Universidad Politécnica de Cartagena

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

Author - Wai Yan Kyaw
Supervisor - Juan Pedro Muñoz Gea
Reviewer - María Dolores Cano Baños

Table of Contents

1. Introduction

With the rapidly increasing number of IoT smart devices and user demands, future wireless networks must be able to seamlessly interface terrestrial and satellite networks. Therefore, satellite networks will play a crucial role in the future wireless network. In Space Information Networks (SIN), Low Earth Orbit satellite (LEO) will be eminently paramount among Medium Earth Orbit (MEO) and Geostationary Earth Orbit (GEO). Compared to MEO and GEO satellites, Low Earth Orbit (LEO) satellites are closer to the Earth. Hence, they are more suitable for supporting delay-sensitive communications worldwide and it can reduce the average launch cost and deployment time. From 2012 to the second quarter of 2023, about 7824 LEO satellites have been successfully launched. Even though there have already been launched almost 8000 LEO satellites in Space, there are a lot of security and reliability issues interfacing between satellites and terrestrial networks. Additionally, there is a lack of literature on the security and reliability issues of LEO Satellite Communication Systems (SCSs). The things most researchers did not describe about LEO SCSs are insufficient research of existing papers, lack of consideration for the inherent characteristics of LEO SCSs and lack of design guidelines of secure and reliable LEO SCS. In this review paper based on the survey of Low Earth Orbit Satellite Security and Reliability, the author aims to focus on this lack of information.

LEO satellites, with their low-latency and high-frequency data transmission, are essential for real-time connectivity across vast and isolated regions. They support sustainable practices in agriculture, enhance urban living through smart technology, and provide life-saving communication in emergencies. By covering both urban and remote areas, LEO satellites are fundamental to building resilient, connected and efficient systems across the globe. Fig 1 illustrates three application scenarios where LEO satellites play a crucial role in enabling smart, interconnected systems across diverse sectors, especially Internet of Remote Things (IoRT), smart city and emergency rescue.

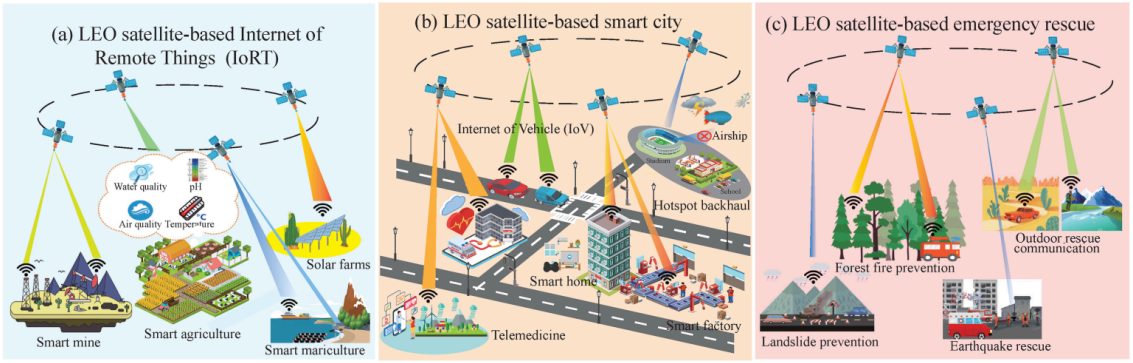

Fig. 2. The application scenarios of LEO SCSs.

2. Background

In this section, the author summarizes the system architecture of LEO satellites and its inherent characteristics and research developments of LEO constellations. Fig. 2 illustrates the system architecture of LEO SCSs. The system architecture of Low Earth Orbit Satellite Communication Systems (LEO SCSs) is divided into three segments: space, ground, and user. The space segment includes LEO satellites and Inter-Satellite Links (ISLs), though not all systems, such as OneWeb, have ISLs. The ground segment consists of gateways and a Network Control Center (NCC), which manages operations and connects to

satellites via feeder links. If ISLs are absent, more gateways are needed to ensure satellite visibility, connected by optical fiber for reliability. The user segment comprises numerous terminals that connect to LEO satellites through user links.

