Analysis on the Security of Satellite Internet

Huan Cao¹, Lili Wu², Yue Chen², Yongtao Su¹, Zhengchao Lei²(✉),
and Chunping Zhao³

¹ Beijing Key Laboratory of Mobile Computing and Pervasive Device, Institute of Computing
Technology, Chinese Academy of Sciences, Beijing 100190, China
caohuan@ict.ac.cn

² National Computer Network Emergency Response Technical Team/Coordination Center
of China, Beijing 100029, China
leizhengchao@cert.org.cn

³ Beijing Sylincom Technology Co., Ltd., Beijing, China

Abstract. Satellite Internet (SI) is a new way to provide internet access all over the world. It will bring great convenience to international communication. Compared with the traditional communication networks, SI has a significant change in network architecture and communication model, which will have an important impact on national information network security. For example, the global interconnected SI consists of a large number of small satellites and each satellite has multi-beams to cover a vast area, which leads to the disorderly flow of information across the border, and greatly increases the difficulty of network protection. Therefore, it is necessary to closely track the development of SI and analyze security problems brought by SI. In this paper, we analyze the security risks of SI from the perspective of national security, network security and equipment security, and thirteen security issues have been summarized to provide reference for the healthy development of SI industry.

Keywords: Satellite internet · Network security

1 Introduction

In recent years, the world's space powers have proposed low-earth-orbit (LEO) satellite constellation plans, which has triggered a boom in satellite internet (SI) development. Concerning the development of SI, the white paper published by China Center for Information Industry Development (CCID) points out that the world is on the eve of the dense launch of man-made satellites [1]. It is estimated that the low Earth orbit (LEO) satellites will deploy a total of about 57000 by 2029. A space resource race of satellite orbits is quietly beginning, countries all over the world have joined in the space race of SI, and the earth surface will be covered by a large number of LEO satellites intensively. Therefore, security problems brought by this will become a new challenge [2–4]. With the construction of SI becoming a national strategy all over the world, the industry has entered a period of rapid market growth [5, 6], and it specifically reflected in the following aspects:

- Fighting for frequency and orbit resources: The competition for frequency and orbit resources among countries has become increasingly white-hot. According to the data submitted to international telecommunications union (ITU), satellite companies in France, United States and United Kingdom have the largest number of resources such as key frequency bands and orbital heights. For example, OneWeb has submitted at least seven materials of network resources to ITU, including THEO, STRIPE, 102, etc., covering 8425 km / 8575 km, 1200 km and other medium and low orbital altitude, as well as Ku / Ka / V and other frequency bands; SpaceX submitted twelve materials to ITU, including usasat-ngso-3a-r / 3b-r / 3C, 3D / 3E / 3F / 3G / 3H / 3I, usasat-ngso-3j / 3K / 3l, covering 345.6–1325 km orbital altitude and Ku / Ka / V frequency bands.
- Large-scale network deployment: SI constellation construction has entered the stage of large-scale network deployment. SpaceX plans to launch 42000 satellites, and 482 broadband Starlink satellites have been launched by June 5, 2020. In addition, OneWeb has launched 74 satellites in the past two years [7].
- International operation: The service providers of SI have been striving for landing rights in countries around the world. For example, OneWeb initially obtained market access authorization in about 19 countries in 2019.

SI can be mainly used for emergency rescue, rural and remote area coverage, maritime market (including cruise ships, merchant ships, fishing boats, yachts, etc.), aviation market, military and government applications [8]. Compared with the terrestrial mobile communication system (TMCS), the SI will face the following new security challenges:

- Due to the limited computing and storage capacity, the satellites in SI constellation don't support high-complexity encryption protocols and algorithms, resulting in the weak protection of traffic data.
- The topological structure of the LEO satellite networks are constantly changing, the openness of the satellite's orbit makes it very difficult to be supervised.
- Communication satellite is a highly integrated product, its components are supplied by many manufacturers. There may be security holes and design defects in all aspects of integration. Especially, the technology of on-orbit satellite reprogramming is not mature, which makes it very difficult to make up for the security holes of on-orbit satellites.
- Satellite communication has the characteristics of wide coverage [9], which can broadcast data to a large number of user terminals in a large range. When the SI network is attacked, the impact is greater than that of the TMCS, so it is easier to become the target of hackers.

