated by debris, especially sharp debris
	Preventing further debris generation	Slow response because of balloon inflation
'Suicide' Satellites	Preventing further debris generation	Not able to be reused
	Low cost	Suitable for larger debris

is space debris located in it. Once the debris is identified, the remaining task is to decide how to remove it. Since reinforcement learning relies on reward collection, it fits the objective of the active multi-debris removal mission planning problem of LEO SCSs [343]. The experiments relying on the Iridium 33 system confirmed that reinforcement learning constitutes a beneficial online reactive planner. However, not all the debris can be 'de-orbited' in time to avoid causing interruption to the inter-satellite laser links. The authors of [344] thus discussed several common laser link interruption scenarios, followed by an interruption risk perception model relying on a powerful ML tool, which lays the foundation for developing adaptive routing strategies. In summary, the AI family, especially the ML and DL techniques have diverse wide applications both in active and passive security provision and in reliability enhancement solutions. The existing literature on AI-based enhancement solutions is summarized at a glance in Fig. 21.

Lessons Learned: Reducing the probability of collision risk caused by space debris requires each country and research institution to bear corresponding responsibilities and establish an international cooperation mechanism as well as a shared resource platform to jointly research and carry out space debris clean-up actions. This is the only way of effectively reducing the impact of space debris for ensuring the smooth and sustainable development of future space activities. First of all, each country and institution should reach a consensus and adopt measures for preventing the creation of additional space debris.

Firstly, during the satellite launch process, consider the reusability and recyclability of the spacecraft exemplified by SpaceX's Falcon series rockets [345]. Once the lifespan of a satellite ends, we must consider the safe and effective removal of the satellite from its orbit. This removal process aims for ensuring that the satellite is completely burned up in the Earth's atmosphere, thus preventing any potential space debris from posing a future threat to other spacecraft.

To deal with the existing space debris, all countries should introduce effective debris removal measures, such as robotic arms, giant balloons, nets as well as harpoons, to collect large space debris and pull it back into the atmosphere for direct burning.

During a satellite's operation, it is necessary to detect and track space debris by SSA. Ground-based radar and optical telescopes are commonly used for detecting and tracking space debris. In the event of a collision risk, the satellite can be controlled by the ground segment to perform emergency avoidance maneuvers. Meanwhile, the satellite itself should be equipped with SBRs or SBCs, which can also help reduce collision risks. Furthermore, the exploitation of AI tools for learning and training on data generated by these SBRs and SBCs results in the improvement of detection and tracking.

4) Radiation Resistance: Radiation resistance is an engineering problem involving advanced chip technology and different forms of redundancy for ensuring the reliable operation of the space-borne payload in harsh space environments. The formulation of radiation resistance measures usually obeys the process shown in Fig. 22. The time-invariant functions should be implemented by ASICs, while the programs that have to be upgraded or iterated should be implemented using FPGAs because of their flexibility.

For the program implemented in FPGAs, usually, TMR is adopted for preventing the impact of SEUs [346]. Briefly, TMR is a fault-masking scheme based on feeding the outputs of three identical copies of the original program module to a majority voter. If the output of the three modules is the same, the system will be regarded to operate normally. If any faults occur in one of the modules, the other modules can mask the fault. Thus, TMR can efficiently prevent single faults from propagating to the output.

However, there is a trade-off between resource consumption and integrity. The resource consumption of TMR is three times that of the original program module. Hence, designers usually apply the TMR philosophy only to the key part of the program,

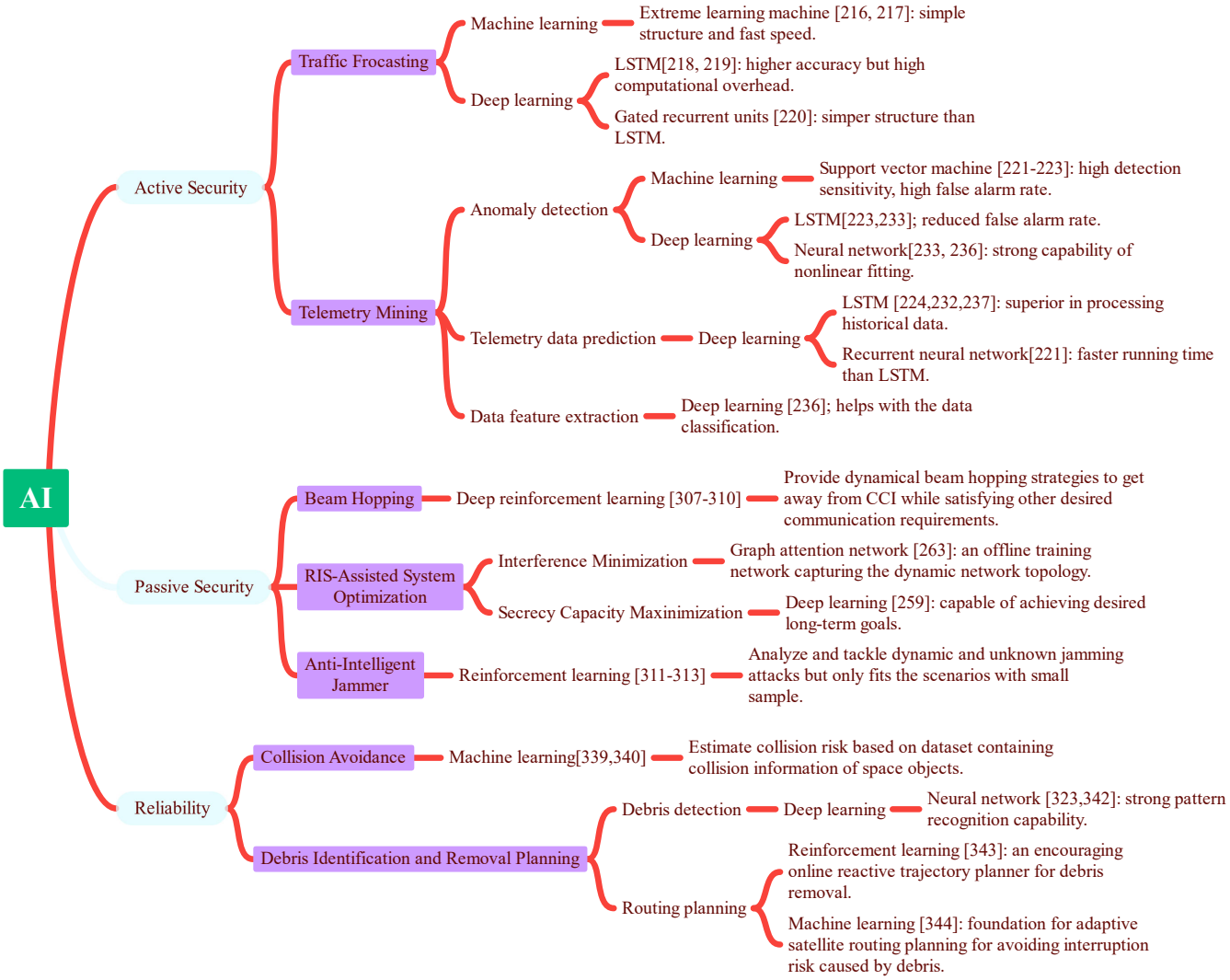


Fig. 21: Literature review for AI-based enhancement solutions.

such as the control part.

Another radiation resistance solution is periodical refreshing [347], which can correct errors by refreshing the program without interrupting its execution, as detailed in [348]. However, the block Random Access Memory (RAM) used in FPGAs will be initialized during the periodical-refreshing operation when its real-time state is lost. Hence the block RAM should also adopt TMR for coping with the impact of SEUs [349].

Lessons Learned: Based on our detailed literature review, we can clearly identify the advantages and disadvantages of both TMR and periodical refreshing. TMR is capable of detecting the occurrence of SEUs and correcting their effect. Thus, there is no doubt that TMR mitigates the impact of SEUs, but at the cost of certain additional resource consumption. The resource consumption of TMR may be as high as three times that of the original program module [350]. Although periodical refreshing does not impose additional resource consumption, it cannot cover all types of FPGAs resources, such as block RAM. As a remedy, the combination of partial TMR and periodical refreshing may improve the FPGAs' reliability.

D. Trade-offs in Quality of Service (QoS) guarantees

As mentioned above, in consideration of service type, inherent characteristics of LEO SCSs, security and reliability issues as well as solutions, there exists substantial trade-offs in QoS guarantees.

- It is of vital importance to determine the specific choice of solutions to be employed by the different segments of LEO SCSs according to the specific trade-offs between the security improvement attained and its cost in terms of the overhead imposed. As detailed in [19], [26], [145], data confidentiality can be maintained by traditional mathematics-based encryption schemes. However, LEO satellites are considered to have limited computation capabilities [351], hence the encryption schemes relying on excessive computational complexity are unsuitable for them, but they are routinely used at ground segments for improving the security level.
- There is a trade-off between the integrity related to traffic rate and anti-jamming capabilities indicated by the integrity when using the DSSS technique. More specifically, given the communication bandwidth, the traffic rate

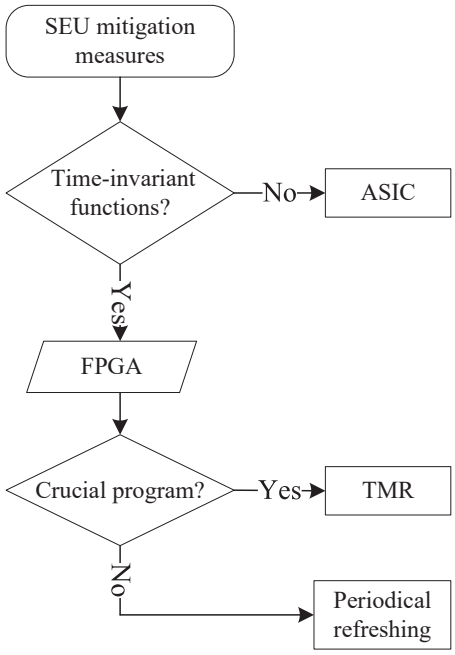


Fig. 22: A flow chart of radiation resistance measures.

is related to the spreading factor. When the jamming is strong, the spreading factor should be increased to improve the anti-jamming capability, hence leading to integrity reduction and *vice versa*.
There is also a trade-off between integrity and the confidentiality of MC-DSSS systems, as seen in Fig. 17 and Fig. 18. As reported in [352], a fraction of the sub-carriers may be hidden in the existing signals, which improves the confidentiality of the transmitted signal, but potentially degrades the integrity indicated by BER, and *vice versa*.

- Non-SS jamming suppression techniques, including transform domain adaptive filtering and temporal domain adaptive filtering, can be used for improved jamming mitigation. Between them, the LMS algorithm, which is a low-complexity design option for the temporal domain adaptive filtering technique, is eminently suitable for space-borne payloads. However, there is a trade-off concerning its iterative step size. The authors of [293] provided evidence that a higher step size leads to faster convergence but also to a higher variance of the weights. Furthermore, the more rapid convergence of the weights results in low latency, hence promptly tracking and mitigating malicious jamming. However, the resultant higher variance of the weights may affect the performance of jamming mitigation, which undoubtedly degrades the integrity.
- TMR is capable of not only detecting the occurrence of SEUs but also correcting its effect. Thus, there is no doubt that TMR mitigates the impact of SEUs, but at the cost of a certain additional resource consumption [347]. The resource consumption of TMR is three times that of the original program module. As a remedy, the combination of partial TMR and periodical refreshing may improve the FPGAs' reliability [348], [349].

VII. The Road Ahead

Given the rapid developments of satellite technologies, Integrated Sensing and Communication (ISAC) has great potential in terms of mitigating some of the challenges of LEO SCSs. This section will address their new opportunities in stimulating future research. Computer Vision (CV)-aided communication may provide new perspectives for secure space communications since accurate target detection, identification, and tracking can be offered by exploiting the information extracted. Additionally, the development of efficient and low-cost satellite production lines expedited the Mega-constellation planning and commercialization, which however exacerbates their security challenges. This section will address the emerging new opportunities for stimulating future research.

A. ISAC-aided Secure Transmission

With the rapid proliferation of connected devices and satellites, the available frequency spectrum assigned for wireless communications tends to be increasingly congested, which motivates network designers to seek spectrum reuse opportunities for the better exploration of bands originally assigned to other technologies. In recent years, the similarities between communications and sensing, such as their hardware components, antenna architecture, and signal processing modules attracted scholars to study a technology combining the two functional modules, leading to the concept of ISAC. The philosophy is to allow the communication systems to access large portions of the spectrum available at radar frequencies [353], [354].

The advantages offered by ISAC for SCSs include alleviating the shortage of radio frequencies, reducing overall system costs, cutting energy consumption, and miniaturizing the devices. In particular, the strong directivity, low sidelobe, and anti-interference capability of radar are capable of enhancing the information security, transmission reliability, communication quality, and coverage of the LEO SCSs [355]. Additionally, the sensing part in ISAC can partially characterize the propagation environment, which potentially improves the CSI estimation accuracy and reduces the channel estimation overhead. Moreover, the sensed movement and location information of high-mobility objects facilitates LEO SCSs to improve their beam alignment strategies and routing protocols [356].

On the other hand, the information obtained from communications, in turn, assists high-accuracy localization, real-time tracking, and high-precision imaging, as well as activity recognition [356], which has great potential in safeguarding the security of LEO SCSs. For instance, high-accuracy localization and tracking lay solid foundations for the debris removal operation. Additionally, the high-precision imaging relying on the support of AI allows LEO SCSs to be trained to dramatically reduce the risk of space collisions. The LEO SCSs are also expected to have high classification accuracy to detect anomalies and impending faults by continually sensing their surroundings.

The application of ISAC brings along additional challenges. The bottlenecks faced by ISAC in other wireless networks also

exist in LEO SCSs. For instance, it has to investigate unified performance metrics that examine the communication-sensing trade-off, clarify the fundamental limits of ISAC under practical considerations, and develop low-complexity, yet accurate ISAC signal processing algorithms [357]. Moreover, the mobility and hardware limitations of LEO satellites introduce further challenges, including limited synchronization resolution, restricted channel coherence time, high-speed moving targets, and insufficient computational capability. These factors make it more challenging to employ ISAC in LEO SCSs efficiently and reliably. Additionally, the massive amounts of data generated by ISAC, which contain sensitive information, impose further challenges on securing LEO SCSs. However, there is a paucity of literature on the integration of ISAC into LEO SCSs. Only a brief conference paper [361] has considered the simultaneous communication and sensing capabilities, highlighting the inevitable propagation delay and significant Doppler shifts in LEO SCSs that necessitate sophisticated solutions. Therefore, substantial further investigations are required to explore how to leverage the unique advantages of ISACs to enhance the security of LEO SCSs, while addressing the accompanying challenges.

B. CV-aided Space Communication

Recently, some researchers proposed CV-aided [358]–[361] communication schemes for mmWave or THz transmission systems in which LoS propagation is critically important. In contrast to ISAC, the core idea of CV-aided methods is to extract, recognize, and estimate useful information about the associated static system topology, including the terminals' positions, distances among themselves, and their number. It is also beneficial to keep track of their velocity, direction, and their number. The objective is to achieve new potential benefits in terms of improving wireless system design/optimization, such as resource scheduling and allocation, algorithm/protocol design, and so on.

Therefore, a pair of salient features of CV-aided schemes, which are beneficial for the security of LEO SCSs, can be summarized as follow: 1) One-way sensing capability: By employing optical cameras/devices [362], no RF signals have to be transmitted and received, hence resulting both in low detection probability by adversaries and in low resource consumption; 2) Hostile target/non-partner detection: Targets can be detected, identified, and distinguished via optical processing algorithms, and thus secure/covert information delivery schemes can be designed and implemented to avoid/hinder potential eavesdropping/perturbation [363].