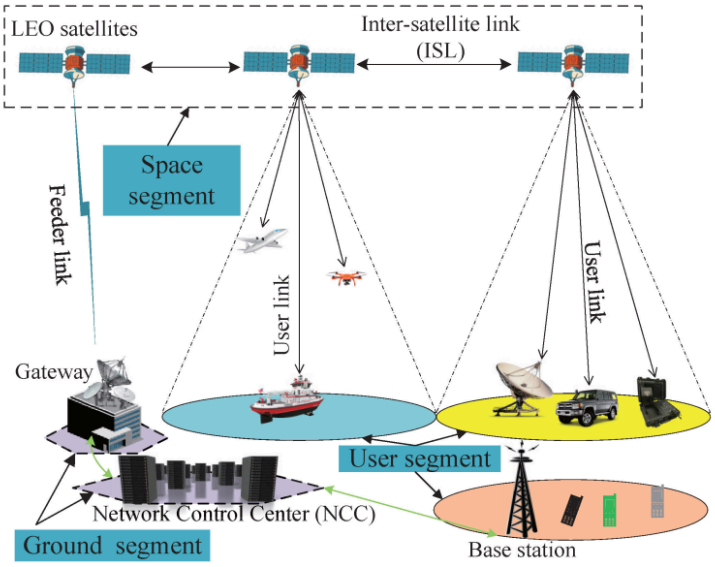

Fig. 2. The System Architecture of LEO SCSs.

Compared to MEO and GEO satellites, LEO satellites are more affordable and reduce the average launch cost and are compatible with terrestrial communication networks. That is why researchers and commercial companies are focusing on LEO for their future network systems especially for 6G and Internet of Things (IoT) networks. Table I summarizes the inherent characteristics between GEO, MEO and LEO satellites.

TABLE I
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	90 to 100 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

Although the improvement of LEO SCSs is operating fully with terrestrial networks, there are some unique challenges due to their inherent characteristics, as follows.

- The specific orbit of LEO satellites degrades both the security and reliability
- The high mobility of LEO satellites degrades both the security and reliability
- The large number of LEO satellites or gateways degrades the security
- The limited resources of LEO satellites degrades both the security and reliability
- The production of low-cost satellites degrades both the security and reliability
- Quality of Service (QoS) guarantee when designing security and reliability solutions

3. Security and Reliability Requirements

When considering security, it is essential to address the principles of **Confidentiality, Integrity, Accountability** and **Low Latency**. In addition, it is imperative to consider security threats targeting the Space, Air and Ground segments, as these can result in unpredictable challenges for future networks. Besides, collisions on debris and spacecraft can lead to reliability issues on LEO satellites. Fig 3. illustrates the classification of security and reliability issues in LEO satellites interfacing with terrestrial communication networks.

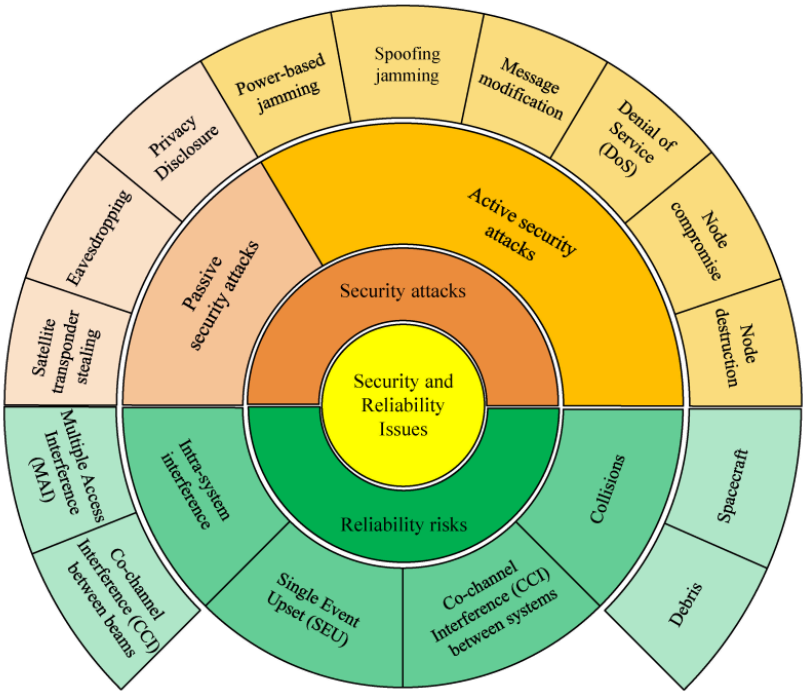

Fig. 3. Classification of security and reliability issues.