In summary, the security problems faced by the SI are more severe than those of the TMCS. If the SI is attacked, it will have a wider range of influence and cause greater damage. Therefore, it is necessary to carry out the research on the security problems faced by the SI.

2 Related Work

The research on the security problems of SI is still in its infancy. 3GPP puts forward the network architecture of non-terrestrial networks (NTN) [10], but there is no systematic analysis on the security problems of NTN. Sat5G analyzes the security threats of the integration of satellite network and 5G networks, mainly including the following three main aspects [11]:

1. Security threats of satellite connections as transport network for backhaul
One of the main security threats perceived by the terrestrial network is the tampering or eavesdropping of the data transmitted (the control plane signaling or the user plane data) over the backhaul connection. In addition, another threat perceived by terrestrial networks in case of sharing of the satellite network is the tampering and eavesdropping of traffic via the shared network.
2. Security threats of satellite connections as transport network among 5G core networks
In this case, the two terrestrial networks usually are not in the same trust domain, and the intermediate satellite network is not considered to be part of the trust domain of either of the two terrestrial networks. At the same time, it is very common for satellite networks to be shared among multiple terrestrial networks. The security threats perceived by the terrestrial network are tampering, eavesdropping and unauthorized traffic redirection (i.e. traffic ‘hijacking’) [12, 13].
3. Security threats to content delivery via satellite

Security threats related to content delivery networks (CDN) are DDOS at-tacks; Content leakages, such as unauthorized access to content, which is aggravated by local caching and the use of MEC servers; Deep linking, in this case, all media slices can be accessed by accessing a manifest file due to use MPEG DASH.

However, Sat5G has made a preliminary analysis of the security issues of SI, but it is not comprehensive enough. This paper summarizes and analyzes the security issues faced by SI in the future from the aspects of national security, network security and equipment security based on the existing research.

3 Analysis of SI Security

3.1 Overview of Security Issues of SI

The system architecture of SI can be divided into user segment, space segment and ground segment. The user segment includes various satellite terminals; the space segment includes satellite constellation [14], which can be divided into constellation with inter satellite link (ISL) and constellation without ISL [15]; the ground segment includes gateway station (GS), operation management and control system (OMCS), measurement and control system (MCS), network management system (NMS), etc. According to the characteristics of SI, the possible security problems in SI are summarized in Table 1.

Table 1. Security issues of SI.

Classification	ID	Security problem	Description
National security	(1)	National and military security threats	<ul style="list-style-type: none"> • Illegal organizations can steal strategic information of target countries by deploying earth observation payload on LEO satellites • LEO satellite provides communication platform for future information warfare weapons
	(2)	Frequency and orbit resource preemption	To occupy limited orbit resources by planning LEO satellite constellation
	(3)	Interference in astronomical exploration	The launch of a large number of LEO satellites can cause serious interference to astronomical observation
Network security	(4)	Identity impersonation	<ul style="list-style-type: none"> • Disguised as a satellite terminal (ST) to access the SI and destroy the network • Disguised as a satellite to trick legitimate STs into accessing a false network to obtain the ST's location or identification information
	(5)	Data eavesdropping	Illegal organizations illegally receive and analyze transmitted traffic data or signaling data through wireless links (feedback link, user link, ISL)
	(6)	Data integrity issues	Modify, insert, replay, delete user or signaling data to destroy data integrity
	(7)	Information interception	Illegal interception of user location or identification information transmitted by ST through wireless links
	(8)	Signal interference	Attackers interfere with satellite wireless links by emitting high-power electromagnetic waves
	(9)	Denial of service	Interfere with satellite or gateway, and interfere with data or signaling physically or by protocol, which makes SI unable to provide normal services for legitimate ST
	(10)	Anonymous attack	Attackers attack the satellite node in space, but the satellite cannot determine the attackers

(continued)

Table 1. (continued)

Classification	ID	Security problem	Description
Equipment security	(11)	Malicious occupation of satellite bandwidth resources	Sending illegal signals to the satellite through wireless link, because the satellite will not check the legitimacy of the signals, so the illegal signals will occupy the bandwidth resources of the satellite
	(12)	Malicious satellite control	By issuing malicious instructions or injecting viruses to satellite nodes from ground facilities or space to achieve the goal of controlling satellites
	(13)	Malicious consumption of satellite resources	Malicious consumption of satellite propellant resources to achieve the goal of reducing satellite life

The distribution of the above thirteen security issues in the SI is shown in Fig. 1.