Situational awareness in space has already been established by applying various optical and radar sensors, e.g., electro-optical/infrared systems and optical telescopes, they only survey, identify, and predict objects in orbit. However, at the time of writing, no literature exists on applying CV-aided methods to safeguard information transmissions in space. Given the unique high-dynamic and large-scale space scenarios of LEO SCSs, a number of challenges have to be tackled for realizing CV-aided space secure/covert communications in the field of ultra-high-speed target detection, carrying out reliable on-broad data processing and robust as well as secure transmission.

C. Mega-Consetellations

In light of the impending mega-constellation launch proposals, the number of active satellites in orbit will soar to around 50,000 in ten years, leading to an unprecedented scale of LEO SCSs. The operators of mega-constellations thus suffer from a heavy computational burden, since they have to supervise and manage the operational status and diverse functions of hundreds or even thousands of satellites in real-time. A minor computational or command error might have severe consequences for this giant network. Furthermore, large LEO SCSs require numerous ground stations and gateways. The authors of [364] estimate that around 123 ground station locations and 3500 gateway antennas are necessary for the 4400-satellite version of Starlink to approach the throughput limits. Such a large-scale deployment will require highly automated and secure management systems.

Additionally, the information exchange between the mega-constellations and ground stations relies on the inter-satellite network constructed by ISLs within the constellation. This is different from the traditional small-scale constellations, where the information exchange can be realized by the satellite-ground links or by the relaying assistance of the GEO satellites. Although the ISL strategy reduced the deployment costs of ground stations and relay satellites, the multi-hop inter-satellite networks are more vulnerable to malicious attacks due to their predominantly LoS propagation. The authors of [365] also highlighted that the total transmission delay of the multi-hop inter-satellite network should be taken into account in the context of security problems. In fact, a malicious node might succeed in masquerading as one of the legitimate nodes in ISLs to deliberately extend the data forwarding delay. Emergencies may even aggravate disasters, such as collisions and large-scale destruction. The solution proposed in [365] was based on the investigation of suitable routing algorithms by exploiting the knowledge of the degree of trust concerning each satellite, combined with other existing security technologies, including encryption, digital signatures, and so on. Nevertheless, the investigation of the security problems in mega-constellations is at an early stage, which urgently requires the researchers' attention to fill this gap.

D. LEO SCS Commercialization

Although there are still numerous open problems, the LEO SCS has reached a certain maturity. The vibrant LEO economy is attracting companies and investors. However, the crowded space and limited channel resources have resulted in intense competition among major companies. It will be hard to unify the quality of the satellites and their associated products with more and more partners entering the satellite communication industry.

Moreover, the commercialization also assists the development of LEO satellite applications, such as the IoTs, smart cities, and intelligent manufacturing, which provides tech giants with more business opportunities for combining the

space industry with hybrid network applications to boost their profit. However, the resultant trend imposes further aggravated security challenges, because the diverse nature of terminals, standards, and operational policies are more prone to attackers. For example, the ground segments of satellites in the Arctic are of strategic importance to the North Atlantic Treaty Organization, given their ability to collect intelligence from some leasehold commercial satellites. Hence the ground segment of these commercial satellites is increasingly, employed for both civilian and defense purposes, which makes them vulnerable to military targets [366]. In fact, the booming commercial applications, in turn, stimulate the production of LEO satellites. Their small size is a clear advantage from a financial perspective, but generally, this is achieved at the cost of a shortened life span. Therefore, companies also must have end-of-life plans before launching new satellites.

Although the future of the LEO SCS market seems bright at the time of writing, the experience due to financial issues should not be forgotten. Many companies, such as LeoSat, and OneWeb, have to scale back or even cancel their intended constellations unless they secure additional investment. The COVID-19 pandemic has inflicted uncertainty and challenges upon LEO SCS commercialization. On the other hand, their high cost makes the satellite-connectivity options expensive, which can only be afforded by a limited market segment, where terrestrial solutions are uneconomical. Investors might provide low-tariff space services at reduced profits to attract business at the beginning. Clearly, the LEO SCS market requires substantial upfront investment and cannot provide immediate positive cash flow, which thus increases the risk of financial challenges. Hence it is necessary to reduce costs, from materials to manufacturing, from the launch to the user equipment. Clearly, the cost reduction option should be carefully investigated to avoid low-quality products improving security problems.

VIII. Design Guidelines

The design of an LEO SCS is complex because it must consider numerous potentially conflicting design factors. In this section, we provide tangible design guidelines for LEO SCSs from a security and reliability perspective, which is derived from our critical review of the literature and the lessons learned concerning the security and reliability requirements, issues, and their corresponding solutions. The iterative procedure of our design guidelines is as follows.

A. Orbit Selection

The selection of satellite orbit is extremely complex. It is necessary to submit an application to the ITU as a prerequisite. From the perspective of reliability, the orbit selection has to consider two aspects: orbit altitude and orbit inclination. The selection of orbit altitude has to consider the distribution of already approved or deployed LEO satellites. The intensifying deployment of LEO mega-constellations has made low orbits more crowded, as shown in Fig. 11. On the other hand, the orbit inclination affects the probability of SEUs. In low Earth orbits, the higher the orbit inclination, the higher the probability of SEUs. Therefore, the orbit inclination has to be considered from two perspectives: collision avoidance (the number of satellites deployed in existing orbit inclinations) and reducing the probability of SEUs.

B. Frequency Selection

Similar to orbit selection, the frequency resources of LEO satellites also have to be requested from the ITU. From the perspective of security and reliability, frequency selection has to be based on both the business type and usage scenarios. For example, given the limited energy support of the IoT devices and narrow band low-speed communication of LEO satellites empowering the Internet of Remote Things as shown in Fig. 2(a), the L-band with low propagation loss is a good choice, whereas the K-band frequency is the preferred choice for high-throughput backhaul services supported by LEO satellites, as seen in Fig. 2(b).

When selecting specific frequencies, the existing frequency allocation should also be considered to avoid inter-system interference, as shown in Fig. 13. Additionally, the expanding emerging frequency bands can alleviate the problem of inter-frequency interference caused by the spectrum crunch. This is also one of the important reasons why THz and laser communications are gradually replacing the original K-band for ISLs [59].

C. Waveform Selection

Considering their inherent characteristics of concealment and anti-interference, SS waveforms, including DSSS, FHSS, and MC-DSSS, remain the most competitive. Among them, MC-DSSS has the feature of flexible sub-carrier allocation, which can be combined with CR to dynamically adjust its sub-carriers for mitigating the inter-frequency interference between systems.

D. Considerations before Design: On-board Processing is More Secure than Transponder

Attackers utilize satellite transmissions with no onboard processing to forward their own information, which is defined as transponder stealing in this paper, but the algorithms or programs running on the onboard processing system effectively prevent these illegal transmissions. Hence the onboard processing system avoids this eavesdropping behavior. In fact, the benefits of the onboard processing system in terms of improving security and reliability are not limited to this. A transparent forwarding system requires a large number of connected ground segments for achieving global coverage. The sheer number of ground segments is appealing to potential attackers, while the onboard processing system can achieve global coverage by relying on ISLs, and only a few ground segments are needed for stable operation. Additionally, in a transponder system, security and reliability enhancement solutions are concentrated on the ground segment, while onboard processing satellites can carry out extra security and reliability enhancement actions.

According to the inherent characteristics and the serious security challenges of LEO SCSs, the pertinent security and

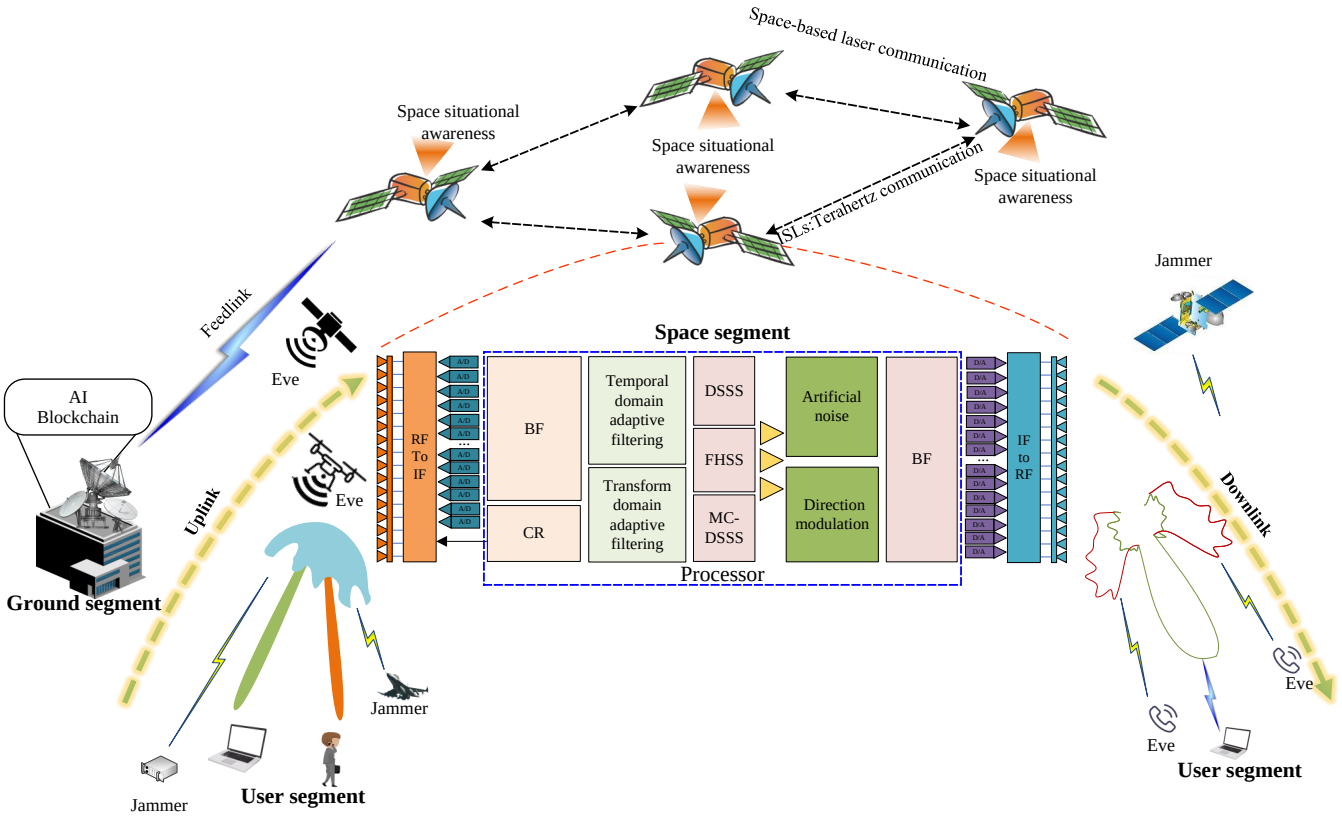


Fig. 23: Design guidelines of secure and reliable LEO SCSs.

reliability requirements were summarized in Sec. III, which are regarded as the most crucial requirements. Hence, the particular security specifications constitute the initial guiding policies for a designer. As an overriding principle, usually, complex encryption algorithms are harnessed in the ground segments of LEO SCSs as a benefit of their abundant resources, but they are typically unsuitable for the resource-limited satellites. They tend to require lightweight and low-power solutions.

E. LEO SCSs Secure and Reliable Design

After selecting the satellite orbits, the frequencies, and the waveforms, the secure and reliable LEO SCSs design has to proceed by bearing the aspects in Fig. 23 in mind.

1) Uplink: Advanced security-oriented antennas are adopted for mitigating eavesdropping and jamming. Furthermore, the increasing number of LEO satellites is laying the foundation for satellite cooperation. By combining the signals received from each satellite, the integrity of the combined signal with improved SNR can be maintained while allowing the terminal to transmit at reduced power, thereby improving security. Additionally, non-SS jamming suppression techniques [93], [94], including temporal domain adaptive filtering [291] and transform domain adaptive filtering [292], can be further used for improved jamming mitigation.

2) Downlink: Advanced security-oriented antennas can also be adopted for mitigating the eavesdropping and jamming probability in the downlink. The artificial noise can be released in directions other than that of legitimate users to drown out potential eavesdroppers. Moreover, the amplitude and phase of the downlink signals can be adjusted with the aid of RISs to further hinder the malicious actions of eavesdroppers and jammers.

3) The Processor of Space Segment: The increased probability of SEUs poses serious challenges to the reliable operation of programs or algorithms running onboard the satellites. Therefore, the processors have to be radiation-resistant, as intimated in Fig. 22.

4) Ground Segment: Again, the ground segment is the center of operation, management, and control for the entire LEO SCS. Any malfunction of the ground segment can potentially bring the system to a halt, hence it often becomes the preferred target of attackers. The ground segment having abundant power makes it possible to run more complex algorithms, such as encryption, machine learning, and blockchain, in the interest of improving security.

These algorithms can effectively address challenges like message modification, node compromise, DoS attacks, etc.

5) User Segment: Each user should update the patches at regular intervals for reducing the probability of successful attacks. Additionally, each user has to cooperate with the space segment, for example by adjusting the operating frequency or transmit power, for dealing with intra-system interference, such as MAI and CCI between beams.

F. LEO SCSs Secure and Reliable Operation

After completing the design of LEO SCSs, measures must also be taken to ensure their reliable and stable operation.

1) Collision Avoidance: Again, the increasing number of spacecraft and space debris in low Earth orbit poses a serious challenge to the reliable operation of LEO satellites. To address this issue, the maintenance personnel of the ground segment has to closely monitor the operational status of spacecraft and provide advance warning of potential collisions. Additionally, each satellite should be equipped with SBRs or SBCs to detect sudden, erratic space debris movements, and take immediate action to adjust the satellite's altitude to avoid collisions in case of risk.

2) Interference Coordination: According to ITU regulations [69], LEO SCSs shall not impose unacceptable interference on GEO SCSs. Under the coordination of LEO satellites, users carry out precise power control of the uplink signal to reduce their impact on the GEO system. Additionally, LEO SCSs may perform beam drifting for forcing the LEO satellite users to use their other beams in the downlink before interference actually occurs.

IX. Summary

LEO SCSs have attracted increasing attention as a benefit of their seamless global coverage with low latency. However, there are many open issues in the course of exploiting the full potential of LEO SCSs, including their security issues. Due to inherent characteristics such as special location, high mobility, and so on, LEO SCSs suffer severe security challenges. Not only security attacks, such as eavesdropping and DoS but also reliability risks, such as collisions and SEUs, affected the safe operation of LEO SCSs.

In this paper, we classified the issues encountered by LEO SCSs, summarized their characteristics, and discussed their lessons learned. To deal with these issues, we then introduced and summarized some corresponding solutions, which can be divided into security and reliability enhancement solutions. Moreover, we also provided numerous trade-offs and lessons. Based on this, we highlighted ISAC-aided secure transmission, CV-aided space communication, mega-constellation security problems, and commercialization issues for future research. Finally, we presented high-level design guidelines for secure LEO SCSs.

References

[1] J. Shi, Z. Li, J. Hu *et al.*, "OTFS enabled LEO satellite communications: A promising solution to severe Doppler effects," *IEEE Netw.*, pp. 1–7, Feb. 2023, doi:10.1109/MNET.129.2200458.

[2] N. Yang and A. Shafie, "Terahertz communications for massive connectivity and security in 6G and beyond era," *IEEE Commun. Mag.*, Oct. 2022, doi:10.1109/MCOM.001.2200421.

