Security Threat Analysis and Corresponding Countermeasures for HTS Communication System

Yongchun Ma*, Deyun Yang2, Depeng Zhang1, Hailin Wu1, ChaoRan Li1 and Qianqian Du1
1 Space Star Technology Co., Beijing, 100086, China
2 China Academy of Space Technology, Beijing, 100086, China
*Corresponding author’s e-mail: maych@space.star.com.cn

Abstract. In recent years, satellite communication has been widely used in various fields. With the increase of the satellite communication business, the requirement for information security is stronger. System security plays a significant role in the HTS communication system. First, this article gives a brief description of the HTS communication system, introducing the composition and characteristics of the system. Then, the security threats to the HTS communication system are analysed in three aspects: physical security threats, operational security threats and data security threats. Finally, the corresponding countermeasures for security threats are put forward, which can enhance the overall security level of the HTS communication system.

1. Introduction
In recent years, with the research and development of advanced technology, satellite communication has entered the stage of rapid development which plays an important role in the next generation of communication. However, the present satellite communication systems cannot meet the needs of higher transmission rate and larger system capacity. Therefore, the High Throughput Satellite (HTS) communication system has been developed to satisfy the needs of higher transmission rate and larger system capacity [1-3].

The HTS communication system adopted many advanced technologies, such as multiple spot beams and frequency reuse. Under the situation of using the same amount of satellite spectrum, the HTS communication system provides greater capacity than a traditional satellite communication system. The capacity of system increases several times or dozens of times, which greatly increases the transmission rate and reduces the cost of satellite bandwidth [3-5]. At present, China has two high throughput satellites, namely ChinaSat 16 and APSTAR-6D. ChinaSat 16 user beams operating in Ka frequency band. APSTAR-6D user beams operating in Ku frequency band.

With the promotion of the HTS communication system, the security issues have become increasingly complicated and prominent. Satellite link has the characteristics of long distance transmission, wide coverage and complex environment. Compared to other transmission media, such as optical fiber cable and digital microwave link, the satellite link is vulnerable to various attacks [6]. Meanwhile, the HTS communication system has the characteristics of resource-constrained, large propagation delay and dynamic topology [2]. Safety protection technologies for the traditional communication system are not completely applicable for the satellite communication system.
Therefore, we should research and analyse corresponding countermeasures for security threats according to the characteristics of the HTS communication system.

2. HTS communication system overview

2.1. System composition
The HTS communication system consists of space segment, ground segment and user segment. The space segment includes GEO satellites, MEO satellites and LEO satellites, which provide ground segment and user segment with communication links. The ground segment includes satellite gateway and operating center. The satellite gateway provides access service for user beams correspond to the feeder beam, which has the following functions: signal transmitting and receiving of feeder link, baseband processing and data exchanging with operating center. The operating center is the center of system management, satellite data processing and data exchange, which plays a significant role in the HTS communication system. It has the following functions: business operation support, network management and connection to the Internet and 4G/5G network. The user segment includes stationary terminals, portable terminals and mobile terminals. The antenna dimension of terminals are in the range 0.45 to 1.2m [7-9].

2.2. System characteristics

2.2.1. Satellites are open and exposed in space.
In the HTS communication system, representative satellites move in geosynchronous orbits about 36000 km above the earth. Satellites are located in a harsh space environment, and are vulnerable to illegal interception, interference and destruction. Due to lack of reasonable and effective protection methods, satellite-ground link is very susceptible to various interferences, such as malicious electromagnetic radiation, atmospheric electromagnetic radiation and cosmic rays.
2.2.2. The limited bandwidth resources.
Although the HTS communication system has bigger communication capacity than a traditional satellite communication system, which can meet various business requirements. The bandwidth resources are still very valuable since satellite transponders are resource restricted. Satellites are mainly affected or restricted by power supply, memory space and computational ability, which have limited data processing capacity [7].

2.2.3. Large propagation delay and high bit error rate of channel.
Propagation delay is a measure of the necessary time for signals to propagate from the Earth sender to the Earth receiver. The propagation delay for geosynchronous satellites is about 270 milliseconds. Compared to the ground communication system, the HTS communication system has a larger propagation delay. In addition, satellites in a harsh space environment for the HTS communication system made more rigorous requirements. Satellite links include uplink and downlink are easily influenced by rainstorms, snowstorms and sunspot activities etc. Hence, the bit error rate of the HTS communication system is higher than the ground communication system.