Fig. 1. The distribution of security issues in SI system

3.2 National Security Issues

National and Military Security

The security threats include national strategic information security and military security threats.

National Strategic Information Security

SI involves a large number of satellites, and the orbit altitude is concentrated between 300 km and 2000 km. If the corresponding satellites equipped with high-resolution scanning observation payloads, such a large number of satellites will expose the important military infrastructure of countries all over the world and threaten national security. Recently, earth observation industry (EOI) company is promoting the development of a new very low earth orbit (VLEO) satellite constellation. Its propulsion system and innovative design will enable the satellite to run in a very low orbit. In order to support continuous monitoring service, the initial constellation consists of 30 satellites with an average revisit time of two hours. The company plans to launch its first satellite by the end of 2022. EOI company's mission is to enable defense and intelligence agencies and commercial customers to easily access ultra-high resolution images at affordable prices to support a range of applications such as resource management, environment and disaster assessment, asset monitoring, logistics planning, infrastructure mapping, public security, homeland security, insurance and real estate. For example, Fig. 2 shows the image of naval ship captured by EOI company's VLEO satellite.

Fig. 2. Image of naval ship captured by EOI's VLEO satellite

Military Security Threat

1. The low cost and high launch success rate (LSR) of SI will pose new challenges to the technical field of anti-satellite weapons.

The existing kinetic energy anti-satellite weapons (KEAW) rely on the momentum of high-speed moving objects to destroy the target, which has a strong lethality for satellites with high cost and low LSR. However, for the large-scale and low-cost SI, traditional KEAW are facing many challenges. Taking Starlink constellation of SpaceX as an example:

- a. The traditional KEAW are all disposable. It means that a large number of KEAW need to be manufactured and maintained to deal with the threat of the Starlink constellation of 42000 satellites, and the cost will be astronomical.
 - b. The traditional KEAW adopts the hard-kill method. The method will generate a large number of space debris, which may hit more satellites, causing uncontrollable and irreversible chain reaction, making the whole earth surrounded by satellite debris.
 - c. If we give up the hard-kill method and study more advanced weapons such as soft-kill method, it will cost a lot of money to tackle key technical problems, and the development cycle will very long.
2. The cooperative operation of SI and drone swarm will pose great challenges to the national defense system.

With the accelerated evolution of the war form, a large number of intelligent equipment appear in the war. As an important part of intelligent warfare, Unmanned Aerial Vehicle (UAV) cluster warfare poses great challenges to the traditional defense system. However, the UAV cluster warfare relies on the communication link among each UAV to achieve real-time information interaction, and also relies on the control system to achieve collaborative command, so the overall viability and combat ability of the UAV cluster depends on the security and controllability of the communication link and control system. If the communication link or the control system is jammed by enemy, the UAV cluster will likely to be completely annihilated. Starlink constellation can make up for this defect, it can provide large bandwidth, low delay and wide coverage communication services through a large number of LEO satellites without being affected by any terrain and climate. It can help the UAV cluster get rid of the dependence on land-based communication system, and significantly improve the overall combat effectiveness of the cluster through flight control, situation awareness, information sharing, target allocation and intelligent decision-making, which makes it more difficult for the national defense system to deal with the threat of UAV cluster warfare.

Frequency and Orbit Resource Preemption

According to international regulations, all countries have the right to explore outer space peacefully. Radio frequencies and satellite orbits are limited natural resources and must be used equally, reasonably, economically and effectively. Effective interference control mechanisms should be adopted to make full use of frequency and orbit resources. Effective interference control mechanisms should be adopted to make full use of the limited resources. According to the ITU rules [16], orbit resources are mainly allocated in the principle of first come, first served, and the later declarers cannot cause adverse interference to the satellites of the first declarers. The LEO constellation system should not only launch the satellite in accordance with ITU regulations, but also provide relevant services to the public in accordance with the specified time and proportion, so as to legalize the frequency usage. In other words, the development and utilization of LEO constellation can not only occupy the limited space resources of LEO satellite, but also help to seize the priority use right of spectrum, which has an important impact on the channel use range of battlefield communication.