[3] F. Tang, C. Wen, X. Chen *et al.*, "Federated learning for intelligent transmission with space-air-ground integrated network (SAGIN) toward 6G," *IEEE Netw.*, Aug. 2022, doi:10.1109/MNET.104.2100615.

[4] C.-X. Wang, X. You, X. Gao *et al.*, "On the road to 6G: Visions, requirements, key technologies, and testbeds," *IEEE Commun. Surveys Tuts.*, vol. 25, no. 2, pp. 905–974, Second Quart. 2023.

[5] Z. Xiao, J. Yang, T. Mao *et al.*, "LEO satellite access network (LEO-SAN) towards 6G: Challenges and approaches," *IEEE Wirel. Commun.*, Dec. 2022, doi:10.1109/MWC.011.2200310.

[6] C. Guo, X. Chen, J. Yu *et al.*, "Design of joint device and data detection for massive grant-free random access in LEO satellite internet of things," *IEEE Internet Things J.*, Dec. 2022, doi:10.1109/JIOT.2022.3228730.

[7] X. Zhou, K. Ying, Z. Gao *et al.*, "Active terminal identification, channel estimation, and signal detection for grant-free NOMA-OTFS in LEO satellite internet-of-things," *IEEE Trans. Wireless Commun.*, vol. 22, no. 4, pp. 2847–2866, Apr. 2023.

[8] G. Pan, J. Ye, J. An, and S. Alouini, "Latency versus reliability in LEO mega-constellations: Terrestrial, aerial, or space relay," *IEEE Trans. Mobile Comput.*, Apr. 2022, doi:10.1109/TMC.2022.3168081.

[9] X. Qin, T. Ma, Z. Tang *et al.*, "Service-aware resource orchestration in ultra-dense LEO satellite-terrestrial integrated 6G: A service function chain approach," *IEEE Trans. Wireless Commun.*, Jan. 2023, doi:10.1109/TWC.2023.3239080.

[10] T. Ma, B. Qian, X. Qin *et al.*, "Satellite-terrestrial integrated 6G: An ultra-dense LEO networking management architecture," *IEEE Wirel. Commun.*, Dec. 2022, doi:10.1109/MWC.011.2200198.

[11] Z. Jia, M. Sheng, J. Li *et al.*, "Towards data collection and transmission in 6G space-air-ground integrated networks: Cooperative HAP and LEO satellite schemes," *IEEE Internet Things J.*, vol. 9, no. 13, pp. 10 516–10 528, Jul. 2022.

[12] M. Ying, X. Chen, and X. Shao, "Exploiting tensor-based bayesian learning for massive grant-free random access in LEO satellite internet of things," *IEEE Trans. Commun.*, vol. 71, no. 2, pp. 1141–1152, Feb. 2023.

[13] H. D. Le, H. D. Nguyen, C. T. Nguyen *et al.*, "FSO-based space-air-ground integrated vehicular networks: Cooperative HARQ with rate adaptation," *IEEE Trans. Aerosp. Electron. Syst.*, Jan. 2023, doi:10.1109/TAES.2023.3236904.

[14] Z. Han, C. Xu, G. Zhao *et al.*, "Time-varying topology model for dynamic routing in LEO satellite constellation networks," *IEEE Trans. Veh. Technol.*, vol. 72, no. 3, pp. 3440–3454, Mar. 2023.

[15] J.-H. Lee, J. Park, M. Bennis *et al.*, "Integrating LEO satellites and multi-UAV reinforcement learning for hybrid FSO/RF non-terrestrial networks," *IEEE Trans. Veh. Technol.*, vol. 72, no. 3, pp. 3647–3662, Mar. 2023.

[16] L. Zong, D. Qiao, H. Wang *et al.*, "Sustainable cross-regional transmission control for the industrial augmented intelligence of things," *IEEE Trans. Industr. Inform.*, Jan. 2023, doi:10.1109/TII.2022.3230674.

[17] D. Zhou, M. Sheng, J. Wu *et al.*, "Gateway placement in integrated satellite–terrestrial networks: Supporting communications and Internet of Remote Things," *IEEE Internet Things J.*, vol. 9, no. 6, pp. 4421–4434, Mar. 2022.

[18] I. Butun, P. Österberg, and H. Song, "Security of the Internet of Things: Vulnerabilities, attacks, and countermeasures," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 1, pp. 616–644, First Quart. 2020.

[19] B. Li, Z. Fei, C. Zhou *et al.*, "Physical-layer security in space information networks: A survey," *IEEE Internet Things J.*, vol. 7, no. 1, pp. 33–52, Jan. 2020.

[20] R. Han, L. Bai, C. Jiang *et al.*, "A secure architecture of relay-aided space information networks," *IEEE Netw.*, vol. 35, no. 4, pp. 88–94, Jul/Aug. 2021.

[21] Z. Bao, M. Luo, H. Wang *et al.*, "Blockchain-based secure communication for space information networks," *IEEE Netw.*, vol. 35, no. 4, pp. 50–57, Jul./Aug. 2021.

[22] W. Li, Z. Su, R. Li *et al.*, "Blockchain-based data security for artificial intelligence applications in 6G networks," *IEEE Netw.*, vol. 34, no. 6, pp. 31–37, Nov/Dec. 2020.

[23] J. Liu, Y. Shi, Z. M. Fadlullah *et al.*, "Space-air-ground integrated network: A survey," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 4, pp. 2714–2741, Fourth Quart. 2018.

[24] M. Lin, Q. Huang, T. de Cola *et al.*, "Integrated 5G-satellite networks: A perspective on physical layer reliability and security," *IEEE Wireless Commun.*, vol. 27, no. 6, pp. 152–159, Dec. 2020.

[25] P. Wang, J. Zhang, X. Zhang *et al.*, "Convergence of satellite and terrestrial networks: A comprehensive survey," *IEEE Access*, vol. 8, pp. 5550–5588, Dec. 2019.

[26] L. Mucchi, S. Jayousi, S. Caputo *et al.*, "Physical-layer security in 6G networks," *IEEE Open J. Commun. Soc.*, vol. 2, pp. 1901–1914, Aug. 2021.

[27] V.-L. Nguyen, P.-C. Lin, B.-C. Cheng *et al.*, "Security and privacy for 6G: A survey on prospective technologies and challenges," *IEEE Commun. Surveys Tuts.*, vol. 23, no. 4, pp. 2384–2428, Fourth Quart. 2021.

TABLE XII: List of acronyms

Acronyms	Definitions	Acronyms	Definitions
6G	Sixth-generation	MAI	Multiple Access Interference
ADS-B	Automatic Dependent Surveillance-Broadcast	MC-DSSS	Multi-Carrier Direct Sequence Spread Spectrum
AI	Artificial Intelligence	MEO	Medium Earth Orbit
AN	Artificial Noise	MIMO	Multiple Input Multiple Output
ASIC	Application Specific Integrated Circuit	ML	Machine Learning
BER	Bit Error Rate	MmWave	Millimeter Wave
BF	Beamforming	ms	Milliseconds
CCI	Co-channel Interference	NASA	National Aeronautics and Space Administration
CCSDS	Consultative Committee for Space Data Systems	NCC	Network Control Center
CDEKF	Continuous-discrete Extended Kalman Filtering	NTN	Non-terrestrial Network
CIR	Carrier to Interference Ratio	OGS	Optical Ground Station
COTS	Commercial Off The Shelf	PA	Phased Array
CV	Computer Vision	PG	Processing Gain
DDoS	Distributed DoS	PLS	Physical Layer Security
DoS	Denial of Service	PSD	Power Spectral Density
DSSS	Direct Sequence Spread Spectrum	PU	Primary User
ESA	European Space Agency	PUF	Physical Unclonable Function
FDA	Frequency Diverse Array	QKD	Quantum Key Distribution
FH	Frequency Hopping	QSDC	Quantum Secure Direct Communications
FHSS	Frequency Hopping Spread Spectrum	RAM	Random Access Memory
FFHSS	Fast Frequency Hopping Spread Spectrum	RIS	Reconfigurable Intelligent Surface
FPGA	Field Programmable Gate Array	RSO	Resident Space Objects
GEO	Geostationary Earth Orbit	SAGIN	Space-air-ground Integrated Network
GHz	Gigahertz	SBC	Space-borne Camera
GPS	Global Position System	SBR	Space-borne Radar
HTS	High Throughput Satellites	SIN	Space Information Network
IDS	Intrusion Detection Systems	SCS	Satellite Communication System
IoRT	Internet of Remote Things	SDR	Software Defined Radio
IoT	Internet of Things	SEU	Single Event Upset
IoV	Internet of Vehicles	SNR	Signal to Noise Ratio
ISAC	Integrated Sensing and Communication	SS	Spread Spectrum
ISL	Inter-satellite Link	SSA	Space Situational Awareness
ISRO	Indian Space Research Organisation	SU	Secondary User
ITU	International Telecommunications Union	TIRA	Tracking and Imaging Radar
kg	kilogram	THz	Terahertz
km	kilometer	TMR	Triple Module Redundancy
LEO	Low Earth Orbit	TPC	Transmit Precoding
LFDA	Linear Frequency Diverse Array	TT&C	Telemetry, Tracking, and Command
LMB	Labeled Multi-Bernoulli	UAV	Unmanned Aerial Vehicle
LMS	Least Mean Square	WLAN	Wireless Local Area Networks

[28] H. Guo, J. Li, J. Liu *et al.*, "A survey on space-air-ground-sea integrated network security in 6G," *IEEE Commun. Surveys Tuts.*, vol. 24, no. 1, pp. 53–87, First Quart. 2022.

[29] H. Xie, Y. Zhan, G. Zeng *et al.*, "LEO mega-constellations for 6G global coverage: Challenges and opportunities," *IEEE Access*, vol. 9, pp. 164 223–164 244, Dec. 2021.

[30] Y. Wang, Z. Su, J. Ni *et al.*, "Blockchain-empowered space-air-ground integrated networks: Opportunities, challenges, and solutions," *IEEE Commun. Surveys Tuts.*, vol. 24, no. 1, pp. 160–209, First Quart. 2022.

[31] M. Xu, D. Niyato, Z. Xiong *et al.*, "Quantum-secured space-air-ground integrated networks: Concept, framework, and case study," *IEEE Wireless Commun.*, Oct. 2022, doi:10.1109/MWC.008.2200163.

[32] D. Zhou, M. Sheng, J. Li *et al.*, "Aerospace integrated networks innovation for empowering 6G: A survey and future challenges," *IEEE Commun. Surveys Tuts.*, vol. 25, no. 2, pp. 975–1019, Second Quart. 2023.

[33] X. Lu, L. Xiao, P. Li *et al.*, "Reinforcement learning-based physical cross-layer security and privacy in 6G," *IEEE Commun. Surveys Tuts.*, vol. 25, no. 1, pp. 425–466, First Quart. 2023.

[34] M. Strohmeier, D. Moser, M. Schafer *et al.*, "On the applicability of satellite-based air traffic control communication for security," *IEEE Commun. Mag.*, vol. 57, no. 9, pp. 79–85, Sep. 2019.

[35] C. Hao, X. Wan, D. Feng *et al.*, "Satellite-based radio spectrum monitoring: Architecture, applications, and challenges," *IEEE Netw.*, vol. 35, no. 4, pp. 20–27, Aug. 2021.

[36] M. Centenaro, C. E. Costa, F. Granelli *et al.*, "A survey on technologies, standards and open challenges in satellite IoT," *IEEE Commun. Surveys Tuts.*, vol. 23, no. 3, pp. 1693–1720, Third Quart. 2021.

[37] M. Vaezi, A. Azari, S. R. Khosravirad *et al.*, "Cellular, wide-area, and non-terrestrial IoT: A survey on 5G advances and the road towards 6G," *IEEE Commun. Surveys Tuts.*, vol. 24, no. 2, pp. 1117–1174, Second Quart. 2022.

[38] H. Al-Hraishawi, H. Chougrani, S. Kisseleff *et al.*, "A survey on non-geostationary satellite systems: The communication perspective," *IEEE Commun. Surveys Tuts.*, vol. 25, no. 1, pp. 101–132, First Quart. 2023.

[39] M. Manulis, C. P. Bridges, R. Harrison *et al.*, "Cyber security in new space: Analysis of threats, key enabling technologies and challenges," *International Journal of Information Security*, no. 3, May 2020.

[40] P. Tedeschi, S. Sciancalepore, and R. Di Pietro, "Satellite-based communications security: A survey of threats, solutions, and research challenges," *Computer Networks*, vol. 216, p. 109246, Oct. 2022.

[41] M. Höyhtyä, S. Boumard, A. Yastrebova *et al.*, "Sustainable satellite communications in the 6G era: A European view for multilayer systems and space safety," *IEEE Access*, vol. 10, pp. 99 973–100 005, Sep. 2022.

[42] B. Shen, Y. Wu, J. An *et al.*, "Random access with massive MIMO-OTFS in LEO satellite communications," *IEEE J. Sel. Areas Commun.*,