As shown above, passive security attacks such as eavesdropping, satellite transponder stealing and privacy disclosure aim to intercept and interpret transmitted messages without altering them. Subsequently, this can lead to active attacks which can compromise data confidentiality.

- Eavesdropping - Wireless nature is easy for attackers to intercept and interpret transmitted data.

- Satellite Transponder Stealing - The deployment of satellites is impossible for every country due to high cost and advanced technology and therefore, the attackers try to steal these satellites to make their own transmissions between satellites.
- Privacy Disclosure - The closer to Earth, the better LEO satellites are for IoRT. However, it could result in a breach of user privacy due to eavesdropping.

In active security attacks, the attacks between terrestrial networks and LEO satellites can be considered as power-based jamming, spoofing jamming, message modification, denial of service, node compromise, node destruction These attacks can alter, manipulate, or disrupt data and system operations, which can result to integrity and availability.

- Power-based Jamming is to disrupt legitimate signals by releasing power-based jamming and there are three types of power-based jamming such as space-based jamming, air-based jamming and ground-based jamming. Space-based jamming mainly affects downlink transmissions. Air-based jamming impacts both downlink and uplink transmissions, whereas ground-based jamming primarily affects uplink transmissions.
- Spoofing Jamming is a more insidious and technically sophisticated form of electronic attack compared to power-based jamming. It frequently occurs in civilian GPS systems.
- Message Modification involves altering the contents of data transmitted from the sender to the receiver.
- Denial of Service attack is to disrupt or shut down a device or network. It can occur in ground and space segments. DoS attacks are difficult to detect and mitigate because the attackers use hit-and-run tactics from numerous IoT devices.
- Node Compromise: When an attacker gains control of a legitimate node, they can exploit it to launch attacks or spread malicious activities, putting the entire network at risk. This is particularly dangerous because the compromised node appears to be a trusted component of the network, making it more challenging to detect and mitigate the threat.
- Node Destruction: LEO satellites can be destroyed by anti-satellites weapons such as missiles and high-power laser beams.

Table II summarizes the important differences between active and passive security attacks.

Table II

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

Having described security attacks, it is now essential to describe reliability risks. In terms of reliability risks, there are four main issues in LEO satellites: intra-system interference, co-channel interference between systems, single event upsets and collisions.

- Intra-System Interference - It contains multi-access interference and co-channel interference between beams. MAI can cause near-far effects. Multi-beam satellites boost capacity by reusing frequencies, but this can lead to co-channel interference (CCI) in overlapping areas where beams share the same frequency.
- CCI between Systems - GEO SCSs and LEO SCSs have to coexist within the same spectrum to address the spectrum scarcity problem because of an increasing number of LEO satellites over the last few years. It can cause CCI between GEO and LEO SCSs. Figure 4 describes CCI between LEO SCSs and GEO SCSs.
- Single Event Upsets - SEUs constitute reversible soft errors. The probability of SEUs is related to the orbit altitude and orbit inclination. At altitudes below 2000 km, the probability of SEUs occuring increases with higher orbit altitudes. In addition, the probability of SEUs occurring increases as the orbit inclination approaches 90°.
- Collisions - The probability of collisions in space increases with the frequency of space launch activities. LEO satellites move around the planet at approximately 7 km/s, with relative speeds reaching 10 km/s or higher. Therefore, even a tiny piece of debris can pose a serious hazard.