Generally, at the end of a geostationary earth orbit (GEO) satellite's life, it will increase more than 200 km by using its final energy and enter the grave orbit to complete its self-destruction, so as to release the original working orbit. But the LEO satellite communication system is different, it needs many small satellites to maintain a complete network to provide communication services. When some small satellites cannot work normally or reach the end of their life, it is necessary to launch new satellites to supplement the network, so they will always occupy the frequency and orbit resources. However, the near earth orbit resources can only hold about 60000 satellites, the United States, the United Kingdom, France, Canada, Norway, the Netherlands and other countries have taken the lead in the deployment of SI. SpaceX alone plans to launch 42000 LEO satellites, which will further compress the available orbit resources of other countries.

In addition, all countries except the United States have gaps in the supervision technology of SI, and corresponding laws are not perfect. Once the design and construction of SIs are completed, it will lead to difficulties for countries to effectively supervise the communication services provided by SI, leaving huge security loopholes.

Interference in Astronomical Exploration

Due to the huge scale of SI constellations, astronomical observation will become more difficult as small satellites in constellations are launched one after another. Starlink will launch 42000 satellites, with an average of about 400 satellites observed at any time and at any place. Although they are invisible to the naked eye in orbit, they have a great influence on the astronomical research of optical, infrared and radio telescopes, and are easy to leave traces in the astronomical images. The large-scale integrated Sky Survey Telescope (such as China sky eye) will be greatly affected, which will reduce our ability to observe and warn near Earth Asteroids.

In addition, LEO constellations have the most interference for astronomers who detect dark matter and dark energy, because the signals detected by related instruments are very weak. A large number of LEO satellites will interfere with the space observation of various countries to a certain extent when passing over them, and affecting the corresponding research.

3.3 Network Security Issues

Identity Impersonation

Due to the lack of identity authentication mechanism in SI's user link, feedback link and ISL, there are three problems of identity impersonation in the following aspects:

1. If the transmission mechanism adopted by the communication system is public, the attacker can calculate the uplink signal according to the downlink signal of the satellite, and then use the satellite communication equipment to disguise as a legitimate ST to access the network and illegally obtain network services.
2. The attacker disguised himself as a satellite network and induced legal STs to access the satellite network to obtain relevant user identification information and location information.
3. The attacker disguised himself as adjacent satellites in the same orbit or different orbit to induce the target satellite to establish an ISL with it, so as to obtain the relevant data transmitted by the ISL.

Data Eavesdropping and Data Integrity Attack

Due to the openness of wireless communication of user link, ISL and feed link of SI, the data transmitted through satellite network can be easily eavesdropped. In addition, data encryption will increase the cost of satellite terminal equipment and reduce the utilization rate of satellite link resources. Many satellite communication networks do not encrypt the transmitted data, so it is very easy to cause data leakage.

The most possible attack methods are as follows:

1. The attacker uses a kind of satellite data receiving card to steal data, which is similar to the computer network card with low cost.
2. The attacker makes use of retired equipment abandoned by manufacturers to perform network attacks.
3. The attacker can use the VLEO or LEO satellite in the overseas satellite constellation to eavesdrop the service data on the user link and feeder link of the domestic satellite system.
4. If the satellite constellation built in a country has an ISL, which uses microwave communication, the attacker can control the foreign satellite to approach the target satellite as close as possible to implement data eavesdropping.

Data eavesdropping is often combined with data integrity attack. The attacker often implements data eavesdropping, then inserts, modifies, falsifies the stolen data, and finally send it to the data receiver to achieve the purpose of destroying data integrity.

Information Interception

If the orbit of a foreign satellite is lower than that of a domestic satellite (for example, the lowest orbit of SpaceX is about 300-500km), the attacker can use the attack means similar to the terrestrial pseudo base station to carry out network attack. For example, the

torpedo attack method in 4G system can be used in SI, the attacker can use legitimate ST to launch multiple paging to the attacked ST, and this will expose the user identification information, which can be intercepted by the LEO satellite and terrestrial equipment owned by the attacker, so as to track the user's location and bring great security threat.