vol. 40, no. 10, pp. 2865–2881, Aug. 2022.
[43] B. Al Homssi, A. Al-Hourani, K. Wang *et al.*, "Next generation mega satellite networks for access equality: Opportunities, challenges, and performance," *IEEE Commun. Mag.*, vol. 60, no. 4, pp. 18–24, Apr. 2022.
[44] Z. Tan, H. Qin, L. Cong *et al.*, "New method for positioning using Iridium satellite signals of opportunity," *IEEE Access*, vol. 7, pp. 83 412–83 423, Jun. 2019.
[45] F. J. Dietrich, P. Metzen, and P. Monte, "The Globalstar cellular satellite system," *IEEE Trans. Antennas Propagat.*, vol. 46, no. 6, pp. 935–942, Jun. 1998.
[46] R. Cochetti, *Low Earth Orbit (LEO) Mobile Satellite Communications Systems*. Wiley, Oct. 2014, pp. 119–156.
[47] Y. Henri, *The OneWeb Satellite System*. Cham: Springer International Publishing, Feb. 2020, pp. 1–10.
[48] L. Perino-Gallice, O. Masson, M. Bel *et al.*, "Batteries for satellites constellation, using lean manufacturing for space industry," in *Proc. European Space Power Conference*, Juan-les-Pins, France, Dec. 2019, pp. 1–6.
[49] M. Asad Ullah, K. Mikhaylov, and H. Alves, "Massive machine-type communication and satellite integration for remote areas," *IEEE Wireless Commun.*, Aug. 2021.
[50] T.38.811, "Study on new radio (NR) to support non-terrestrial network," Oct. 2020.
[51] T. 38.821, "Solutions for NR to support non-terrestrial networks (NTN)," Jan. 2020.
[52] T. 23.737, "Study on architecture aspects for using satellite access in 5G," Mar. 2021.
[53] T. 22.822, "Study on using satellite access in 5G," Aug. 2018.
[54] T. 23.737, "Study on architecture aspects for using satellite access in 5G," Jul. 2020.
[55] T. 28.808, "Study on management and orchestration aspects of integrated satellite components in a 5G network," Jan. 2021.
[56] T. 24.821, "Study on PLMN selection for satellite access," Feb. 2021.
[57] Q. Chen, W. Meng, S. Han *et al.*, "Service-oriented fair resource allocation and auction for civil aircrafts augmented space-air-ground integrated networks," *IEEE Trans. Veh. Technol.*, vol. 69, no. 11, pp. 13 658–13 672, Sep. 2020.
[58] B. Wang, Z. Chang, S. Li *et al.*, "An efficient and privacy-preserving blockchain-based authentication scheme for low earth orbit satellite assisted Internet of Things," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 58, no. 6, pp. 5153–5164, Jun. 2022.
[59] S. R. Pratt, R. A. Raines, C. E. Fossa *et al.*, "An operational and performance overview of the Iridium low earth orbit satellite system," *IEEE Commun. Surveys Tuts.*, vol. 2, no. 2, pp. 2–10, Second Quart. 1999.
[60] J. Huang and J. Cao, "Recent development of commercial satellite communications systems," *Artificial Intelligence in China*, pp. 531–536, Feb. 2020.
[61] P. Tedeschi, S. Sciancalepore, and R. Di Pietro, "Security in energy harvesting networks: A survey of current solutions and research challenges," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 4, pp. 2658–2693, Fourth Quart. 2020.
[62] D. Gómez-Casco, J. A. López-Salcedo, and G. Seco-Granados, "Optimal post-detection integration techniques for the reacquisition of weak GNSS signals," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 56, no. 3, pp. 2302–2311, Jun. 2020.
[63] Z. Gao, L. Zhang, R. Han *et al.*, "Reliability evaluation of Turbo decoders implemented on SRAM-FPGAs," in *Proc. IEEE 38th VLSI Test Symposium (VTS)*, San Diego, CA, USA, 05-08 Apr. 2020, pp. 1–6.
[64] I. Ashraf, Y. Park, S. Hur *et al.*, "A survey on cyber security threats in IoT-enabled maritime industry," *IEEE Tran. Intell. Transp. Syst.*, vol. 24, no. 2, pp. 2677–2690, Feb. 2023.
[65] D. P. Moya Osorio, I. Ahmad, J. D. V. Sánchez *et al.*, "Towards 6G-enabled Internet of Vehicles: Security and privacy," *IEEE Open J. Commun. Soc.*, vol. 3, pp. 82–105, Jan. 2022.
[66] B. Jiang, Y. Yan, L. You *et al.*, "Robust secure transmission for satellite communications," *IEEE Trans. Aerosp. Electron. Syst.*, 2022.
[67] Z. Xiang, W. Yang, G. Pan *et al.*, "Physical layer security in cognitive radio inspired NOMA network," *IEEE J. Sel. Top. Signal Process.*, Feb. 2019.
[68] J. Wang, C. Jiang, and L. Kuang, "Turbo iterative DSSS acquisition in satellite high-mobility communications," *IEEE Trans. Veh. Technol.*, vol. 70, no. 12, pp. 12 998–13 009, Dec. 2021.
[69] P. Gu, R. Li, C. Hua *et al.*, "Cooperative spectrum sharing in a co-existing LEO-GEO satellite system," in *Proc. IEEE Globecom Workshops*, Taipei, Taiwan, 7-11 Dec. 2020, pp. 1–6.
[70] G. Schroder and M. Hashem Sherif, "The road to G.729: ITU 8-kb/s speech coding algorithm with wireline quality," *IEEE Communi. Mag.*, vol. 35, no. 9, pp. 48–54, Sep. 1997.
[71] Y. Zou, J. Zhu, X. Li *et al.*, "Relay selection for wireless communications against eavesdropping: A security-reliability trade-off perspective," *IEEE Netw.*, vol. 30, no. 5, pp. 74–79, Sep. 2016.
[72] J. Wang, C. Jiang, H. Zhang *et al.*, "Thirty years of machine learning: The road to Pareto-Optimal wireless networks," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 3, pp. 1472–1514, Third Quart. 2020.
[73] Y.-S. Shiu, S. Y. Chang, H.-C. Wu *et al.*, "Physical layer security in wireless networks: A tutorial," *IEEE Wireless Commun.*, vol. 18, no. 2, pp. 66–74, Apr. 2011.
[74] J. Pavur and I. Martinovic, "SOK: Building a launchpad for impactful satellite cyber-security research," Oct. 2020. [Online]. Available: https://arxiv.org/abs/2010.10872
[75] F. Dong, W. Wang, X. Li *et al.*, "Joint beamforming design for dual-functional MIMO radar and communication systems guaranteeing physical layer security," *IEEE Trans. Green Commun. Netw.*, vol. 7, no. 1, pp. 537–549, Mar. 2023.
[76] Z. Lu and Y. Jiao, "Efficiently all-digital code tracking for band-limited DSSS systems," *IEEE Commun. Lett.*, vol. 27, no. 2, pp. 686–690, Feb. 2023.
[77] F. Wang, W. Cui, and J. Tian, "A super-resolution multipath estimation algorithm for DSSS systems," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 59, no. 1, pp. 109–124, Feb. 2023.
[78] L. Cassano, S. D. Mascio, A. Palumbo *et al.*, "Is RISC-V ready for space? a security perspective," in *2022 IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT)*, Austin, TX, USA, 19-21 Oct. 2022, pp. 1–6.
[79] Y. Su, Y. Liu, Y. Zhou *et al.*, "Broadband LEO satellite communications: Architectures and key technologies," *IEEE Wireless Commun.*, vol. 26, no. 2, pp. 55–61, Apr. 2019.
[80] X. Zhu, C. Jiang, L. Kuang *et al.*, "Non-orthogonal multiple access based integrated terrestrial-satellite networks," *IEEE J. Sel. Areas Commun.*, vol. 35, no. 10, pp. 2253–2267, Oct. 2017.
[81] J. Pavur, D. Moser, V. Lenders *et al.*, "Secrets in the sky: On privacy and infrastructure security in DVB-S satellite broadband," in *Proc. Conference on Security and Privacy in Wireless and Mobile Networks*, Miami, FL, USA, May 2019, pp. 277–284.
[82] R. Wang, S. Zhang, B. Yang *et al.*, "Enabling data sharing through data trusts in LEO satellite internet," *IEEE Wireless Commun.*, Jan. 2023, doi:10.1109/MWC.013.2200233.
[83] Y. Zuo, M. Yue, M. Zhang *et al.*, "OFDM-based massive connectivity for LEO satellite internet of things," *IEEE Trans. Wireless Commun.*, Mar. 2023, doi:10.1109/TWC.2023.3261362.
[84] Z. Yin, N. Cheng, Y. Hui *et al.*, "Multi-domain resource multiplexing based secure transmission for satellite-assisted IoT: AO-SCA approach," *IEEE Trans. Wireless Commun.*, Mar. 2023, doi:10.1109/TWC.2023.3250227.
[85] P. K. Chowdhury, M. Atiquzzaman, and W. Ivancic, "Handover schemes in satellite networks: state-of-the-art and future research directions," *IEEE Commun. Surv. Tutor.*, vol. 8, no. 4, pp. 2–14, Fourth Quart. 2006.
[86] H. Cui, J. Zhang, Y. Geng *et al.*, "Space-air-ground integrated network (SAGIN) for 6G: Requirements, architecture and challenges," *China Commun.*, vol. 19, no. 2, pp. 90–108, Feb. 2022.
[87] C. Chen, Z. Jiang, and J. Ma, "Privacy protection for marginal-sensitive community individuals against adversarial community detection attacks," *IEEE Trans. Comput. Social Syst.*, Dec. 2022, doi:10.1109/TCSS.2022.3229162.
[88] M. Zadsar, A. Abazari, A. Ameli, J. Yan, and M. Ghafouri, "Prevention and detection of coordinated false data injection attacks on integrated power and gas systems," *IEEE Trans. Power Syst.*, Oct. 2022, doi:10.1109/TPWRS.2022.3216118.
[89] J. E. Varghese and B. Muniyal, "An efficient ids framework for DDoS attacks in SDN environment," *IEEE Access*, vol. 9, pp. 69 680–69 699, May 2021.
[90] H. Pirayesh and H. Zeng, "Jamming attacks and anti-jamming strategies in wireless networks: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 24, no. 2, pp. 767–809, Second Quart. 2022.
[91] H. Cao, L. Wu, Y. Chen *et al.*, "Analysis on the security of satellite internet," in *China Cyber Security Annual Conference*, Beijing, China, Dec. 2020, pp. 193–205.

[92] Y. Zou, J. Zhu, X. Wang *et al.*, "A survey on wireless security: Technical challenges, recent advances, and future trends," *Proc. IEEE*, vol. 104, no. 9, pp. 1727–1765, Sep. 2016.

[93] K. Mayyas, "Performance analysis of the deficient length LMS adaptive algorithm," *IEEE Trans. Signal Process.*, vol. 53, no. 8, pp. 2727–2734, Aug. 2005.

[94] R. Merched and A. Sayed, "An embedding approach to frequency-domain and subband adaptive filtering," *IEEE Trans. Signal Process.*, vol. 48, no. 9, pp. 2607–2619, Sep. 2000.

[95] D. He, S. Chan, and M. Guizani, "Communication security of unmanned aerial vehicles," *IEEE Wireless Commun.*, vol. 24, no. 4, pp. 134–139, Aug. 2017.

[96] S. A. Chaudhry, A. Irshad, M. A. Khan *et al.*, "A lightweight authentication scheme for 6G-IoT enabled maritime transport system," *IEEE Trans. Intell. Transp. Syst.*, vol. 24, no. 2, pp. 2401–2410, Feb. 2023.

[97] A. S. Abdalla, K. Powell, V. Marojevic *et al.*, "UAV-assisted attack prevention, detection, and recovery of 5G networks," *IEEE Wireless Commun.*, vol. 27, no. 4, pp. 40–47, Aug. 2020.

[98] P. Bhale, D. R. Chowdhury, S. Biswas *et al.*, "OPTIMIST: Lightweight and transparent IDS with optimum placement strategy to mitigate mixed-rate DDoS attacks in IoT networks," *IEEE Internet Things J.*, vol. 10, no. 10, pp. 8357–8370, May 2023.

[99] G. Cluley. Could this be the world's most harmless IoT botnet? (May 08, 2020). [Online]. Available: https://www.bitdefender.com/blog/hotforsecurity/worlds-harmless-iot-botnet

[100] J. A. Ruiz de Azúa, A. Calveras, and A. Camps, "Internet of satellites (IoSat): Analysis of network models and routing protocol requirements," *IEEE Access*, vol. 6, pp. 20 390–20 411, Apr. 2018.

[101] R. F. Hayat, S. Aurangzeb, M. Aleem *et al.*, "ML-DDoS: A blockchain-based multilevel DDoS mitigation mechanism for IoT environments," *IEEE Trans. Eng. Manag.*, May 2022, doi:10.1109/TEM.2022.3170519.

[102] A. Roy-Chowdhury, J. S. Baras, M. Hadjitheodosiou *et al.*, "Security issues in hybrid networks with a satellite component," *IEEE Wireless Commun.*, vol. 12, no. 6, pp. 50–61, Dec. 2005.

[103] E. Shi and A. Perrig, "Designing secure sensor networks," *IEEE Wireless Commun.*, vol. 11, no. 6, pp. 38–43, Dec. 2004.

[104] G. Barseghyan, Y. Yuan, and M. Anakpa, "Model for detection of masquerade attacks based on variable-length sequences," *IEEE Access*, vol. 8, pp. 210 140–210 157, Nov. 2020.

[105] Y. Zou, J. Zhu, L. Yang *et al.*, "Securing physical-layer communications for cognitive radio networks," *IEEE Commun. Mag.*, vol. 53, no. 9, pp. 48–54, Sep. 2015.

[106] L. H. Newman. Hackers are building an army of cheap satellite trackers. (Aug. 04, 2020). [Online]. Available: https://www.wired.com/story/nyansat-open-source-satellite-tracker/

[107] X. Chen, K. Makki, K. Yen *et al.*, "Sensor network security: A survey," *IEEE Commun. Surveys Tuts.*, vol. 11, no. 2, pp. 52–73, Second Quart. 2009.

[108] R. Radhakrishnan, W. W. Edmonson, F. Afghah *et al.*, "Survey of inter-satellite communication for small satellite systems: Physical layer to network layer view," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 4, pp. 2442–2473, Fourth Quart. 2016.

[109] J. P. Choi and C. Joo, "Challenges for efficient and seamless space-terrestrial heterogeneous networks," *IEEE Commun. Mag.*, vol. 53, no. 5, pp. 156–162, May 2015.

[110] H. Chen, Y. Xiao, J. Li *et al.*, "The OCC-CDMA/OS for 4G wireless," *IEEE Veh. Technol. Mag.*, vol. 1, no. 3, pp. 12–21, Sep. 2006.

[111] H. Chen, D. Hank, M. E. Maganaz *et al.*, "Design of next-generation CDMA using orthogonal complementary codes and offset stacked spreading," *IEEE Wireless Commun.*, vol. 14, no. 3, pp. 61–69, Jul. 2007.

[112] J. Li, A. Huang, M. Guizani *et al.*, "Inter-group complementary codes for interference-resistant CDMA wireless communications," *IEEE Trans. Wireless Commun.*, vol. 7, no. 1, pp. 166–174, Jan. 2008.

[113] Y. Couble, C. Rosenberg, E. Chaput, J.-B. Dupé, C. Baudoin, and A.-L. Beylot, "Two-color scheme for a multi-beam satellite return link: Impact of interference coordination," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 5, pp. 993–1003, May 2018.

[114] J. Ye, G. Pan, and M. S. Alouini, "Earth rotation-aware non-stationary satellite communication systems: Modeling and analysis," *IEEE Trans. Wireless Commun.*, vol. 20, no. 9, pp. 5942–5956, Apr. 2021.

[115] S. Chen, Y. C. Liang, S. Sun *et al.*, "Vision, requirements, and technology trend of 6G: How to tackle the challenges of system coverage, capacity, user data-rate and movement speed," *IEEE Wireless Commun.*, vol. 27, no. 2, pp. 218–228, Apr. 2020.

[116] M. Jia, Z. Li, X. Gu, and Q. Guo, "Joint multi-beam power control for LEO and GEO spectrum-sharing networks," in *Proc. IEEE Int. Conf. Comm.*, Xiamen, China, Jul. 2021, pp. 841–846.

[117] E. Lagunas, S. Maleki, S. Chatzinotas *et al.*, "Power and rate allocation in cognitive satellite uplink networks," in *Proc. IEEE Int. Conf. Comm.*, Kuala Lumpur, Malaysia, May 2016, pp. 1–6.

[118] X. Lin, S. Cioni, G. Charbit *et al.*, "On the path to 6G: Embracing the next wave of low earth orbit satellite access," *IEEE Commun. Mag.*, vol. 59, no. 12, pp. 36–42, Dec. 2021.

[119] V. Vargas, P. Ramos, R. Velazco *et al.*, "Evaluating SEU fault-injection on parallel applications implemented on multicore processors," in *Proc. Latin American Symposium on Circuits Systems*, Montevideo, Uruguay, Feb. 2015, pp. 1–4.

[120] G. Quaglione and M. Giovannoni, "Orbital inclination effects on communications satellite system design," *IEEE Trans. Aerosp. Electron. Syst.*, vol. AES-19, no. 3, pp. 447–453, May 1983.

[121] F. Zhang, G. Guo, Y. Qin *et al.*, "Prediction of proton-induced single event effect on SRAM's in-orbit soft error rate on typical satellite orbit," *Spacecraft Environment Engineering*, vol. 35, no. 4, pp. 365–370, Aug. 2018.