2.2.4. Highly dynamic network topology.
The HTS communication system has a complex and dynamic structure, which consists of a large number of terminals. These terminals have the features of wide distribution, high mobility and long distance between sender and receiver. With the joining and exiting of terminals, the structure is constantly changing, so network maintenance becomes difficult and complicated.

2.2.5. The asymmetry of forward link and reverse link.
The HTS communication system dynamically changes the forward link and reverse link based on business requirement. The information rate of forward link can reach 10 Mbps to 100 Mbps. But, the information rate of reverse link is probably only 1 Mbps [8].

3. Security threat analysis

3.1. Physical security threats

3.1.1. Physical damage.
Physical damage refers to tangible injury to infrastructure, including satellites, gateways, the operating center, etc. There are lots of uncontrollable factors in the natural environment, such as sunspot activities, floods and earthquakes. These infrastructures are under threat and damage from unexpected natural activities. The normal running of the HTS communication system could be influenced by a variety of unexpected natural activities, which will cause the system to interrupt, the appearance of serious results. Besides, the operating center as the data exchange and processing center, if one of the operating center devices is destroyed, the whole system might have been paralyzed.

3.1.2. Affected by natural environment.
The communication quality of satellite links affected by natural environment sun outages, eclipses, rainstorms and snowstorms have a deleterious effect. We should pay close attention to the impact of rainstorms and snowstorms on the HTS communication system. Rain attenuation is the significant determinant that influences the quality of transmission in satellite link with Ku band and Ka band. In the HTS communication system, the higher frequency tends to be more easily influenced by rain attenuation. This is because with the increase of operating frequency, the wavelength decreases, giving raindrops more scattering and absorption abilities to the signal.
3.1.3. Signal interference.
Signal interference means satellite links are influenced by natural or artificial electromagnetic disturbance. The HTS communication system works in a complicated electromagnetism environment, and is vulnerable to malicious electromagnetic radiation, atmospheric electromagnetic radiation and cosmic rays. The signal interference is composed mainly of deceptive jamming and suppression jamming. The deceptive jamming is an electronic countermeasure technique that generates forged signals to confuse users. The suppression jamming refers to the satellite signal that is interfered by high power noise in the same frequency band, which will cause the reduction of signal noise ratio [10].

3.2. Operational security threats

3.2.1. Illegal access.
Some terminals in the HTS communication system have the features of access and quit dynamically. It is possible that the identity of legal terminal is faked by illegal users. This could lead to some serious security risks. For example, the operating center or the NMS is operated by an illegal user, which will cause system exception, even system paralysis.

3.2.2. Replay attack.
Replay attack is where the satellite channel data is intercepted by unauthorized users and fraudulently replayed or delayed back to the receiver. The replay attacks in HTS communication system allow intruders to impersonate real users. These attacks cause breaches of system security, which lead to reduced network availability.

3.2.3. Denial of service attack.
Denial of service attack is composed of bandwidth consumption attack and connectivity attack. The bandwidth consumption attack seeks to consume limited bandwidth resources, which will make available bandwidth resources depleted, such that legitimate requests cannot arrive at their destination. The connectivity attack aims to reduce system connectivity through huge amounts of connection requests, which will make available computing resources depleted, such that legitimate requests cannot handle.

3.2.4. Malicious program attack.
The HTS communication system has many vulnerabilities, such as security vulnerability and invalid configuration. Malicious programs execute unauthorized activities on the HTS communication system. These malicious programs include lots of particular types of attacks such as worms, Trojan horses and other viruses that could lead to system exception. The HTS communication system can even be operated remotely by unauthorized users, which brings major security threat [11-12].

3.3. Data security threats

3.3.1. Forged or modified routing information.
In the routing process, satellite data is confronted with all sorts of threats, especially forged attack and modified attack. On the one hand, illegal users can fake the identity of legal users joining the network, which will result in data transmission exception and data leakage of legitimate terminals. On the other hand, attackers can forge and modify routing information, which will generate vast amounts of invalid routing information. Hence, with the increase of network overhead and propagation delay, the network performance will be seriously degraded.