Signal Interference

This kind of attack is the most common but effective, and it is often used in wars. Interference can be divided into blocking interference and noise interference. Strong interference signals will cause the satellite to be unable to receive the signal normally and provide the service for the legitimate ST.

The possible attack methods are as follows:

1. If the orbit of the overseas satellite is lower than that of the domestic satellite, the attacker can deliberately transmit signals on the working frequency band of the feeder link, user link or ISL of the domestic satellite system to cause interference or interruption of the domestic satellite service.
2. Satellite transponders can be divided into on-board processing transponders and bent-pipe transparent transponders. On-board processing transponders can rely on channel coding, advanced modulation technology, spread spectrum technology, coherent intermodulation product cancellation, etc. to resist interference attacks. But the bent-pipe transponder has a simple structure and does not process any communication signals, so it is easy to encounter signal interference attack. Attackers can interfere with satellites by transmitting signals from high-power transmitters.

Denial of Service

The attack mode against terrestrial network is also applicable to satellite network, such as DDoS attack. Attackers make use of software to simulate massive satellite terminals to send legitimate and bogus requests, which leads to the failure of satellites to provide effective services to legitimate STs. This kind of attack is difficult to defend due to the diversity of satellite communication links. Each ST's client has a receiving and transmitting system. If the transceiver fails to get effective processing when it has problems, it will lead to unstable connection and generate a large number of connection requests. In addition, access requests will also increase greatly when satellite links suffer from signal fading caused by severe weather. However, satellites cannot blindly defend these requests, and the system design of satellite system will not defend these requests as well as the network firewall. Because satellites cannot distinguish whether these requests come from legitimate STs or malicious attackers, which leads to denial of service problems.

Anonymous Attack

Space belongs to the global commons and has no national boundaries. Therefore, it is possible for attackers to launch anonymous attacks against the target satellite in space. Moreover, it is difficult for the attacked satellite to determine and trace the attacks due to the long distance and limited information. On the one hand, there are many factors that lead to satellite failure, such as changes in space environment, design defects, device

problems and even debris effects. Attacks are not the only reason for the failure of satellites in orbit. On the other hand, it is difficult for the ground station to accurately judge what is happening in space limited by distance, meteorology, technical capability and other conditions. The combined effect of these factors enables the attacker to find reasonable excuses to deny the attack.

Malicious Occupation of Satellite Bandwidth Resources

Satellite is a typically resource limited system, on-board computing resources, wireless resources are very scarce, so they are not suitable for complex communication payloads. Most of the on-orbit satellites adopt the bent-pipe transponder without signal unpacking, so it is not possible to determine whether the received data is from a legitimate user. When the attacker sends his own illegal signal, the satellite will still forward the signal to the GS. At this time, if the attacker builds a receiving system to demodulate, decode the data and extract useful data, the purpose of privately communicating with the aid of the satellite is achieved, and a complete method of stealing satellite resources is formed. Moreover, attackers will use their own encryption algorithm to effectively encrypt communication data.

3.4 Equipment Security Issues

Malicious Satellite Control

Due to the lack of network security standards for commercial satellites, coupled with the complex supply chain of satellites, satellite manufacturing uses ready-made technologies to maintain low cost. The wide availability of these components means that hackers can analyze their security vulnerabilities. In addition, many components use open source technology, and hackers may insert backdoors and other vulnerabilities in satellite software, making satellites vulnerable to security risks that are maliciously controlled by attackers.