[122] Union of Concerned Scientists. UCS Satellite Database. (Jan. 31, 2023). [Online]. Available: https://www.ucsusa.org/resources/satellite-database

[123] D. M. Lear. STS-118 Radiator Impact Damage. (Jan. 1, 2008). [Online]. Available: https://ntrs.nasa.gov/citations/20080010742

[124] L. David. Effects of worst satellite breakups in history still felt today. (Jan. 28, 2013). [Online]. Available: https://www.space.com/19450-space-junk-worst-events-anniversaries.html

[125] K. Tate. Russian satellite crash with Chinese ASAT debris explained. (Mar. 9, 2013). [Online]. Available: https://www.space.com/20145-russian-satellite-chinese-debris-crash-infographic.html

[126] Accessed: Apr. 18, 2022. [Online]. Available: https://www.wikiwand.com/en/Satellite_collision

[127] Accessed: Apr. 18, 2022. [Online]. Available: https://www.iol.co.za/news/ecuador-satellite-hits-soviet-era-space-junk-1521111

[128] L. David. Copernicus Sentinel-1A satellite hit by space particle. (Aug. 31, 2016). [Online]. Available: https://www.space.com/33920-european-satellite-space-particle-strike.html

[129] M. Kramer. A piece of space junk chipped one of the Space Station's huge windows. (May. 12, 2016). [Online]. Available: https://www.space.com/20145-russian-satellite-chinese-debris-crash-infographic.html

[130] J. Foust. ESA spacecraft dodges potential collision with starlink satellite. (Sep. 2, 2019). [Online]. Available: https://spacenews.com/esa-spacecraft-dodges-potential-collision-with-starlink-satellite/

[131] Accessed: Dec. 28, 2021. [Online]. Available: https://www.unoosa.org/oosa/en/oosadoc/data/documents/2021/aac.105/aac.1051262_0.html

[132] Accessed: Apr. 18, 2022. [Online]. Available: https://directory.eoportal.org/web/eoportal/satellite-missions/k/kompsat-1

[133] E. Howell. Space station robotic arm hit by orbital debris in 'lucky strike'. (May 31, 2021). [Online]. Available: https://www.space.com/space-station-robot-arm-orbital-debris-strike

[134] Accessed: Dec. 28, 2021. [Online]. Available: https://www.esa.int/Safety_Security/Space_Debris/Space_debris_by_the_numbers

[135] J. Drmola and T. Hubik, "Kessler syndrome: System dynamics model," *Space Policy*, vol. 44-45, pp. 29–39, Aug. 2018.

[136] Accessed: Dec. 28, 2021. [Online]. Available: https://www.esa.int/ESA_Multimedia/Images/2009/05/ESA_built-solar_cells_retrieved_from_the_Hubble_Space_Telescope_in_2002

[137] Accessed: Apr. 18, 2022. [Online]. Available: https://timesofindia.indiatimes.com/india.html

[138] Space debris and human spacecraft. (May 26, 2021). [Online]. Available: https://www.nasa.gov/mission_pages/station/news/orbital_debris.html

[139] B. Li, J. Huang, Y. Feng *et al.*, "A machine learning-based approach for improved orbit predictions of LEO space debris with sparse tracking data from a single station," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 56, no. 6, pp. 4253–4268, Dec. 2020.

[140] M. Maffei, A. Aubry, A. De Maio *et al.*, "An ontology for spaceborne radar debris detection and tracking: Channel-target phenomenology and motion models," *IEEE Aerosp. Electron. Syst. Mag.*, vol. 36, no. 6, pp. 18–42, Jun. 2021.

[141] D. F. Crouse, "On measurement-based light-time corrections for bistatic orbital debris tracking," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 51, no. 3, pp. 2502–2518, Jul. 2015.

[142] X. Bai, M. Xing, F. Zhou *et al.*, "High-resolution three-dimensional imaging of spinning space debris," *IEEE Trans. Geosci. Remote Sens.*, vol. 47, no. 7, pp. 2352–2362, Jul. 2009.

[143] M. Maffei, A. Aubry, A. De Maio *et al.*, "Spaceborne radar sensor architecture for debris detection and tracking," *IEEE Trans. Geosci. Remote Sens.*, vol. 59, no. 8, pp. 6621–6636, Aug. 2021.

[144] Z. Wei, T. Long, R. Shi *et al.*, "Scheduling optimization of multiple hybrid-propulsive spacecraft for geostationary space debris removal missions," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 58, no. 3, pp. 2304–2326, Jun. 2022.

[145] V. Hassija, V. Chamola, A. Agrawal *et al.*, "Fast, reliable, and secure drone communication: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 23, no. 4, pp. 2802–2832, Fourth Quart. 2021.

[146] J. Liu, W. Liu, W. U. Qianhong *et al.*, "Survey on key security technologies for space information networks," *J. Commun. Netw-S. KOR*, vol. 1, no. 1, p. 14, Apr. 2016.

[147] B. Yang, "Research on the strategy how to clean up space debris," in *Proc. International Conference on Education, Management and Computing Technology*, Hangzhou, China, Apr. 2016, pp. 1054–1057.

[148] T. Pratt and J. E. Allnutt, *Satellite communications*. John Wiley & Sons, 2019.

[149] F. Gao, B. Wang, C. Xing *et al.*, "Wideband beamforming for hybrid massive MIMO terahertz communications," *IEEE J. Sel. Areas Commun.*, vol. 39, no. 6, pp. 1725–1740, Jun. 2021.

[150] S. Otoum, N. Guizani, and H. Mouftah, "On the feasibility of split learning, transfer learning and federated learning for preserving security in ITS systems," *IEEE Trans. Intell. Transp. Syst.*, vol. 24, no. 7, pp. 7462–7470, Jul. 2023.

[151] J. Wang, C. Jiang, and L. Kuang, "Turbo iterative DSSS acquisition in satellite high-mobility communications," *IEEE Trans. Veh. Technol.*, vol. 70, no. 12, pp. 12 998–13 009, Dec. 2021.

[152] Y. Cao, Y. Zhao, Q. Wang *et al.*, "The evolution of quantum key distribution networks: On the road to the qinternet," *IEEE Commun. Surveys Tuts.*, vol. 24, no. 2, pp. 839–894, Second Quart. 2022.

[153] C. W.-Q. L. W.-Y. Liao, S.-K. *et al.*, "Satellite-to-ground quantum key distribution," *Nature*, vol. 549, p. 43–47, Aug. 2017.

[154] Y. Y. Juan, Y. Cao *et al.*, "Satellite-to-ground entanglement-based quantum key distribution," *Phys. Rev. Lett.*, vol. 119, p. 200501, Nov. 2017.

[155] H. J. S.K. Liao, W.Q. Cai *et al.*, "Satellite-relayed intercontinental quantum network," *Phys. Rev. Lett.*, vol. 120, p. 030501, Jan. 2018.

[156] G. Zhang, J. Y. Haw, H. Cai *et al.*, "An integrated silicon photonic chip platform for continuous-variable quantum key distribution," *Nat. Photonics*, vol. 13, no. 12, pp. 839–842, Dec. 2019.

[157] J.-P. Chen, C. Zhang, Y. Liu *et al.*, "Sending-or-not-sending with independent lasers: Secure twin-field quantum key distribution over 509 km," *Phys. Rev. Lett.*, vol. 124, p. 070501, Feb. 2020.

[158] T. A. Eriksson, R. S. Luis, B. J. Puttnam *et al.*, "Wavelength division multiplexing of 194 continuous variable quantum key distribution channels," *J. Lightwave Technol.*, vol. 38, no. 8, pp. 2214–2218, Apr 2020.

[159] R. Valivarthi, S. Etcheverry, J. Aldama *et al.*, "Plug-and-play continuous-variable quantum key distribution for metropolitan networks," *Opt. Express*, vol. 28, no. 10, pp. 14 547–14 559, May 2020.

[160] Y. Zhang, Z. Chen, S. Pirandola *et al.*, "Long-distance continuous-variable quantum key distribution over 202.81 km of fiber," *Phys. Rev. Lett.*, vol. 125, p. 010502, Jun. 2020.

[161] L. Y. L. S. Yin, J. *et al.*, "Entanglement-based secure quantum cryptography over 1120 kilometres," *Nature*, vol. 582, p. 501–505, Jun. 2020.

[162] Z. Q. C. T. Chen, YA. *et al.*, "An integrated space-to-ground quantum communication network over 4600 kilometres," *Nature*, vol. 589, p. 214–219, Jan. 2021.

[163] N. Hosseinidehaj, Z. Babar, R. Malaney *et al.*, "Satellite-based continuous-variable quantum communications: State-of-the-art and a predictive outlook," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 1, pp. 881–919, First Quart. 2019.

[164] G.-L. Long and X.-S. Liu, "Theoretically efficient high-capacity quantum-key-distribution scheme," *Physical Review A*, vol. 65, no. 3, p. 032302, Feb. 2002.

[165] F.-G. Deng, G. L. Long, and X.-S. Liu, "Two-step quantum direct communication protocol using the Einstein-Podolsky-Rosen pair block," *Physical Review A*, vol. 68, no. 4, p. 042317, Oct. 2003.

[166] F.-G. Deng and G. L. Long, "Secure direct communication with a quantum one-time pad," *Physical Review A*, vol. 69, no. 5, p. 052319, May 2004.

[167] F. Yan and X. Zhang, "A scheme for secure direct communication using EPR pairs and teleportation," *The European Physical Journal B-Condensed Matter and Complex Systems*, vol. 41, no. 1, pp. 75–78, Sep. 2004.

[168] C. Wang, F.-G. Deng, Y.-S. Li *et al.*, "Quantum secure direct communication with high-dimension quantum superdense coding," *Physical Review A*, vol. 71, p. 044305, Apr. 2005.

[169] Z. Zhou, Y. Sheng, P. Niu *et al.*, "Measurement-device-independent quantum secure direct communication," *Science China Physics, Mechanics & Astronomy*, vol. 63, no. 3, pp. 1–6, Dec. 2019.

[170] A. Huang, S. Barz, E. Andersson *et al.*, "Implementation vulnerabilities in general quantum cryptography," *New Journal of Physics*, vol. 20, no. 10, p. 103016, Oct. 2018.

[171] D. Chandra, A. S. Cacciapuoti, M. Caleffi *et al.*, "Direct quantum communications in the presence of realistic noisy entanglement," *IEEE Trans. Commun.*, vol. 70, no. 1, pp. 469–484, Jan. 2022.

[172] Z. Sun, L. Song, Q. Huang *et al.*, "Toward practical quantum secure direct communication: A quantum-memory-free protocol and code design," *IEEE Trans. Commun.*, vol. 68, no. 9, pp. 5778–5792, Jul. 2020.

[173] Y. Cao, Y. Zhao, J. Zhang *et al.*, "Software-defined heterogeneous quantum key distribution chaining: An enabler for multi-protocol quantum networks," *IEEE Commun. Mag.*, vol. 60, no. 9, pp. 38–44, Aug. 2022.

[174] Z. Zhou, Y. Tian, J. Xiong *et al.*, "Blockchain-enabled secure and trusted federated data sharing in IIoT," *IEEE Trans. Industr. Inform.*, vol. 19, no. 5, pp. 6669–6681, May 2023.

[175] R. Han, L. Bai, J. Liu *et al.*, "Blockchain-based GNSS spoofing detection for multiple UAV systems," *J. Commun. Netw.*, vol. 4, no. 2, pp. 81–88, Jun. 2019.

[176] Y. Chen, L. Wang, and S. Wang, "Stochastic blockchain for IoT data integrity," *IEEE Trans. Netw. Sci. Eng.*, vol. 7, no. 1, pp. 373–384, Mar. 2020.

[177] P. Yuan, B. Li, Y. Zhang *et al.*, "A PUF-based lightweight broadcast authentication protocol for multi-server systems using blockchain," in *Proc. IEEE 6th International Conference on Signal and Image Processing*, Nanjing, China, 22-24 Oct. 2021, pp. 1035–1041.

[178] G. Spathoulas, N. Giachoudis, G.-P. Damiris *et al.*, "Collaborative blockchain-based detection of distributed denial of service attacks based on internet of things botnets," *Future Internet*, vol. 11, no. 11, p. 226, Oct. 2019.

[179] A. Kumar and A. R. Pais, "Blockchain based en-route filtering of false data in wireless sensor networks," in *Proc. International Conference on Communication Systems Networks*, Bengaluru, India, 7-9 Jan. 2019, pp. 1–6.

[180] I. A. Hemadeh, K. Satyanarayana, M. El-Hajjar *et al.*, "Millimeter-wave communications: Physical channel models, design considerations, antenna constructions, and link-budget," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 2, pp. 870–913, Second Quart. 2018.

[181] S. Xia, Q. Jiang, C. Zou *et al.*, "Beam coverage comparison of LEO satellite systems based on user diversification," *IEEE Access*, vol. 7, pp. 181 656–181 667, Dec. 2019.

[182] T. Duan and V. Dinavahi, "Starlink space network-enhanced cyber–physical power system," *IEEE Trans. Smart. Grid.*, vol. 12, no. 4, pp. 3673–3675, Mar. 2021.

[183] D. DiSanto, T. Shirley, and R. Shimon, "Technology options for mm-wave test and measurement equipment," in *Proc. IEEE Compound Semiconductor Integrated Circuit Symposium*, Miami, FL, USA, Oct. 2017, pp. 1–6.

[184] H. Ding and K. G. Shin, "Context-aware beam tracking for 5G mmwave V2I communications," *IEEE Trans. Mobile Comput.*, vol. 22, no. 6, pp. 3257–3269, Jun. 2023.

[185] Z. Song, J. An, H. Ding *et al.*, "Optimal relay probing for UAV millimeter wave communications with beam training overhead," *IEEE Trans. Veh. Technol.*, vol. 72, no. 6, pp. 7351–7363, Jun. 2023.

[186] Q. Xia and J. M. Jornet, "Multi-hop relaying distribution strategies for terahertz-band communication networks: A cross-layer analysis," *IEEE Trans. Wireless Commun.*, vol. 21, no. 7, pp. 5075–5089, Jul. 2022.

[187] S. Nie and I. F. Akyildiz, "Channel modeling and analysis of inter-small-satellite links in Terahertz band space networks," *IEEE Trans. Commun.*, vol. 69, no. 12, pp. 8585–8599, Dec. 2021.

[188] K. Tekbiyik, A. R. Ekti, G. K. Kurt *et al.*, "A holistic investigation of terahertz propagation and channel modeling toward vertical heterogeneous networks," *IEEE Commun. Mag.*, vol. 58, no. 11, pp. 14–20, Nov. 2020.

[189] J. N. Pelton, S. Madry, and S. Camacho-Lara, *New Millimeter, Terahertz, and Light-Wave Frequencies for Satellite Communications*. Springer International Publishing, Jan. 2017.

[190] Q. Wu, C. Lin, B. Lu *et al.*, "A 21 km 5 Gbps real time wireless communication system at 0.14 THz," in *Proc. International Conference on Infrared, Millimeter, and Terahertz Waves*, Cancun, Mexico, Sep. 2017, pp. 1–2.

[191] H. Kaushal and G. Kaddoum, "Optical communication in space: Challenges and mitigation techniques," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 1, pp. 57–96, First Quart. 2017.

[192] M. Toyoshima, "Trends in satellite communications and the role of optical free-space communications," *Journal of Optical Networking*, vol. 4, no. 6, pp. 300–311, May 2005.

[193] A. U. Chaudhry and H. Yanikomeroglu, "Free space optics for next-generation satellite networks," *IEEE Consum. Electron. Mag.*, vol. 10, no. 6, pp. 21–31, Nov. 2021.

[194] Q. Chen, G. Giambene, L. Yang *et al.*, "Analysis of inter-satellite link paths for LEO mega-constellation networks," *IEEE Trans. Veh. Technol.*, vol. 70, no. 3, pp. 2743–2755, Mar. 2021.

[195] A. U. Chaudhry and H. Yanikomeroglu, "Laser intersatellite links in a starlink constellation: A classification and analysis," *IEEE Veh. Technol. Mag.*, vol. 16, no. 2, pp. 48–56, Apr. 2021.

[196] T. Tolker-Nielsen and G. Oppenhauser, "In-orbit test result of an operational optical intersatellite link between ARTEMIS and SPOT4, SILEX," in *Proc. Free-Space Laser Communication Technologies*, vol. 4635, San Jose, CA, USA, Apr. 2002, pp. 1–15.