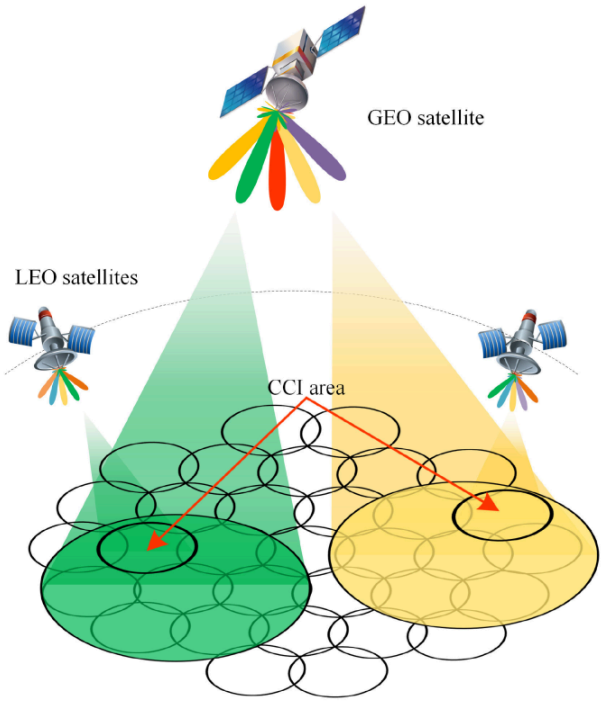

Figure. 4. CCI between LEO and GEO SCSs.

In addition, there will be a trade-off in finding an optimal orbit altitude that ensures both low collision risk and low probability of SEUs. The closer the orbit inclination is to 90°, the more seamless the global coverage becomes, but the probability of SEUs also increases.

4. Security and Reliability Enhancement Solutions

Security attacks and reliability issues have already been described in the preceding section. In this section, the essential principles of prevention, detection and mitigation of security attacks and reliability issues will be summarized. Firstly, Terahertz (THz) and laser techniques are capable of coping with CCI by avoiding frequency reuse between GEO and LEO SCSs for prevention. In addition, deploying firewalls and antivirus software are also paramount for prevention. For detection, using an intrusion detection system (IDS) is the most suitable technique. Lastly, Spread Spectrum (SS) techniques such as Frequency Hopping Spread Spectrum (FHSS), Direct Sequence Spread Spectrum (DSSS), Time Hopping Spread Spectrum (THSS) and Fast Frequency Hopping Spread Spectrum (FFHSS) are popular due to their immunity to jamming and eavesdropping.

Fig 5 describes the classification of solutions dealing with security and reliability in LEO SCSs. In order to focus on security enhancement solutions, both active and passive solutions are implemented to address security attacks.

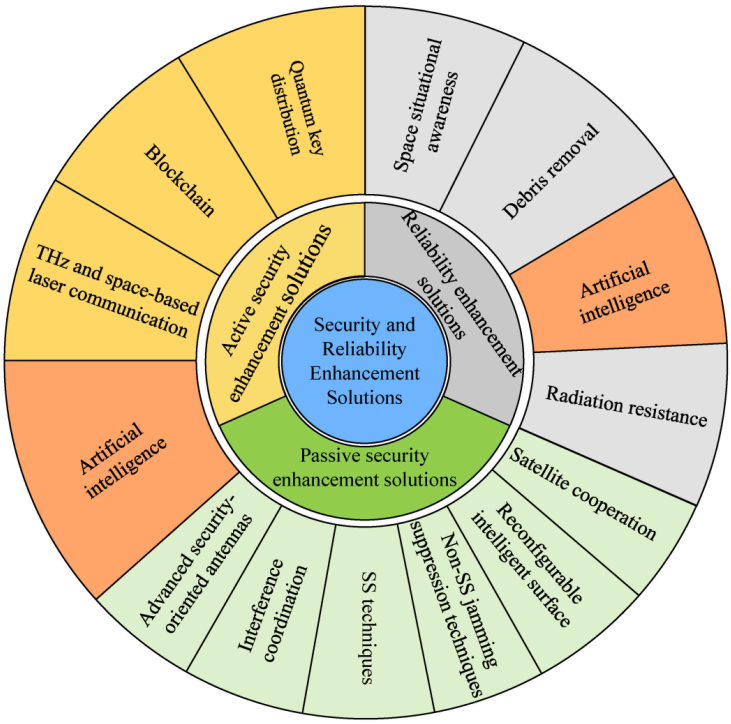

Figure. 5. The classification of solutions dealing with security and reliability in LEO SCSs.

Active enhancement solutions including QKD, blockchain, THz, space-based laser communications, and AI, aim for prevention or actively detecting impending deleterious issues.

Quantum Key Distribution (QKD) is a secure method for encrypting data. It generates a secret key, which is used to encrypt and decrypt messages. This key must be shared securely between the sender and receiver. Traditional cryptography assumed it would take a long time for an eavesdropper to crack the key, but quantum computers challenge this assumption. QKD uses quantum channels for key negotiation, making it more secure. It typically relies on optical fibers or free-space links to transmit quantum signals.