The means to control the satellite maliciously are as follows:

1. The attacker can capture the target satellite in space and drag the captured satellite out of the working orbit, causing the whole satellite constellation unable to provide continuous services. Moreover, the attacker can inject virus into the captured target satellite after it has been dragged off the working orbit, and then it will be pushed back to the working orbit, causing the virus to spread throughout the whole SI. The technology of capturing on-orbit satellites is already available and has been used in the service of extending the life of on-orbit satellites in orbit. Once this technology is used by hackers, the target satellites can be captured arbitrarily.
2. Satellites are usually controlled by the GSs. These stations are vulnerable to the same network attacks as computers. Although the satellite control attack is not as simple as stealing other people's email, but it can be realized. If there are security loopholes that can be exploited by hackers in the GS, the hackers may invade these stations, and then they can send malicious instructions to control the satellite, or they can use special tools to trick the satellite, and finally achieve the purpose of attacking the SI. For example, the attacker can carry out further attacks after controlling the target

satellite: the attacker can use the broadcast channel of the target satellite to send a large amount of garbage data or spread viruses to the whole SI; shutting down the target satellite to make it unable to provide normal services; if the hackers control the target satellite and it has a propeller device, they can change the orbit of the satellite and hit it on the ground, other satellites or even the international space station.

Malicious Consumption of Satellite Resources

Attackers can also directly affect the life of satellites by consuming propellants, depleting the write life of charged erasable programmable read-only memory (EEPROM) and other attacks.

4 Conclusion

The rapid development of SI has brought some security risks. On the one hand, we should actively develop SI industry, giving full play to the unique advantages of SI, which is not affected by geographical obstacles and disasters; on the other hand, in view of the different levels of security threats faced by SI, it is necessary to carry out forward-looking research on the satellite network security, so as to fill in the regulatory gaps.

Acknowledgement. This research was supported by GF science and technology foundation enhancement program, National computer network and information security management center (XDA-Y07-02).

References

1. CCID. research on the development of China's satellite Internet industry. In: CCID. <https://zhuanlan.zhihu.com/p/144513640> (2020)
2. De Azúa, J.A.R., Calveras, A., Camps, A.: Internet of Satellites. IoSat), Analysis of Network Models and Routing Protocol Requirements. (2018)
3. Su Y., Liu Y., Zhou Y., Yuan J., Cao H., Shi J.: Broadband LEO Satellite Communications: Architectures and Key Technologies (2019).
4. Cao H., Su Y., Zhou Y., Hu J.: QoS Guaranteed Load Balancing in Broadband Multi-Beam Satellite Networks (2019).
5. Anpilogov V.R., Gritsenko A.A., Chekushkin Y.N., Zimin I.V.: A Conflict in the Radio Frequency Spectrum of LEO-HTS and HEO-HTS Systems (2018).
6. Tong, X., et al.: Normalized Projection Models for Geostationary Remote Sensing Satellite: A Comprehensive Comparative Analysis (January 2019). IEEE Trans. Geosci. Remote Sens. **57**(57), 9643 (2019)
7. Foust J.: SpaceX's space-Internet woes: Despite technical glitches, the company plans to launch the first of nearly 12,000 satellites in 2019 (2019).
8. 3GPP: Study on using Satellite Access in 5G. TR 22.822 (2018). <https://3gpp.org/DynaReport/38-series.htm>.

9. Sacchi, C., Rossi, T., Murrioni, M., Ruggieri, M.: Extremely High Frequency (EHF) Bands for Future Broadcast Satellite Services: Opportunities and Challenges. *IEEE Trans. Broadcast.* **65**(65), 609 (2019)
10. 3GPP.: Solutions for NR to support non-terrestrial networks (NTN). TR 38.821 R16 (2018). <https://3gpp.org/DynaReport/38-series.ht>.
11. Sat5G. Extending 5G Security to Satellites. D4.5 (2019). <https://www.sat5g-project.eu/public-deliverables>.
12. 3GPP.: Security architecture and procedures for 5G system. TS 33.501 (2019). <https://3gpp.org/DynaReport/33-series.htm>.
13. 3GPP.: System Architecture for the 5G System (5GS); Stage 2. TS 23.501 (2019). <https://3gpp.org/DynaReport/23-series.htm>.
14. Jiang J., Yan S., Peng M.: Regional LEO Satellite Constellation Design Based on User Requirements (2018).
15. Xia S., Jiang Q., Zou C., Li G.: Beam Coverage Comparison of LEO Satellite Systems Based on User Diversification (2019).
16. ITU.: Radio Regulations 2016 Edition (2016).

Open Access This chapter is licensed under the terms of the Creative Commons Attribution 4.0 International License (<http://creativecommons.org/licenses/by/4.0/>), which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.