[197] T. Jono, Y. Takayama, K. Shiratama *et al.*, "Overview of the inter-orbit and the orbit-to-ground laser communication demonstration by OICETS," in *Proc. Free-Space Laser Communication Technologies XIX and Atmospheric Propagation of Electromagnetic Waves*, vol. 6457, San Jose, CA, USA, Mar. 2007, pp. 9–18.

[198] M. Gregory, F. Heine, H. Kämpfner *et al.*, "TESAT laser communication terminal performance results on 5.6Gbit coherent inter satellite and satellite to ground links," in *Proc. International Conference on Space Optics*, E. Armandillo, B. Cugny, and N. Karafolas, Eds., vol. 10565, Rhodes Island, Greece, Nov. 2017, pp. 324–329.

[199] M. Toyoshima, T. Fuse, D. R. Kolev *et al.*, "Current status of research and development on space laser communications technologies and future plans in NICT," in *2015 IEEE International Conference on Space Optical Systems and Applications*, Oct. 2015, pp. 1–5.

[200] T. Wang, P. Lin, F. Dong *et al.*, "Progress and prospect of space laser communication technology," *Strategic Study of Chinese Academy of Engineering*, vol. 22, no. 3, pp. 92–99, May 2020.

[201] H. Zech, F. Heine, D. Tröndle *et al.*, "LCT for EDRS: LEO to GEO optical communications at 1.8 Gbps between Alphasat and Sentinel 1a," in *Proc. Advanced Free-Space Optical Communication Techniques and Applications*, vol. 9647, Toulouse, France, Oct. 2015, pp. 85–92.

[202] B. V. Oaida, M. J. Abrahamson, R. J. Witoff *et al.*, "OPALS: An optical communications technology demonstration from the international space station," in *Proc. IEEE Aerospace Conference*, Big Sky, MT, USA, May 2013, pp. 1–20.

[203] A. Carrasco-Casado, H. Takenaka, D. Kolev, *et al.*, "LEO-to-ground optical communications using sota (small optical transponder)–payload verification results and experiments on space quantum communications," *Acta Astronaut.*, vol. 139, pp. 377–384, Oct. 2017.

[204] W. Chen, L. Sun, i, K. Xie *et al.*, "5.12Gbps optical communication link between LEO satellite and ground station," in *Proc. IEEE International Conference on Space Optical Systems and Applications*, Naha, Japan, Nov. 2017, pp. 260–263.

[205] T. S. Rose, D. W. Rowen, S. LaLumondiere *et al.*, "Optical communications downlink from a 1.5U Cubesat: OCSD program," in *Proc. International Conference on Space Optics*, Z. Sodnik, N. Karafolas, and B. Cugny, Eds., vol. 11180, Chania, Greece, Jul. 2019, pp. 201–212.

[206] H. Takenaka, A. Carrasco-Casado, M. Fujiwara *et al.*, "Satellite-to-ground quantum-limited communication using a 50-kg-class microsatellite," *Nature photonics*, vol. 11, no. 8, pp. 502–508, Aug. 2017.

[207] R. Zhang, W. Zhang, X. Zhang *et al.*, "Research status and development trend of high earth orbit satellite laser relay links," *Laser Optoelectronics Progress*, vol. 58, no. 5, pp. 1–13, Mar. 2021.

[208] D. Calzolaio, F. Curreli, J. Duncan *et al.*, "EDRS-C – the second node of the european data relay system is in orbit," *Acta Astronaut.*, vol. 177, pp. 537–544, Dec. 2020.

[209] C. Xu, Y. Jin, L. Li *et al.*, "Wireless transmission technology of satellite-terrestrial integration for 6G mobile communication," *Journal of Electronics Information Technology*, vol. 43, no. 1, pp. 28–36, Jan. 2021.

[210] A. Carrasco-Casado, P. X. Do, D. Kolev *et al.*, "Intersatellite-link demonstration mission between CubeSOTA (LEO CubeSat) and ETS9-HICALI (GEO Satellite)," in *Proc. IEEE International Conference on Space Optical Systems and Applications*, Portland, OR, USA, Oct. 2019, pp. 1–5.

[211] H. Hauschildt, N. le Gallou, S. Mezzasoma *et al.*, "Global quasi-real-time-services back to Europe: EDRS Global," in *Proc. International Conference on Space Optics*, vol. 11180, Chania, Greece, Oct. 2018, pp. 353–357.

[212] H. Hauschildt, C. Elia, A. Jones *et al.*, "ESAs ScyLight programme: Activities and status of the high throughput optical network" HydRON"," in *Proc. International Conference on Space Optics*, vol. 11180, Chania, Greece, Oct. 2018, pp. 1–8.

[213] X. Li, J. Ma, S. Yu *et al.*, "Investigation of optical intensity fluctuation in the presence of satellite vibration for intersatellite optical communications," in *Proc. International Conference on Computer Science and Network Technology*, vol. 1, Harbin, China, Dec. 2011, pp. 65–67.

[214] Q. Yang, L. Tan, and J. Ma, "Doppler characterization of laser inter-satellite links for optical LEO satellite constellations," *Opt. Commun.*, vol. 282, no. 17, pp. 3547–3552, Sep. 2009.

[215] Z. Li, "A machine learning solution for satellite health and safety monitoring," *J. Space Oper. Commun.*, vol. 18, no. 1, Jan. 2022.

[216] Z. Na, Z. Pan, X. Liu *et al.*, "Distributed routing strategy based on machine learning for LEO satellite network," *Wirel. Commun. Mob. Comput.*, vol. 2018, Jul. 2018.

[217] Y. Bie, L. Wang, Y. Tian *et al.*, "A combined forecasting model for satellite network self-similar traffic," *IEEE Access*, vol. 7, pp. 152 004–152 013, Oct. 2019.

[218] C. Han, A. Liu, L. Huo *et al.*, "A prediction-based resource matching scheme for rentable LEO satellite communication network," *IEEE Commun. Lett.*, vol. 24, no. 2, pp. 414–417, Nov. 2019.

[219] H. Jia, C. Jiang, L. Kuang *et al.*, "Adaptive access control and resource allocation for random access in NGSO satellite networks," *IEEE Trans. Netw. Sci. Eng.*, vol. 9, no. 4, pp. 2721–2733, Jul.-Aug. 2022.

[220] N. Li, L. Hu, Z.-L. Deng *et al.*, "Research on GRU neural network satellite traffic prediction based on transfer learning," *Wirel. Pers. Commun.*, vol. 118, no. 1, pp. 815–827, Jan. 2021.

[221] S. Fuertes, G. Picart, J.-Y. Tourneret *et al.*, "Improving spacecraft health monitoring with automatic anomaly detection techniques," in *14th international conference on space operations*, Daejeon, Korea, 16-20 May 2016, p. 2430.

[222] T. Yairi, N. Takeishi, T. Oda *et al.*, "A data-driven health monitoring method for satellite housekeeping data based on probabilistic clustering and dimensionality reduction," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 53, no. 3, pp. 1384–1401, Jun. 2017.

[223] Y. Wang, J. Gong, J. Zhang *et al.*, "A deep learning anomaly detection framework for satellite telemetry with fake anomalies," *Int. J. Aerosp. Eng.*, vol. 2022, Jan. 2022, doi:10.1155/2022/1676933.

[224] K. Hundman, V. Constantinou, C. Laporte *et al.*, "Detecting spacecraft anomalies using LSTMs and nonparametric dynamic thresholding," in *Proceedings of the 24th ACM SIGKDD international conference on knowledge discovery & data mining*, Jul. 2018, pp. 387–395.

[225] S. Tariq, S. Lee, Y. Shin *et al.*, "Detecting anomalies in space using multivariate convolutional LSTM with mixtures of probabilistic PCA," in *Proceedings of the 25th ACM SIGKDD international conference on knowledge discovery & data mining*, Jul. 2019, pp. 2123–2133.

[226] Z. Zeng, G. Jin, C. Xu *et al.*, "Satellite telemetry data anomaly detection using causal network and feature-attention-based LSTM," *IEEE Trans. Instrum. Meas.*, vol. 71, pp. 1–21, Feb. 2022.

[227] S. K. Ibrahim, A. Ahmed, M. A. E. Zeidan, and I. E. Ziedan, "Machine learning methods for spacecraft telemetry mining," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 55, no. 4, pp. 1816–1827, Jul. 2018.

[228] Y. Wang, Y. Wu, Q. Yang, and J. Zhang, "Anomaly detection of spacecraft telemetry data using temporal convolution network," in *2021 IEEE International Instrumentation and Measurement Technology Conference (I2MTC)*. Glasgow, United Kingdom: IEEE, 17-20 May 2021, pp. 1–5.

[229] N. Moustafa, I. A. Khan, M. Hassanin *et al.*, "DFSat: Deep federated learning for identifying cyber threats in IoT-based satellite networks," *IEEE Trans. Industr. Inform.*, Oct. 2022, doi:10.1109/TII.2022.3214652.

[230] H. Li, J. He, X. Wang, and H. Yang, "Research review and prospect of fault diagnosis method of satellite power system based on machine learning," *DEStech Trans. Comput. Sci. Eng*, 03 2019.

[231] J. Dong, Y. Ma, and D. Liu, "Deep learning based multiple sensors monitoring and abnormal discovery for satellite power system," in *2019 International Conference on Sensing, Diagnostics, Prognostics,*

and Control (SDPC). Beijing, China: IEEE, 15-17 Aug 2019, pp. 638–643.

[232] F. Cheng, X. Guo, Y. Qi *et al.*, "Research on satellite power anomaly detection method based on LSTM," in *2021 IEEE International Conference on Power Electronics, Computer Applications (ICPECA)*. Shenyang, China: IEEE, 22-24 Jan. 2021, pp. 706–710.

[233] G. Zhang, J. Zhou, F. Han *et al.*, "Data-based anomaly detection model for solar array power of in-orbit satellites," in *2016 Prognostics and System Health Management Conference (PHM-Chengdu)*, Chengdu, China, 19-21 Oct. 2016, pp. 1–5.

[234] N. Coulter and H. Moncayo, "An online machine learning paradigm for spacecraft fault detection," in *AIAA Scitech 2021 Forum*, Jan. 2021, p. 1339.

[235] L. Gunn, P. Smet, E. Arbon *et al.*, "Anomaly detection in satellite communications systems using LSTM networks," in *2018 Military Communications and Information Systems Conference (MilCIS)*. Canberra, ACT, Australia: IEEE, 13-15 Nov. 2018, pp. 1–6.

[236] P. Henarejos, M. Á. Vázquez, and A. I. Pérez-Neira, "Deep learning for experimental hybrid terrestrial and satellite interference management," in *2019 IEEE 20th International Workshop on Signal Processing Advances in Wireless Communications (SPAWC)*. Cannes, France: IEEE, 02-05 Jul. 2019, pp. 1–5.

[237] L. Pellaco, N. Singh, and J. Jaldén, "Spectrum prediction and interference detection for satellite communications," in *International Communications Satellite Systems Conference*. Okinawa, Japan: IET, 29 Oct.-1 Nov. 2019, pp. 64–18.

[238] J. Qin, F. Zhang, K. Wang *et al.*, "Interference signal feature extraction and pattern classification algorithm based on deep learning," *Electronics*, vol. 11, no. 14, p. 2251, Jul. 2022.

[239] Z. Na, Y. Liu, Y. Cui *et al.*, "Research on aggregation and propagation of self-similar traffic in satellite network," *Int. J. Hybrid Inf. Technol.*, vol. 8, no. 1, pp. 325–338, Jan. 2015.

[240] F. Zhu, L. Liu, and T. Lin, "An LSTM-based traffic prediction algorithm with attention mechanism for satellite network," in *Proc. 3rd Int. Conf. Artif. Intell. Pattern Recognit.*, Jan. 2020, pp. 205–209.

[241] D. Shi, Z. Guo, K. H. Johansson *et al.*, "Causality countermeasures for anomaly detection in cyber-physical systems," *IEEE Trans. Autom. Control*, vol. 63, no. 2, pp. 386–401, Feb. 2018.

[242] W. Yu and F. Yang, "Detection of causality between process variables based on industrial alarm data using transfer entropy," *Entropy*, vol. 17, no. 8, pp. 5868–5887, Aug. 2015.

[243] A. Alsaedi, N. Moustafa, Z. Tari *et al.*, "TON_IoT telemetry dataset: A new generation dataset of IoT and IIoT for data-driven intrusion detection systems," *IEEE Access*, vol. 8, pp. 165 130–165 150, Sep. 2020.

[244] N. Moustafa and J. Slay, "UNSW-NB15: A comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set)," in *Proc. Military Communications and Information Systems Conference (MilCIS)*, Canberra, ACT, Australia, 10-12 Nov. 2015, pp. 1–6.

[245] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180–2189, Jun. 2008.

[246] X. Ding, T. Song, Y. Zou *et al.*, "Security-reliability tradeoff analysis of artificial noise aided two-way opportunistic relay selection," *IEEE Trans. Veh. Technol.*, vol. 66, no. 5, pp. 3930–3941, May 2017.

[247] Y. Deng, L. Wang, S. A. R. Zaidi *et al.*, "Artificial-noise aided secure transmission in large scale spectrum sharing networks," *IEEE Trans. Commun.*, vol. 64, no. 5, pp. 2116–2129, May 2016.

[248] S. Yun, J.-M. Kang, I.-M. Kim *et al.*, "Deep artificial noise: Deep learning-based precoding optimization for artificial noise scheme," *IEEE Trans. Veh. Technol.*, vol. 69, no. 3, pp. 3465–3469, Mar. 2020.

[249] Y. Liao, J. Wang, and Q. H. Liu, "Transmit beampattern synthesis for frequency diverse array with particle swarm frequency offset optimization," *IEEE Trans. Antennas Propag.*, vol. 69, no. 2, pp. 892–901, Feb. 2021.

[250] W. Wang, "Frequency diverse array antenna: New opportunities," *IEEE Antennas Propagat. Mag.*, vol. 57, no. 2, pp. 145–152, Apr. 2015.

[251] Y. Liao, W.-q. Wang, and H. Shao, "Symmetrical logarithmic frequency diverse array for target imaging," in *Proc. IEEE Radar Conference*, Oklahoma City, OK, USA, 23-27 Apr. 2018, pp. 0039–0042.

[252] K. Gao, J. Cai, and J. Xiong, "Decoupled frequency diverse array range–angle-dependent beampattern synthesis using non-linearly increasing frequency offsets," *IET Microw. Antennas Propag.*, vol. 10, pp. 880–884(4), Jun. 2016.

[253] J. Hu, S. Yan, F. Shu *et al.*, "Artificial-noise-aided secure transmission with directional modulation based on random frequency diverse arrays," *IEEE Access*, vol. 5, pp. 1658–1667, Jan. 2017.

[254] Y. Xu, X. Shi, W. Li *et al.*, "Low-sidelobe range-angle beamforming with FDA using multiple parameter optimization," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 55, no. 5, pp. 2214–2225, Oct. 2019.

[255] P. Rocca, R. L. Haupt, and A. Massa, "Interference suppression in uniform linear arrays through a dynamic thinning strategy," *IEEE Trans. Antennas Propagat.*, vol. 59, no. 12, pp. 4525–4533, Dec. 2011.

[256] Tapan K. S., Hong W., Sheeyun P. *et al.*, "A deterministic least-squares approach to space-time adaptive processing (STAP)," *IEEE Trans. Antennas Propagat.*, vol. 49, no. 1, pp. 91–103, Jan. 2001.