Significant progress has been made in QKD, including the launch of the first quantum satellite-based QKD experiment in 2016. Many countries and organizations are developing their own QKD services.

Blockchain is also one of the solutions to enhance the security and management of Low Earth Orbit (LEO) SCSs. Blockchain is a decentralized system that stores transactional records in a digital ledger across a peer-to-peer network. This ensures confidentiality, accountability, and decentralization. Users need the correct key to access or update information, and once updated, the information is immutable and tamper-proof. If some nodes in the network fail, the others continue to function, maintaining data integrity and network operation. This makes blockchain a robust solution for managing LEO SCSs. Researchers use blockchain to enhance security against various attacks. For example, it helps detect spoofing in UAV networks and protects IoT devices from data modification. Blockchain's distributed nature also makes it immune to DoS and DDoS attacks.

THz and Space-Based Laser Communication: Many Low Earth Orbit (LEO) satellites currently use decimeter and centimeter wave bands, but these frequencies are becoming crowded. To solve this, researchers are exploring higher frequencies such as the THz and optical bands. The THz band offers a lot of bandwidth but has limitations due to water vapor and other effects, making it less suitable for satellite-Earth links. However, it could be useful for inter-satellite links (ISLs) above the atmosphere, especially with large antennas to improve signal strength and reduce eavesdropping. Laser communications, which are highly directional and hard to detect, provide strong anti-interference capabilities and are lighter and more efficient than microwave communications. Starlink has successfully tested laser links between satellites and is expanding this technology to reduce the need for ground stations and extend coverage to remote areas.

Artificial Intelligence: AI has been very successful in terrestrial wireless communication systems and is now being used in LEO SCSs. Machine Learning (ML) is especially useful because it can learn from data and track changes during space missions. This makes ML particularly valuable for analyzing data and enhancing security in space communications such as tele-traffic data, housekeeping data, attack data, power system data and spectrum data.

Passive enhancement solutions directly face the issues and reduce or eliminate their impact as far as possible. The passive enhancement solutions are discussed in the following.

Advanced security-oriented Antennas: Advanced security-oriented antennas enhance satellite communication security by mitigating eavesdropping and jamming. They use techniques such as beamforming and artificial noise to protect signals. Frequency Diverse Arrays (FDA) help secure transmissions by varying beam patterns based on distance and angle. These antennas can also adjust their beam patterns to counteract jamming, ensuring reliable communication even under attack.

Reconfigurable Intelligent Surfaces: Reconfigurable Intelligent Surfaces (RIS) are an exciting new technology in wireless communications. They can manipulate signals to improve communication and security in satellite systems. RIS can reflect signals to avoid eavesdropping and reduce interference, making satellite communications more secure. For example, RIS can help block interference signals from reaching eavesdroppers, ensuring that satellite users receive clear and secure transmissions. Researchers have also proposed using RIS on high-altitude platforms to secure links between satellites and UAVs, even without knowing the eavesdropper's location.There are two types of RIS: passive and active. Passive RIS doesn't use extra power, while active RIS can adjust signal amplitude but introduces some noise. Active RIS can potentially offer better security but needs more research. RIS can also reduce interference within satellite networks, improving signal quality. By increasing the number of RIS elements and

optimizing their design, the communication performance can be significantly enhanced. RIS technology holds great promise for improving the security and reliability of satellite communications.

Interference Coordination: Interference coordination in LEO SCSs involves techniques such as power control, beam drifting, and cognitive radio to mitigate interference and improve spectral efficiency. These methods help manage the spectrum crunch and ensure coexistence with Geostationary Earth Orbit (GEO) satellites. Advanced algorithms and AI are used to optimize these processes, enhancing the overall performance and reliability of LEO SCSs.

SS Techniques: Spread Spectrum (SS) techniques have been used in military communications for over 70 years to secure transmissions by spreading the signal over a wide bandwidth. Common SS techniques include Direct Sequence Spread Spectrum (DSSS), Frequency Hopping Spread Spectrum (FHSS), and Multi-Carrier Direct Sequence Spread Spectrum (MC-DSSS).

