A Survey on Network Security issues in Space Internet

Cheng Gong and Tongwei Liu*
National University of Defense Technology, Changsha, China
{gongc_1106, ltw_5471}@163.com

Abstract

Space Internet, which integrates satellite communication networks, aerial networks, terrestrial networks, and marine communication networks, has been an emerging architecture and attracted intensive research interest during the past years. In consideration of its cooperation characteristics of multi-layer networks, open communication environment, and time-varying topologies, Space Internet faces many unprecedented security challenges. We provide a detailed survey of recent research works on network security issues in Space Internet in the aspects of security threats and defense countermeasures. To the best of our knowledge, we are the first to present the state-of-the-art of security for Space Internet, since existing surveys focused either on a certain segment or on several segments of the integrated network. We first briefly introduce the essential background and the view of the Space Internet, as well as discuss the related security challenges faced by the emerging integrated network architecture. Then, we present a comprehensive review of recent research works concerning network security issues in Space Internet, which we categorize by different research directions. Finally, several future challenges and the respective open research topics are described.

Keywords: space internet; integrated network; security

1 Introduction

With the development of mobile communication technology, especially the advance of the Internet of Things (IoT) and the commercialization of 5G in many countries around the world, traditional terrestrial networks can no longer meet the exploding demands on high-speed and reliable network access at anytime and anywhere on the earth, in consideration of its limited coverage and network capacity. This has aroused widespread concern in the academia and industry on the air-ground coordination and the space-air-ground integrated network. In particular, more and more organizations have released their plans on Space Internet such as the Global Information Grid (GIG), OneWeb, SpaceX, Kuiper, Hongyun, etc. Thanks to the inherent advantages in terms of large coverage, high throughput, and strong resilience, Space Internet can be used in lots of practical fields, including in-flight Internet, marine communication, satellite television, weather forecasting, navigation (GPS) and military communication, environmental monitoring, space research, and so on.

Following the prosperity of various wireless services provided by satellite communications, the security issue has raised growing concerns since the Space Internet is susceptible to being eavesdropped on by illegal adversaries in such a large-scale wireless network, a large number of research works have been published recently, which separately focused on the architecture of Space Internet, access security, encryption algorithm, DDoS attack defense technology, routing strategy, etc.

The purpose of this paper is to describe these technological advances in a structured way and to highlight the main research challenges and open issues. In this direction, Section 2 presents the related security challenges faced by Space Internet. Subsequently, we describe and classify the latest research

Research Briefs on Information & Communication Technology Evolution (ReBICTE), Vol. 7, Article No. 12 (October 31, 2021)
DOI:*10.22667/ReBiCTE.2021.10.31.012*
*Corresponding author

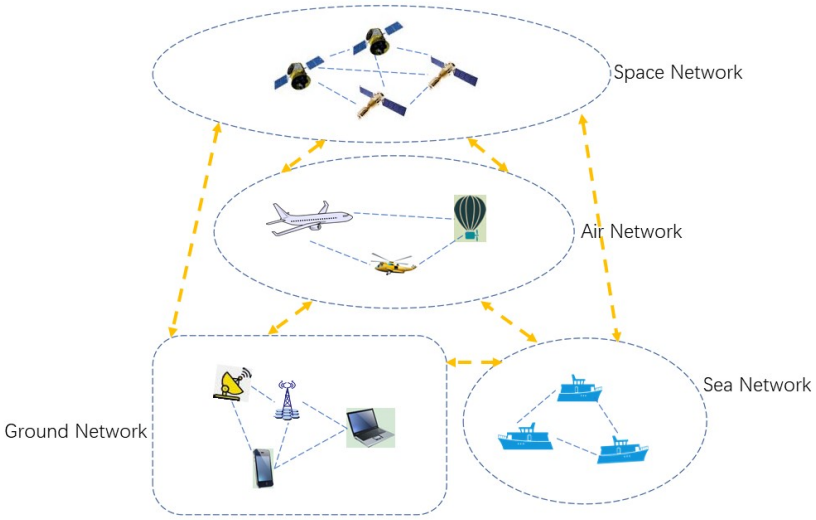

Figure 1: Architecture of Space Internet

works concerning network security issues in Space Internet in terms of 1) architecture of Space Internet, 2) access security, 3) encryption algorithm, 4) DDoS attack defense technology, and 5) routing strategy in Section 3. Finally, Section 4 concludes the whole paper.