3.3.2. Forged or modified network control instructions.
Attackers can forge network control instructions, which causes interference to the normal communication procedure of the system. They also can modify network control instructions, which
result in communication failure between the ground segment and the user segment. Furthermore, if an attacker changes configuration parameters of the NMS, the NMS can make the illegal users in working state quit the network.

3.3.3. Data theft.
During satellite data transmission, the information can be easily intercepted by illegal users, which includes instruction data and business data. If the instruction data is intercepted by intruders, they can maliciously modify the instruction parameter and cause system paralysis. If the business data is intercepted by intruders, which will cause data leakage.

4. Corresponding countermeasures

4.1. Countermeasures for physical security threats

4.1.1. Backup Design.
The satellite gateway and the operating center are data aggregation nodes in the HTS communication system. If they are breaking down or have been sabotaged, which will cause system paralysis. In order to improve the safety and reliability of the HTS communication system, the construction of dual hot-backup technique and redundancy backup technique are significant measures for guaranteeing the normal running of the data aggregation node.

4.1.2. The countermeasure of rain attenuation.
The influence of rain attenuation has been researched in recent years, but we still have no efficient method against rain attenuation. In order to reduce the influence of rain attenuation in the HTS communication system, designers should comprehensively consider the effect of rain attenuation when designing the whole system. To ensure reliable communication, we can adopt adaptive coding modulation (ACM) technology and automatic power control technology to improve the spectrum efficiency of satellites [11-12].

4.1.3. Anti-Interference Design.
Anti-Interference design plays a significant role in improving the robustness of the HTS communication system. Increasing the transmit power improves the signal strength of satellites, which can reduce the influence of suppression jamming in the HTS communication system. Adopting the frequency-hopping modulation technology and spread spectrum technology, which can reduce the influence of deceptive jamming in the HTS communication system. The frequency-hopping modulation technology has outstanding interference resistance capacity. The spread spectrum technology by extending the spectrum bandwidth to achieve anti-interference [10].

4.2. Countermeasures for operational security threats

4.2.1. Identity authentication and access control mechanism.
Identity authentication and access control are a significant part of the system security mechanism and an effective measure to protect the confidentiality, integrity and availability of the data, which check the legal identity of terminals and grant corresponding system authority. The identity authentication and access control mechanism can protect the system against transferring in unauthorized satellite spectrum, transferring with forged or modified IP address, accessing unauthorized services, replay attack and denial of service attack.

4.2.2. The secure control of interconnection between different network domains.
The HTS communication system can achieve interconnection with the Internet, mobile communication network and private communication network. In the process of data exchange between different network domains, the HTS communication system is vulnerable to malicious programs from other
network domains. The HTS communication system is facing various risks, which includes authorization identity is faked and legal users execute over authority. The secure control of interconnection between different network domains against worms, Trojan horses and other viruses from other network domains. Adopting the secure isolation technology of cross network and the data exchange technology of under authority control according to different security levels of network domains.

4.3. Countermeasures for data security threats

4.3.1. Application layer encryption.
Application layer encryption executes in application layer and encrypts various types of data flowing through applications. Date keeps encrypted until it arrives at the destination that holds the corresponding decryption key. Application layer encryption can defend data theft, users can choose different levels of encryption algorithm based on different levels of encryption requirement. Application layer encryption has the disadvantage that the source IP address and the destination IP address are not encrypted. It also increases the complexity of application, the implementation of encryption algorithm and the implementation of application function must be synchronized.

4.3.2. Satellite link encryption.
Satellite Link encryption is a reliable method to protect satellite links independently of other layers. In the HTS communication system, satellites have two forms of satellite link: uplink (the ground or user segment to the space segment) and downlink (the space segment to the ground or user segment). The satellite link encryption can protect uplink and downlink against data theft and unauthorized changes to the gateway. But, because the HTS communication system is restricted by limited bandwidth resources and also has the disadvantages of large propagation delay and high bit error rate of channel. We should adopt a lightweight algorithm according to the characteristics of satellite channels [13-14].