- DSSS: This technique spreads the signal, making it hard for eavesdroppers to detect and providing some resistance to jamming. The signal is spread over a wide bandwidth and then dispersed at the receiver, which increases the Signal to Noise Ratio (SNR) and reduces the impact of jamming.
- FHSS: This method involves rapidly switching frequencies during transmission, making it difficult for jammers to interfere. Fast Frequency Hopping Spread Spectrum (FFHSS) enhances this by hopping multiple times within a single symbol duration, offering strong anti-jamming capabilities.
- MC-DSSS: This technique uses multiple sub-carriers and can adapt to avoid interference by monitoring the frequency spectrum in real-time. It can also hide sub-carriers within existing signals to improve confidentiality, though this can reduce signal integrity.

SS techniques provide robust methods for securing satellite communications by spreading signals and making them harder to intercept or jam.

Non-SS Jamming Suppression Techniques: When jamming power is too high for Spread Spectrum (SS) techniques, special jamming suppression algorithms are used. Temporal Domain Adaptive Filtering as the Least Mean Square (LMS) algorithm, is good for narrowband jamming. It adjusts filter weights to minimize error, balancing speed and accuracy. Transform Domain Adaptive Filtering works in the frequency domain, quickly identifying and filtering out jamming signals before converting the signal back to the time domain. Both techniques help maintain clear communication by reducing the impact of jamming**.**

Satellite Cooperation: Satellite cooperation is essential for enhancing the security and reliability of Low Earth Orbit (LEO) satellites. By combining signals from multiple satellites, the integrity of communications can be maintained while reducing the risk of eavesdropping. This cooperation involves compensating for delays, Doppler shifts, and phase offsets. Additionally, satellites can share resources and information to improve performance, manage jamming, and ensure secure routing through cryptographic and trust mechanisms. This collaborative approach helps address the challenges posed by the increasing number of satellites and diverse applications.

AI Tools: Artificial Intelligence (AI) enhances the security of Low Earth Orbit (LEO) Satellite Communication Systems (SCSs) by solving complex optimization problems and predicting threats. AI techniques such as deep reinforcement learning help manage beam-hopping and mitigate interference. Intelligent anti-jamming methods, such as hierarchical games and deep learning, counteract smart jamming attacks. AI also aids in optimizing passive security measures and improving overall system performance despite limited satellite resources.

Reliability enhancement solutions

The main objective is to ensure the stable operation of Low Earth Orbit (LEO) satellites by using reliability solutions such as Space Situational Awareness (SSA), debris removal, and radiation resistance.

Space Situational Awareness (SSA): SSA programs use ground-based and space-based facilities, along with advanced algorithms, to detect and track space debris. This helps in providing collision warnings and planning debris removal. SSA employs various sensors, including ground-based radars and optical telescopes, which have their own advantages and limitations. Ground-based radars can operate continuously but are costly and less effective for small debris. Optical telescopes are sensitive but limited by weather conditions. Space-borne radars and cameras are also used for closer and more efficient debris detection and tracking.

Debris Removal: Low Earth Orbit (LEO) is heavily contaminated with space debris, posing significant risks to satellites. AI, sensors and filtering algorithms are crucial for debris and removal. Table III summarizes the comparison of debris removal techniques.

Table III
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 my 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
	Effective large space debris such as failing or inoperative spacecraft	Easily penetrated by debris, especially sharp debris

Giant Balloons	Preventing further debris generation	Slow response because of balloon inflation
'Suicide' Satellite	Prevention further debris generation	Not able to be reused
	Low cost	Suitable for larger debris

Artificial Intelligence: It mainly uses Machine Learning (ML) and Deep Learning (DL), to enhance collision avoidance and debris management in Low Earth Orbit (LEO).

- **Collision Avoidance**: The increasing number of objects in LEO, such as satellites and debris, raises collision risks. AI, especially ML, helps predict and avoid collisions by analyzing real-world datasets. For example, the European Space Agency organized an ML competition to improve collision risk estimation.
- **Debris Identification and Removal Planning**: Despite collision avoidance efforts, LEO remains cluttered with debris from various sources. AI techniques and DL, are used to detect and identify debris, even in challenging conditions. Once identified, strategies such as using robotic arms to push debris into Earth's atmosphere for burning are planned. Reinforcement learning is also used to plan and execute debris removal missions effectively.

Overall, AI plays crucial roles in maintaining the safety and reliability of space operations by preventing collisions and managing space debris.

5. The Road Ahead

With the rapid growth of LEO satellites, several challenges have emerged, including accurate target detection, security challenges identification and tracking. Integrated Sensing and Communication (ISAC) holds great potential for addressing some of the challenges in LEO SCSs.