[257] D. Cristallini and W. Burger, "A robust direct data domain approach for STAP," *IEEE Trans. Signal Process.*, vol. 60, no. 3, pp. 1283–1294, Mar. 2012.

[258] S. Xu, J. Liu, Y. Cao *et al.*, "Intelligent reflecting surface enabled secure cooperative transmission for satellite-terrestrial integrated networks," *IEEE Trans. Veh. Technol.*, vol. 70, no. 2, pp. 2007–2011, Feb. 2021.

[259] C. Huang, G. Chen, Y. Zhou *et al.*, "Deep learning empowered secure RIS-assisted non-terrestrial relay networks," in *Proc. Vehicular Technology Conference*, London, UK, Sep. 2022, pp. 1–5.

[260] J. Yuan, G. Chen, M. Wen *et al.*, "Secure transmission for THz-empowered RIS-assisted non-terrestrial networks," *IEEE Trans. Veh. Technol.*, vol. 72, no. 5, pp. 5989–6000, May 2023.

[261] Y. Ge and J. Fan, "Active reconfigurable intelligent surface assisted secure and robust cooperative beamforming for cognitive satellite-terrestrial networks," *IEEE Trans. Veh. Technol.*, vol. 72, no. 3, pp. 4108–4113, Mar. 2023.

[262] Y. Wang, Z. Lin, H. Niu *et al.*, "Secure satellite transmission with active reconfigurable intelligent surface," *IEEE Commun. Lett.*, vol. 26, no. 12, pp. 3029–3033, Dec. 2022.

[263] H. Cao, W. Zhu, W. Feng *et al.*, "Robust beamforming based on graph attention networks for IRS-assisted satellite IoT communications," *Entropy*, vol. 24, no. 3, p. 326, Feb. 2022.

[264] H. Dong, C. Hua, L. Liu *et al.*, "Weighted sum-rate maximization for multi-IRS aided integrated terrestrial-satellite networks," in *IEEE Global Communications Conference (GLOBECOM)*. Madrid, Spain: IEEE, 07-11 Dec. 2021, pp. 1–6.

[265] H. Dong, C. Hua, L. Liu *et al.*, "Towards integrated terrestrial-satellite network via intelligent reflecting surface," in *IEEE International Conference on Communications*, Montreal, QC, Canada, 14-23 Jun. 2021, pp. 1–6.

[266] H. Dong, C. Hua, L. Liu *et al.*, "Intelligent reflecting surface-aided integrated terrestrial-satellite networks," *IEEE Trans. Wireless Commun.*, Oct. 2022.

[267] S. Xu, J. Liu, T. K. Rodrigues *et al.*, "Robust multi-user beamforming for IRS-enhanced near-space downlink communications coexisting with satellite system," *IEEE Internet Things J.*, vol. 9, no. 16, pp. 14 900–14 912, Aug. 2022.

[268] X. Liu, B. Zhao, M. Lin *et al.*, "IRS-aided uplink transmission scheme in integrated satellite-terrestrial networks," *IEEE Trans. Veh. Technol.*, vol. 72, no. 2, pp. 1847–1861, Feb. 2023.

[269] E. Lagunas, S. K. Sharma, S. Maleki *et al.*, "Power control for satellite uplink and terrestrial fixed-service co-existence in Ka-band," in *Proc. Vehicular Technology Conference*, Boston, MA, USA, Sep. 2015, pp. 1–5.

[270] C. Yang, Q. Zhang, Q. Tian *et al.*, "In-line interference mitigation method based on adaptive modulation and coding for satellite system," in *Proc. International Conference on Optical Communications and Networks*, Wuzhen, China, Aug. 2017, pp. 1–3.

[271] C. Zhang, J. Jin, H. Zhang *et al.*, "Spectral coexistence between LEO and GEO satellites by optimizing direction normal of phased array antennas," *China Commun.*, vol. 15, no. 6, pp. 18–27, Jun. 2018.

[272] H. Wang, C. Wang, J. Yuan *et al.*, "Coexistence downlink interference analysis between LEO system and GEO system in Ka band," in *Proc. IEEE Int. Conf. Comm.*, Beijing, China, Aug. 2018, pp. 465–469.

[273] R. Li, P. Gu, and C. Hua, "Optimal beam power control for co-existing multibeam GEO and LEO satellite system," in *Proc. International Conference on Wireless Communications and Signal Processing*, Xi'an, China, Oct. 2019, pp. 1–6.

[274] T. Li, J. Jin, W. Li *et al.*, "Research on interference avoidance effect of OneWeb satellite constellation's progressive pitch strategy," *Int. J. Satell. Commun. Netw.*, Mar. 2021.

[275] C. Zhang, C. Jiang, J. Jin *et al.*, "Spectrum sensing and recognition in satellite systems," *IEEE Trans. Veh. Technol.*, vol. 68, no. 3, pp. 2502–2516, Mar. 2019.

[276] J. Hu, G. Li, D. Bian *et al.*, "Energy-efficient cooperative spectrum sensing in cognitive satellite terrestrial networks," *IEEE Access*, vol. 8, pp. 161 396–161 405, Sep. 2020.

[277] Y. Wang, X. Ding, and G. Zhang, "A novel dynamic spectrum-sharing method for GEO and LEO satellite networks," *IEEE Access*, vol. 8, pp. 147 895–147 906, Aug. 2020.

[278] X. Ding, L. Feng, Y. Zou *et al.*, "Deep learning aided spectrum prediction for satellite communication systems," *IEEE Trans. Veh. Technol.*, vol. 69, no. 12, pp. 16 314–16 319, Dec 2020.

[279] J. Tang, D. Bian, G. Li *et al.*, "Resource allocation for LEO beam-hopping satellites in a spectrum sharing scenario," *IEEE Access*, vol. 9, pp. 56 468–56 478, Apr. 2021.

[280] P. Gu, R. Li, C. Hua *et al.*, "Dynamic cooperative spectrum sharing in a multi-beam LEO-GEO co-existing satellite system," *IEEE Trans. Wireless Commun.*, vol. 21, no. 2, pp. 1170–1182, Feb. 2022.

[281] G. Ding, Y. Jiao, J. Wang *et al.*, "Spectrum inference in cognitive radio networks: Algorithms and applications," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 1, pp. 150–182, First Quart. 2018.

[282] W. Liang, S. X. Ng, and L. Hanzo, "Cooperative overlay spectrum access in cognitive radio networks," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 3, pp. 1924–1944, Third Quart. 2017.

[283] C. Jiang, Y. Chen, K. J. R. Liu *et al.*, "Renewal-theoretical dynamic spectrum access in cognitive radio network with unknown primary behavior," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 3, pp. 406–416, Mar. 2013.

[284] T. Yucek and H. Arslan, "A survey of spectrum sensing algorithms for cognitive radio applications," *IEEE Commun. Surveys Tuts.*, vol. 11, no. 1, pp. 116–130, First Quart. 2009.

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

[286] L. Hanzo, L.-L. Yang, E. Kuan *et al.*, *Single-and multi-carrier DS-CDMA: Multi-user detection, space-time spreading, synchronisation, standards and networking*. John Wiley & Sons, 2003.

[287] R. Iltis and L. Milstein, "Performance analysis of narrow-band interference rejection techniques in DS spread-spectrum systems," *IEEE Trans. Commun.*, vol. 32, no. 11, pp. 1169–1177, Nov. 1984.

[288] M. K. Simon and A. Polydoros, "Coherent detection of frequency-hopped quadrature modulations in the presence of jamming," *IEEE Trans. Commun.*, vol. 29, no. 11, pp. 1644–1660, Nov. 1981.

[289] G. Li, Q. Wang, V. K. Bhargava *et al.*, "Maximum-likelihood diversity combining in partial-band noise," *IEEE Trans. Commun.*, vol. 46, no. 12, pp. 1569–1574, Dec. 1998.

[290] J. Kang and K. Teh, "Performance analyses of coherent fast frequency-hopping spread-spectrum systems with partial band noise jamming and AWGN," in *Proc. Fourth International Conference on Information, Communications and Signal Processing, 2003 and the Fourth Pacific Rim Conference on Multimedia*, vol. 1, Singapore, Dec. 2003, pp. 678–681.

[291] S. C. Douglas, Quanhong Zhu, and K. F. Smith, "A pipelined LMS adaptive FIR filter architecture without adaptation delay," *IEEE Trans. Signal Process.*, vol. 46, no. 3, pp. 775–779, Mar. 1998.

[292] B. Raghothaman, D. A. Linebarger, and D. Begusic, "A new method for low rank transform domain adaptive filtering," *IEEE Trans. Signal Process.*, vol. 48, no. 4, pp. 1097–1109, May 2000.

[293] Z. Wang, M. Lv, and B. Tang, "Paper application of partial coefficient update LMS algorithm to suppress narrowband interference in DSSS system," in *Proc. International Conference on Communication Software and Networks*, Chengdu, China, 27-28 Feb. 2009, pp. 275–278.

[294] P. A. Iannucci and T. E. Humphreys, "Fused low-earth-orbit GNSS," *IEEE Trans. Aerosp. Electron. Syst.*, Jun. 2022, doi:10.1109/TAES.2022.3180000.

[295] Y. Shang and X. Feng, "MLC-SUMPLE algorithm for aligning antenna arrays in deep space communication," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 49, no. 4, pp. 2828–2834, Oct. 2013.

[296] P. Yue, J. Du, R. Zhang, H. Ding, S. Wang, and J. An, "Collaborative LEO satellites for secure and green internet of remote things," *IEEE Internet Things J.*, vol. 10, no. 11, pp. 9283–9294, Jun. 2023.

[297] V. Weerackody, "Satellite diversity to mitigate jamming in LEO satellite mega-constellations," in *2021 IEEE International Conference on Communications Workshops (ICC Workshops)*. Montreal, QC, Canada: IEEE, 14-23 Jun. 2021, pp. 1–6.

[298] A. Anttonen, M. Kiviranta, and M. Höyhtyä, "Space debris detection over intersatellite communication signals," *Acta Astronaut.*, vol. 187, pp. 156–166, Oct. 2021.

[299] Y. Hao, P. Mu, H. Wang *et al.*, "Key generation method based on multi-satellite cooperation and random perturbation," *Entropy*, vol. 23, no. 12, p. 1653, Nov. 2021.

[300] Y. Wang, Y. Zhao, W. Chen *et al.*, "Routing and key resource allocation in SDN-based quantum satellite networks," in *2020 International Wireless Communications and Mobile Computing (IWCMC)*. Limassol, Cyprus: IEEE, 15-19 Jun. 2020, pp. 2016–2021.

[301] G. Cui, P. Duan, L. Xu *et al.*, "Latency optimization for hybrid GEO-LEO satellite assisted IoT networks," *IEEE Internet Things J.*, vol. 10, no. 7, pp. 6286–6297, Apr. 2023.

[302] Z. Yin, L. Zhang, X. Zhou *et al.*, "QoS-guaranteed secure multicast routing protocol for satellite ip networks using hierarchical architecture," *Int. J. Commun. Netw. Syst. Sci.*, vol. 3, no. 04, p. 355, Apr. 2010.

[303] Z. Yu, H. Zhou, and Z. Wu, "A trust-based secure routing protocol for multi-layered satellite networks," in *2012 IEEE International Conference on Information Science and Technology*. Wuhan, China: IEEE, 23-25 Mar. 2012, pp. 313–317.

[304] Y. Ding, Y. Zhao, and R. Zhang, "A secure routing algorithm based on trust value for micro-nano satellite network," in *2020 2nd International Conference on Information Technology and Computer Application (ITCA)*. IEEE, 18-20 Dec. 2020, pp. 229–235.

[305] R.-Y. Cai, M.-Y. Ju, L. Yang *et al.*, "Research on lightweight secure routing technology based on satellite network," in *2020 5th International Conference on Information Science, Computer Technology and Transportation (ISCTT)*. Shenyang, China: IEEE, 13-15 Nov. 2020, pp. 42–47.

[306] G. Zeng, Y. Zhan, and X. Pan, "Failure-tolerant and low-latency telecommand in mega-constellations: The redundant multi-path routing," *IEEE Access*, vol. 9, pp. 34 975–34 985, Feb. 2021.

[307] Y. Zhang, X. Hu, R. Chen *et al.*, "Dynamic beam hopping for DVB-S2X satellite: A multi-objective deep reinforcement learning approach," in *2019 IEEE International Conferences on Ubiquitous Computing & Communications (IUCC) and Data Science and Computational Intelligence (DSCI) and Smart Computing, Networking and Services (SmartCNS)*. Shenyang, China: IEEE, 21-23 Oct. 2019, pp. 164–169.

[308] X. Hu, Y. Wang, Z. Liu *et al.*, "Dynamic power allocation in high throughput satellite communications: A two-stage advanced heuristic learning approach," *IEEE Trans. Veh. Technol.*, vol. 72, no. 3, pp. 3502–3516, Apr. 2023.

[309] X. Hu, Y. Zhang, X. Liao *et al.*, "Dynamic beam hopping method based on multi-objective deep reinforcement learning for next generation satellite broadband systems," *IEEE Trans. Broadcast.*, vol. 66, no. 3, pp. 630–646, Sep. 2020.

[310] X. Hu, X. Liao, Z. Liu *et al.*, "Multi-agent deep reinforcement learning-based flexible satellite payload for mobile terminals," *IEEE Trans. Veh. Technol.*, vol. 69, no. 9, pp. 9849–9865, Sep. 2020.

[311] C. Han, L. Huo, X. Tong *et al.*, "Spatial anti-jamming scheme for internet of satellites based on the deep reinforcement learning and stackelberg game," *IEEE Trans. Veh. Technol.*, vol. 69, no. 5, pp. 5331–5342, May 2020.

[312] C. Han, A. Liu, H. Wang *et al.*, "Dynamic anti-jamming coalition for satellite-enabled army IoT: A distributed game approach," *IEEE Internet Things J.*, vol. 7, no. 11, pp. 10 932–10 944, Nov. 2020.

[313] P. Yan, F. Chu, L. Jia *et al.*, "A cross-layer anti-jamming method in satellite internet," *IET Commun.*, vol. 17, no. 1, pp. 121–133, Oct. 2022.

[314] B. Li, J. Huang, Y. Feng *et al.*, "A machine learning-based approach for improved orbit predictions of LEO space debris with sparse tracking data from a single station," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 56, no. 6, pp. 4253–4268, Dec. 2020.

[315] E. Marchetti, A. G. Stove, E. Hoare *et al.*, "Space-based sub-THz ISAR for space situational awareness - laboratory validation," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 58, no. 5, pp. 4409–4422, Mar. 2022.

[316] N. Li, Y. Xu, G. Basset *et al.*, "Vision based trajectory tracking of space debris in close proximity via integrated estimation and control," in *Proc. 2011 American Control Conference*, San Francisco, CA, USA, 29 Jun.-1 Jul. 2011, pp. 1033–1038.

[317] A. Dhondea, A. K. Mishra, and M. Inggs, "Investigation of variable discretization resolution for CD-EKFs in space object tracking," in *Proc. International Conference on Computer, Communication and Signal Processing*, Chennai, India, 10-11 Jan. 2017, pp. 1–6.

[318] L. Felicetti and M. R. Emami, "Spacecraft formation for debris surveillance," in *Proc. IEEE Aerospace Conference*, Big Sky, MT, USA, 4-11 Mar. 2017, pp. 1–12.

[319] B. Wei and B. Nener, "Consensus labeled multi-bernoulli filtering for distributed space debris tracking," in *Proc. International Conference on Control, Automation and Information Sciences*, Chiang Mai, Thailand, 31 Oct.-1 Nov. 2017, pp. 203–208.