4.3.3. Network layer encryption.
Network layer encryption executes in network layer and encrypts every IP packet through the HTS communication system. The network layer encryption can protect the system against data theft and unauthorized changes to the operating center. Network layer encryption devices have a few strong advantages of excellent operability and scalability. Considering the characteristics of highly dynamic and complex network topology, the network layer encryption devices can connect to the original network architecture transparently, so that the cost of expanding can be dramatically reduced. The disadvantage of network layer encryption is that only the IP address of the user segment is encrypted, unable to encrypt the IP address in the routing process. Applying encryption at the network layer can cause protocol compatibility problems, such as network address translation (NAT) and TCP acceleration will be invalidated [15].

5. Conclusion
With the high rapid development of the HTS communication system, the role of system security is getting more and more significant. The article introduces the security threats to the HTS communication system from three aspects: physical security threats, operational security threats and data security threats. Focused on the characteristics of the HTS communication system, the countermeasures for security threats are discussed and analysed. The countermeasures for security threats adopt advanced technologies, such as backup design, adaptive coding modulation (ACM) technology, automatic power control technology, frequency-hopping modulation technology, spread spectrum technology, identity authentication and access control, encryption technology etc., which can remarkably enhance the security of the HTS communication system.
References

[1] Kaneko, K., Nishiyama, H., Kato, N. (2018) Construction of a flexibility analysis model for flexible high-throughput satellite communication systems with a digital channelizer. IEEE Transactions on Vehicular Technology, 67(03): 2097–2107.

[2] Sun, C.H., Zhang, J.S., Zhao, W.S., Xiao, Y.W. (2020) Comparative analysis of GEO and LEO broadband satellite communication system. Radio Communications Technology, 46(05): 505–510.

[3] Gao, X., Men, J.Z., Liu, X.B., Yao, L. (2020) The development and application exploration of high throughput satellite communication. Satellite Application, 08: 43–48.

[4] Meng, H., Song, J.H. (2018) Application and development of satellite communication in emergency communication. Science and Technology Review, 36(06): 40–46.

[5] Wang, C.T., Zhai, L.J., Xu, X.F. (2020) Development and prospects of space-terrestrial integrated information network. Radio Communications Technology, 46(05): 493–504.

[6] Li, F.H. (2015) Development trends of the information technology and cyberspace security. Chinese Journal of Network and Information Security, 1(01): 8–17.

[7] Pang, L.X., Li, J., Feng, J.Y. (2020) Development of high throughput satellite: a survey and review. Radio Communications Technology, 46(04): 371–376.

[8] Hui, T.F., Zhang, J., Liu, M.Y. (2021) Research on key technology of new generation high throughput satellite communication system. Space Electronic Technology, 18(04): 10–15.

[9] Wang, L., Zheng, J., He, C., Yan, X.F. (2021) Resource allocation in high throughput multibeam communication satellite systems. Chinese Space Science and Technology, 41(05): 85–94.

[10] Huang, L., Tang X.M., Wang, F.X. (2011) Anti-spoofing techniques for GNSS receiver. Geomatics and Information Science of Wuhan University, 36(11): 1344–1347.

[11] Shah, S.M.J., Nasi, A., Ahmed, H. (2014) A Survey Paper on Security Issues in Satellite Communication Network infrastructure. International Journal of Engineering Research and General Science, 2(06): 887–900.

[12] Vacca, J.R. (2013) Computer and Information Security Handbook. Morgan Kaufmann, Cambridge, Massachusetts.

[13] Liu, Y., Dong, Y., Li, Z.H. (2004) Discussion of data security about space-earth all-in-one networking and analysis of CCSDS SCPS. Chinese Space Science and Technology, 1: 31–36.

[14] Li, F.H., Yin, L.H., Wu, W., Zhang, L.J., Shi, G.Z. (2016) Research status and development trends of security assurance for space-ground integration information network. Journal on Communications, 37(11): 156–168.

[15] Zhang, Y.G. (2004) A multilayer IP security protocol for TCP performance enhancement in wireless networks. IEEE Journal on Selected Areas in Communications, 22(04): 767–776.