ISAC- aided Secure Transmission

The idea is to reuse spectrum due to the wireless communication being congested with the rapid proliferation of connected devices and satellites. It means to allow the wireless communication systems to access large portions of the spectrum available at radar frequencies. It can advance alleviating the shortage of radio frequencies, reducing overall system costs, cutting energy consumption and miniaturizing the devices.

CV-aided Space Communication

Researchers have proposed CV-aided communication schemes for mmWave and THz systems, focusing on extracting and estimating information about system topology, such as terminal positions and velocities, to improve wireless system design and optimization. These schemes offer one-way sensing using optical devices, reducing detection probability and resource consumption, and enable hostile target detection to enhance security. While situational awareness in space is established with optical and radar sensors, applying CV-aided methods for secure information transmission in space remains a challenge due to the dynamic and large-scale nature of LEO satellite systems.

Mega-Constellations

According to the 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. There will be a heavy computational burden, since ground segments have to supervise and manage the operational status and diverse functions of hundreds of even thousands of satellites in real-time. A minor computational or command error might have severe consequences for this giant network. ISLs within the constellation will be essential to exchange information between the mega-constellations and ground stations. The more satellites there are in Space,the higher likelihood of collisions between satellites and debris. In addition, the investigation of the security problems in mega-constellations requires the researchers' attention for further improvements.

LEO SCS Commercialization

The thriving LEO economy is drawing interest from companies and investors, but the crowded space and limited channel resources are leading to fierce competition among major companies even though there are still numerous challenges in LEO SCSs. The commercialization enhances the development of LEO satellite applications, such as the IoTs, smart cities, and intelligent manufacturing. The future of the LEO Satellite Communication Systems (SCS) market looks promising, but financial challenges remain significant. Companies such as LeoSat and OneWeb may need to scale back or cancel projects without additional investment. The COVID-19 pandemic has added uncertainty, highlighting the need for substantial upfront investment and cost reduction across all stages to avoid low-quality products and security issues.

6. Design Guideline

Designing an LEO Satellite Communication System (SCS) is complicated and involves balancing many conflicting factors. This section offers practical design guidelines for LEO SCSs, focusing on security and reliability. It must consider the following points:

- Orbit selection - 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 orbit inclination has to constitute from two perspectives: collision avoidance (the number of satellites deployed in existing orbit inclinations) and reducing the probability of SEUs.
- Frequency selection - It has to be based on both the business type and usage scenarios. THz and laster communications are better choices than the K-band cause of alleviating the problem of inter-frequency interference.
- Waveform selection - SS waveforms remain the most competitive. MC-DSSS has the feature of flexible sub-carriers allocation to mitigate the inter-frequency interference between systems by combining with cognitive radio (CR).
- Considerations before design: on-board processing is more secure than transponder - The onboard processing system avoids eavesdropping behavior. By using the onboard processing system, it can achieve global coverage by relying on ISLs, and only a few ground segments are needed for stable operation. However, complex encryption algorithms can process in the ground segment but

not in the space segment because LEO satellites are typically resource-limited satellites and tend to require lightweight and low-power solutions.

After selecting the satellite orbits, the frequencies and the waveforms, Fig.6 illustrates the secure and reliable LEO SCSs design. For the uplink, advanced security-oriented antennas are used to mitigate eavesdropping and jamming. By combining signals from each satellite, the integrity of the combined signal is improved, allowing terminals to transmit at reduced power, thus enhancing security.