2 Security threats in Space Internet

In early research, scholars generally believed that the Space Internet has the following two major security risks due to its node exposure, open channel, high transmission delay, and limited on-board processing capabilities:

1. Physical damage to infrastructure: Failures in the satellite 's own hardware system can paralyze network communications. Facilities such as satellites may also be attacked by anti-satellite weapons, especially in the military field.

   Therefore, researchers have proposed satellite anti-destruction technology to improve the anti-destruction characteristics of satellite infrastructure by optimizing the structure of satellites and ground base stations [1] and multi-station backup [2].

2. Signal interference: the transmission link signal is affected by human or natural electromagnetic interference. Satellites are vulnerable to malicious electromagnetic signal interference in the complex electromagnetic environment, which may lead the result that normal data transmission are affected or even interrupted. At present, signal interference technology mainly includes deception interference and suppression interference. Deceptive jamming technology refers to the jamming technology that enables users to make wrong judgments through satellite signal forwarding and simulation forgery [3, 4]. Suppression jamming technology refers to the jamming technology that the satellite signal is interfered with by high-power noise in the same frequency band, resulting in the reduction of signal-to-noise ratio, thereby reducing or losing availability [5–7].

   For deception jamming, it can be defended by authentication and encryption; for the suppression interference technology, it can be defended by anti-noise channel coding [8], anomaly detection

Table 1: **Traditional security countermeasures for Space Internet**

security threats	countermeasures
Infrastructure security threat	Optimizing Satellite and Ground Base Station Structure Multi-station backup
signal interference	Anti-noise channel coding anomaly detection multi-path fading

[9], and multipath communication [10].

With the continuous growth of the scale, the composition of the Space Internet is more diverse and heterogeneous, and the operating environment is more complex and dynamic. Therefore, it is also faced with three-dimensional and comprehensive new security threats. Specifically, Space Internet security faces three new challenges:

1. Heterogeneity: Covering heterogeneous network nodes, Space Internet is faced with dual security threats of real physical space and virtual network space.

2. Dynamic change of nodes: Satellites move at high speed in large space-time scales and are exposed to harsh environments abroad for a long time, resulting in frequent outbound of domestic data and vulnerable to malicious interference, eavesdropping and attacks by hostile forces.

3. High cost: The high cost of satellite wireless resources and the uneven distribution of satellite users make it difficult to manage network resources effectively.

In order to cope with new security challenges, many research institutions and scholars have put forward many opinions and methods on how to improve the security of Space Internet in recent years.

3 Security countermeasures for Space Internet

3.1 Reconstruction of Space Internet architecture

The closure of Space Internet leads to the inability to quickly and timely introduce new communication and network technologies, and seriously hinders the interoperability of heterogeneous networks, which makes the safe and reliable Space Internet architecture play a crucial role in Space Internet security. In order to make the Space Internet as an important part of the future space-ground integrated communication network, researchers have proposed a series of security architectures about the Space Internet.

Aiming at the problem that the traditional protection technology is difficult to adapt to the evolution of network architecture and the change of attack technology, Ji et al. [11] discussed the application of endogenous security defense technology in space-ground network architecture and key information system, and creatively put forward the endogenous security mechanism of space-ground integrated information network based on mimic defense. The endogenous security mechanism of mimic defense is superimposed on the network and system level, so as to form an endogenous security space-ground integrated network security protection architecture, so as to improve the system security of satellite networks in highly exposed environments.

In [12], Li et al. proposed a world network security that integrates security support layer, access security layer, network security layer, security service layer, security situation warning, unified security

Table 2: **Summary of related works on architecture of Space Internet**

Reference	Features/Advantages	Proposed algorithm/scheme
[11]	Provided reference for the building of security protection system on space-ground integration information network with intrinsic security	Discussed the application of endogenous security defense technology in the world network architecture and key information system
[12]	Divided space-ground network security into four layers	Proposed a security architecture to protect space-ground network
[13]	Suitable for the environment of space-terrestrial integrated situation	Proposed a novel network architecture named space-terrestrial integrated multi-identifier network(STI-MIN)

management, etc. in response to security threats in satellite networks. Guarantee architecture, design implementation mechanisms for unified security management and security situation warning, entity authentication and access protection, multi-domain network interconnection security control, password on-demand service, and dynamic reconfiguration of security services to provide effective support for satellite network security.