[320] X. Yang, Y. Pi, T. Liu *et al.*, "Three-dimensional imaging of space debris with space-based terahertz radar," *IEEE Sensors Journal*, vol. 18, no. 3, pp. 1063–1072, Feb. 2018.

[321] M. Ramírez-Torres, M. Ferreras, C. Hernández *et al.*, "Technological developments for a space-borne orbital debris radar at 94 GHz," in *Proc. IEEE Radar Conference*, Oklahoma City, OK, USA, 23-27 Apr. 2018, pp. 0564–0569.

[322] S. Labsir, A. Giremus, G. Bourmaud *et al.*, "Tracking a cluster of space debris in low orbit by filtering on lie groups," in *Proc. IEEE International Conference on Acoustics, Speech and Signal Processing*, Brighton, UK, 12-17 May 2019, pp. 5481–5485.

[323] J. Tao, Y. Cao, L. Zhuang *et al.*, "Deep convolutional neural network based small space debris saliency detection," in *Proc. International Conference on Automation and Computing*, Lancaster, UK, 5-7 Sep. 2019, pp. 1–6.

[324] J. Xi, Y. Xiang, O. K. Ersoy *et al.*, "Space debris detection using feature learning of candidate regions in optical image sequences," *IEEE Access*, vol. 8, pp. 150 864–150 877, Aug. 2020.

[325] M. Maffei, A. Aubry, A. De Maio *et al.*, "Spaceborne radar sensor architecture for debris detection and tracking," *IEEE Trans. Geosci. Remote Sens.*, vol. 59, no. 8, pp. 6621–6636, Aug. 2021.

[326] D. Cataldo, L. Gentile, S. Ghio *et al.*, "Multibistatic radar for space surveillance and tracking," *IEEE Aerosp. Electron. Syst. Mag.*, vol. 35, no. 8, pp. 14–30, Aug. 2020.

[327] P. Knott and R. Perkuhn, "Non-destructive permittivity measurement of thin dielectric sheets quality conformance testing for the tracking and imaging radar TIRA," in *2015 German Microwave Conference*, Nuremberg, Germany, 16-18 Mar 2015, pp. 25–28.

[328] D. Mehrholz, L. Leushacke, W. Flury *et al.*, "Detecting, tracking and imaging space debris," *ESA Bulletin(0376-4265)*, no. 109, pp. 128–134, Feb. 2002.

[329] R. Opromolla and A. Nocerino, "Uncooperative spacecraft relative navigation with LIDAR-based unscented kalman filter," *IEEE Access*, vol. 7, pp. 180 012–180 026, Dec. 2019.

[330] X. Shen, Z. Song, H. Fan *et al.*, "General Bernoulli filter for arbitrary clutter and target measurement processes," *IEEE Signal Process Lett.*, vol. 25, no. 10, pp. 1525–1529, Oct. 2018.

[331] S. Labsir, A. Giremus, G. Bourmaud *et al.*, "Tracking a cluster of space debris in low orbit by filtering on Lie Groups," in *Proc. IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, Brighton, UK, 12-17 May 2019, pp. 5481–5485.

[332] B. Wei and B. D. Nener, "Multi-sensor space debris tracking for space situational awareness with labeled random finite sets," *IEEE Access*, vol. 7, pp. 36 991–37 003, Mar. 2019.

[333] T. Pultarova. The world's first wooden satellite will launch this year. (Jun. 15, 2021). [Online]. Available: https://www.space.com/first-wooden-satellite-will-launch-in-2021

[334] R. Dudziak, S. Tuttle, and S. Barraclough, "Harpoon technology development for the active removal of space debris," *Adv. Space Res.*, vol. 56, no. 3, pp. 509–527, Aug. 2015.

[335] T. Pultarova, "Robots, harpoons and nets: How to clean up orbital rubbish," *Engineering Technology*, vol. 13, no. 10, pp. 62–65, Nov. 2018.

[336] S. Nishida, S. Kawamoto, Y. Okawa *et al.*, "Space debris removal system using a small satellite," *Acta Astronaut.*, vol. 65, no. 1, pp. 95–102, Aug. 2009.

[337] D. Shiga. Giant balloons could clear out space junk. (Aug. 4, 2010). [Online]. Available: https://www.newscientist.com/article/dn19262-giant-balloons-could-clear-out-space-junk/

[338] B. Ren, "The most optimal device for removing space debris," in *Proc. International Conference on Machinery, Materials, Environment, Biotechnology and Computer*, Tianjin, China, Jun. 2016, pp. 1144–1147.

[339] G. Acciarini, F. Pinto, F. Letizia *et al.*, "Kessler: A machine learning library for spacecraft collision avoidance," in *8th European Conference on Space Debris*, Apr. 2021, pp. 1–9.

[340] T. Uriot, D. Izzo, L. F. Simões *et al.*, "Spacecraft collision avoidance challenge: Design and results of a machine learning competition," *Astrodynamics*, vol. 6, no. 2, pp. 121–140, Apr. 2021.

[341] W. Zhang, F. Li, J. Li *et al.*, "Review of on-orbit robotic arm active debris capture removal methods," *Aerospace*, vol. 10, no. 1, p. 13, Dec. 2022.

[342] Y. Xiang, J. Xi, M. Cong *et al.*, "Space debris detection with fast grid-based learning," in *Proc. IEEE 3rd International Conference of Safe Production and Informatization*, Chongqing City, China, 28-30 Nov. 2020, pp. 205–209.

[343] J. Yang, Y. H. Hu, Y. Liu *et al.*, "On the application of reinforcement learning in multi-debris active removal mission planning," in *2019 IEEE 28th International Symposium on Industrial Electronics (ISIE)*. Vancouver, BC, Canada: IEEE, 12-14 Jun 2019, pp. 605–610.

[344] Z. Ma, Y. Zhao, W. Wang *et al.*, "Adaptive snapshot routing based on space debris risk perception in satellite optical networks," in *2021 International Conference on Optical Network Design and Modeling (ONDM)*, 28 Jun. -01 Jul. 2021, pp. 1–6.

[345] W. Zhang, T. Wu, and H. Ma, "Discussion on the development direction of intelligent integrated space tt&c network," in *2021 7th International Conference on Computer and Communications (ICCC)*. Chengdu, China: IEEE, 10-13 Dec. 2021, pp. 459–463.

[346] M. Cannon, A. Keller, and M. Wirthlin, "Improving the effectiveness of TMR designs on FPGAs with SEU-aware incremental placement," in *Proc. IEEE International Symposium on Field-Programmable Custom Computing Machines*, Boulder, CO, USA, Sep. 2018, pp. 141–148.

[347] O. Gonçalves, G. Prenat, G. Di Pendina *et al.*, "Nonvolatile runtime-reconfigurable FPGA secured through MRAM-based periodic refresh," in *Proc. IEEE International Memory Workshop*, Monterey, CA, USA, Aug. 2013, pp. 170–173.

[348] F. L. Kastensmidt, L. Carro, and R. A. da Luz Reis, *Fault-tolerance techniques for SRAM-based FPGAs*. Springer, 2006, vol. 1.

[349] M. Yin, "SEU-tolerant design of SRAM FPGA for space use," *Spacecraft Environ. Eng.*, vol. 28, no. 6, Dec. 2011.

[350] R. P. Bastos, M. G. Picas, and R. Velazco, "Medium-earth orbit spaceflight radiation effects in triple modular system on programmable device," *IEEE Trans. Nucl. Sci.*, pp. 1–1, 2023. [Online]. Available: 10.1109/TNS.2023.3247174

[351] C. Jiang, X. Wang, J. Wang *et al.*, "Security in space information networks," *IEEE Commun. Mag.*, vol. 53, no. 8, pp. 82–88, Aug. 2015.

[352] E. Meng, X. Bu, and C. Wang, "A novel anti-interception waveform in LEO satellite system," in *Proc. IEEE 4th Information Technology, Networking, Electronic and Automation Control Conference (ITNEC)*, Chongqing, China, 12-14 Jun. 2020, pp. 1183–1187.

[353] F. Liu, C. Masouros, A. P. Petropulu *et al.*, "Joint radar and communication design: Applications, state-of-the-art, and the road ahead," *IEEE Trans. Commun.*, vol. 68, no. 6, pp. 3834–3862, Jun. 2020.

[354] A. Liu, Z. Huang, M. Li, *et al.*, "A survey on fundamental limits of integrated sensing and communication," *IEEE Commun. Surv. Tutor.*, vol. 24, no. 2, pp. 994–1034, Second quart. 2022.

[355] Z. Feng, Z. Fang, Z. Wei *et al.*, "Joint radar and communication: A survey," *China Commun.*, vol. 17, no. 1, pp. 1–27, Jan. 2020.

[356] D. K. P. Tan, J. He, Y. Li *et al.*, "Integrated sensing and communication in 6G: Motivations, use cases, requirements, challenges and future directions," in *2021 1st IEEE International Online Symposium on Joint Communications & Sensing (JC&S)*. Dresden, Germany: IEEE, 23-24 Feb. 2021, pp. 1–6.

[357] A. Liu, Z. Huang, M. Li *et al.*, "A survey on fundamental limits of integrated sensing and communication," *IEEE Commun. Surv. Tutor.*, vol. 24, no. 2, pp. 994–1034, Second Quart. 2022.

[358] Y. Tian, G. Pan, and M.-S. Alouini, "Applying deep-learning-based computer vision to wireless communications: Methodologies, opportunities, and challenges," *IEEE open j. Commun. Soc.*, Dec. 2020.

[359] N. Gonzalez-Prelcic, A. Ali, V. Va, and R. W. Heath, "Millimeter-wave communication with out-of-band information," *IEEE Commun. Mag.*, vol. 55, no. 12, pp. 140–146, Dec. 2017.

[360] Z. Hua, Y. Lu, G. Pan *et al.*, "Computer vision aided mmWave UAV communication systems," *IEEE Internet of Things J.*, vol. 10, no. 14, pp. 12 548–12 561, Jul. 2023.

[361] Y. Tian, G. Pan, H. ElSawy, and M.-S. Alouini, "Satellite-aerial communications with multi-aircraft interference," *IEEE Trans. Wireless Commun.*, Mar. 2023, doi:10.1109/TWC.2023.3247724.

[362] R. Mur-Artal and J. D. Tardós, "ORB-SLAM2: An open-source SLAM system for monocular, stereo, and RGB-D cameras," *IEEE Trans. Robot.*, vol. 33, no. 5, pp. 1255–1262, Oct. 2017.

[363] A. Bochkovskiy, C.-Y. Wang, and H.-Y. M. Liao, "YOLOv4: Optimal speed and accuracy of object detection," 2020. [Online]. Available: 10.48550/arXiv.2004.10934

[364] I. D. Portillo, B. G. Cameron, and E. F. Crawley, "A technical comparison of three low earth orbit satellite constellation systems to provide global broadband," *Acta Astronaut.*, vol. 159, pp. 123–135, Jun. 2019.

[365] Y. Zhan, G. Zeng, and X. Pan, "Networked TT&C for mega satellite constellations: A security perspective," *China Commun.*, vol. 19, no. 9, pp. 58–76, Sep. 2022.

[366] N. Boschetti, N. Gordon, J. Sigholm *et al.*, "Commercial space risk framework assessing the satellite ground station security landscape for NATO in the arctic and high north," in *MILCOM 2022 - 2022 IEEE Military Communications Conference (MILCOM)*, Rockville, MD, USA, 28 Nov. - 02 Dec. 2022, pp. 679–686.

Pingyue Yue (Student Member) received his B.S. degrees from the Zhengzhou University , Zhengzhou, China, in 2016. He is currently a Ph.D. student in the School of Information and Electronics, Beijing Institute of Technology. His research interests include satellite communication, physical-layer security, and interference suppression.

Jianping An (Senior Member, IEEE) received his Ph.D. degree from Beijing Institute of Technology, China, in 1996. He joined the School of Information and Electronics, Beijing Institute of Technology in 1995, where he is now a full professor. He is currently the Dean of the School of Cyberspace Science and Technology, Beijing Institute of Technology. His research interests include digital signal processing, wireless communications, and satellite networks. He has received two national awards for technological inventions and science and technology progress.

Jiankang Zhang (Senior Member, IEEE) is a Senior Lecturer of Computer Science with Bournemouth University. Prior to joining in Bournemouth University, he was a Senior Research Fellow with the University of Southampton, U.K. He serves as an Associate Editor for IEEE ACCESS.

Jia Ye (Member, IEEE) was born in Chongqing, China. She received the Ph.D. degree in electrical and computer engineering from the King Abdullah University of Science and Technology (KAUST), Saudi Arabia, in 2022. Since January 2023, she has been with the School of Electrical Engineering, Chongqing University, Chongqing, China, as an Associate Professor. Her main research interest includes the performance analysis and modeling of wireless information and energy transfer systems.

Gaofeng Pan (Senior Member, IEEE) received his B.Sc in Communication Engineering from Zhengzhou University, Zhengzhou, China, in 2005, and the Ph.D. degree in Communication and Information Systems from Southwest Jiaotong University, Chengdu, China, in 2011. He is currently with the School of Cyberspace Science and Technology, Beijing Institute of Technology, China, as a Professor. He is also serving as an Editor for several jounals, e.g., IEEE TRANSACTIONS ON GREEN COMMUNICATIONS AND NETWORKING, PHYSICAL COMMUNICATION, etc. His research interest spans special topics in communications theory, signal processing, and protocol design.

Shuai Wang (Member, IEEE) received the Ph.D. degree in communications systems from the Beijing Institute of Technology (BIT), China, in 2012. Upon his graduation, he joined the Faculty of the School of Information and Electronics, BIT. In 2021, he transferred to the new-founded School of Cyberspace Science and Technology, where he has been appointed as the Chair Professor of the Department of Information Security and Countermeasures. He has contributed more than 40 peer-reviewed articles, mainly in leading IEEE journals or conferences and holds more than 60 patents. His research interests include satellite communications, anti-interference communications, and datalink technologies for space platforms. He was a co-recipient of the Second Class National Technical Invention Award of China in 2019. He has served as an Editor for IEEE WIRELESS COMMUNICATIONS LETTERS. He is serving as an Editor for China Communications.

Pei Xiao (Senior Member, IEEE) is a professor of Wireless Communications at the Institute for Communication Systems (ICS), home of 5GIC and 6GIC at the University of Surrey. He received the PhD degree from Chalmers University of Technology, Gothenburg, Sweden in 2004. He is currently the technical manager of 5GIC/6GIC, leading the research team in the new physical layer work area, and coordinating/supervising research activities across all the work areas (https://www.surrey.ac.uk/institutecommunication-systems/5g-6g-innovation-centre). Prior to this, he worked at Newcastle University and Queen's University Belfast. He also held positions at Nokia Networks in Finland. He has published extensively in the fields of communication theory, RF and antenna design, signal processing for wireless communications, and is an inventor on over 15 recent 5GIC patents addressing bottleneck problems in 5G systems.

Lajos Hanzo (Life Fellow, IEEE) received the master's and Doctoral degrees from the Technical University (TU) of Budapest in 1976 and 1983, respectively, the Doctor of Sciences (D.Sc.) degree from the University of Southampton in 2004, and the first Honorary Doctoral degree from TU of Budapest in 2009 and the second Honorary Doctoral degree from the University of Edinburgh in 2015. He is the recipient of the 2022 Eric Sumner Field Award. He is a Foreign Member of the Hungarian Academy of Sciences and a former Editor-in-Chief of the IEEE Press. He has served several terms as Governor of both IEEE ComSoc and of VTS. He has published over 2000 contributions at IEEE Xplore, 19 Wiley-IEEE Press books and has helped the fast-track career of 123 Ph.D. students. He is also a Fellow of the Royal Academy of Engineering, IET, and of EURASIP.