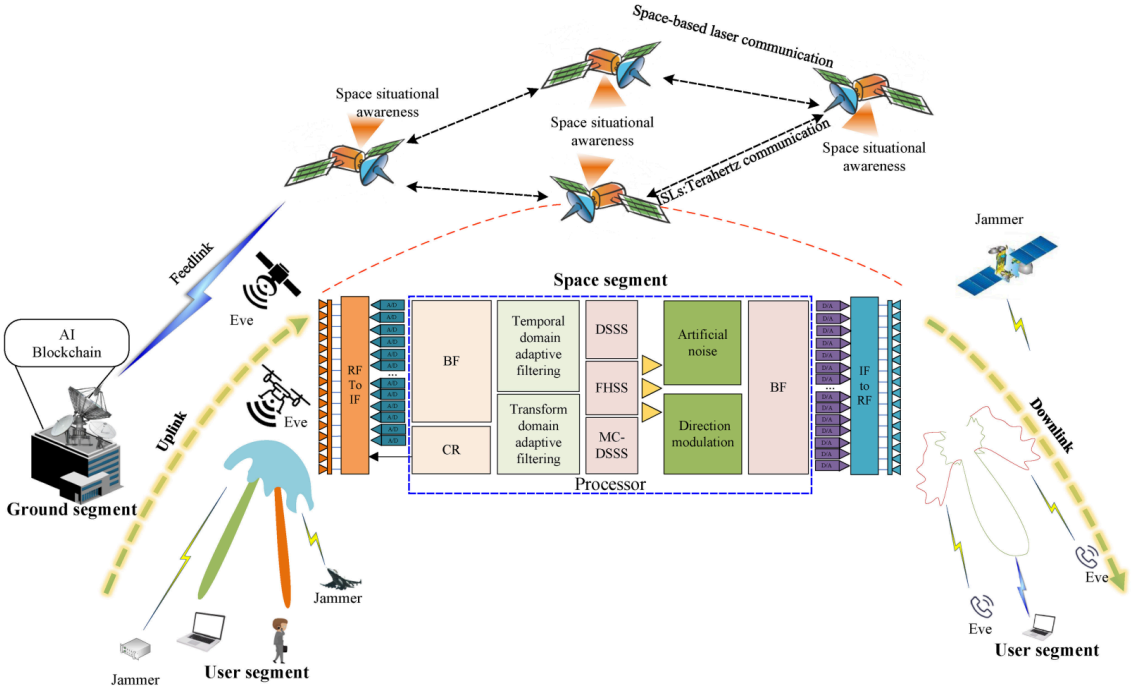

Figure. 6. Design guidelines of secure and reliable LEO SCSs.

For the downlink, advanced antennas and artificial noise are employed to counter eavesdropping and jamming, with the aid of Reconfigurable Intelligent Surfaces (RISs) to adjust signal amplitude and phase. The space segment processors need to be radiation-resistant to minimize errors. The ground segment manages operations and control for the entire LEO SCS, while users must regularly update patches and cooperate with the space segment by adjusting frequency or power to reduce attack risks and manage interference.

7. Summary

To be concluded, Low Earth Orbit Satellite Communication Systems (LEO SCSs) offer global coverage with low latency but face significant security and reliability challenges. These include eavesdropping, denial of service (DoS) attacks, collisions, and single-event upsets (SEUs). This paper provides an overview of these issues, discusses their characteristics, and suggests solutions for enhancing security and reliability. It also highlights areas for future research, such as ISAC-aided secure transmission and CV-aided space communication, and provides design guidelines for secure LEO SCSs.

Table IV
List of Acronyms

Acronyms	Definitions
6G	Sixth-generation wireless
AI	Artificial Intelligence
CCI	Co-Channel Interference
CR	Cognitive Radio
DDoS	Distributed Denial of Service
DL	Deep Learning
DoS	Denial of Service
FDA	Frequency Diverse Arrays
FFHSS	Fast Frequency Hopping Spread Spectrum
FHSS	Frequency Hopping Spread Spectrum
GEO	Geostationary Earth Orbit
GPS	Global Positioning System
IDS	Intrusion Detection System
IoRT	Internet of Remote Things
IoT	Internet of Things
ISAC	Integrated Sensing and Communication
ISL	Inter-Satellite Links
LEO	Low Earth Orbit
MC-DSSS	Multicode Direct Sequence Spread Spectrum
MEO	Medium Earth Orbit
ML	Machine Learning
NCC	Network Control Center
QKD	Quantum Key Distribution
RIS	Reconfigurable Intelligent Surface
UAV	Unmanned Aerial Vehicle
SCS	Satellite Communication System
SEU	Single Event Upset
SIN	Space Information Network
SS	Spread Spectrum
SSA	Space Situational Awareness
THz	Terahertz
THSS	

References

P. Yue *et al.*, "Low Earth Orbit Satellite Security and Reliability: Issues, Solutions, and the Road Ahead," in *IEEE Communications Surveys & Tutorials*, vol. 25, no. 3, pp. 1604-1652, third quarter 2023, doi: 10.1109/COMST.2023.3296160