Aiming at the inherent deficiencies of current Space Internet in terms of service quality, security and mobility, Wei et al. [13] proposed a world-ground integrated multi-identity network architecture. The system's endogenous security mechanism includes three aspects. : Trusted computing active immune security technology for consortium chain, trust-embedded identity authentication mechanism and multi-identity network intelligent threat perception.

3.2 Access security

The channel openness and node exposure of the Space Internet allow attackers to use this security problem to forge or impersonate legitimate nodes to attack the Space Internet, thereby eavesdropping, intercepting, and tampering with network communications. Finally attackers can achieve deception, interference and suppression to satellite-to-ground/inter-satellite communication. In this case, Space Internet urgently need secure and credible identity authentication. At the same time, due to the dynamic changes of the relative positions of Space Internet nodes, there are frequent handovers between nodes and ground base stations, which makes Space Internets have cross-domain and cross-network communication security access and authentication problems. Many researchers have proposed a series of safe and effective solutions to the problems of identity authentication and secure access in the Space Internets.

In [14], Xue et al. proposed a token-based two-way authentication scheme for the problem of roaming authentication in Space Internets. This scheme uses a token mechanism based on a one-way accumulator to perform user access Control and use Bloom Filter to revoke malicious users to protect the safety and reliability of the network. Based on the difficult problem of decomposition of large integers, this scheme proves that the attacker cannot forge the known FLEO identity. In addition, it can realize anti-replay attack, anti-man-in-the-middle attack, key negotiation, and privacy protection. The delay is only 23.074ms.

In [15], Xue et al. proposed a security authentication enhancement scheme suitable for seamless handover and cross-domain roaming scenarios in the world-ground integrated network for the problem of link switching and user cross-domain roaming in Space Internets. Based on the combination of security credentials and hash chains, the scheme realizes the two-way fast authentication between the user and the visited domain. At the same time, two seamless switching mechanisms are proposed to ensure the continuity of user communication.

Aiming at the risk of hijacking the wireless link in the Space Internet, leading to the problem of identity tracking, counterfeiting, and deception, Xu et al. [16] proposed an anti-tracking trusted identity anonymous authentication mechanism to achieve identity anonymity, forward secrecy, two-way authentication, and secure link negotiation. Through the hash function and part of the previous block in the private chain, the mechanism constructs a unique trusted identity. It is tamper-proof and easy to prove. Besides, there is no need to maintain the mapping relationship in this mechanism. Moreover, the storage is lightweight and the query is efficient. At the same time, to solve the problem of the extra cost of re-authentication caused by the dynamic change of the topology, a cross-domain dynamic authentication method based on identity trust transfer is proposed to improve the authentication interoperability and simplify the frequent authentication process. A multi-party trust model is proposed, which builds an identity mutual trust network in a trusted domain through a three-party basic trust transfer. The cross-domain access entity dynamically switches between broadcast-based identity trust delivery and active identity trust delivery to achieve cross-domain two-way authentication based on identity trust and simplify the frequent re-authentication process.

In [17], Xue et al. proposed a new authentication system model and IoT authentication protocol. In this solution, the user and the satellite access point (SAP) perform mutual authentication. The authentication scheme based on this system model reduces the delay in implementing the authentication process, improves the QoS during handover, and can realize batch handover authentication when a group of users all together switches to another satellite.

Aiming at the privacy leakage or unbearable identity verification delay in the existing roaming authentication schemes and the security problems caused by the vulnerability of SIN, Yang et al. [18] designed an anoymous fast roaming authentication scheme for SIN(Space Information Network), which improves the authentication speed through the pre-negotiation mechanism. In the scheme, group signatures are used to provide anonymity for roaming users. It is assumed that the satellite's computing power is limited, so that it has a defined authentication function, to avoid the real-time participation of the home network control center when authenticating roaming users.

Aiming at the low efficiency and slow response speed of traditional network resource allocation and service scheduling optimization methods under the complex and dynamic network environment of Space Internets, Shen et al. [19] proposed network control, resource allocation, network access selection and mobile cache update technologies based on reinforcement learning. The distributed architecture in this solution can seamlessly match heterogeneous network slices, and configure local control intelligence for each slice or even specific network nodes, thereby reducing control signaling bottlenecks and response time. Besides, it optimizes low-orbit Space Internet access and switching mechanisms and can customize dynamic resource allocation strategies. This solution provides a way to learn about unknown network environments based on "observation and trial and error" without pre-setting any prior model. It takes full advantage of mobile edge storage to achieve the purpose of all-weather seamless content services. At the same time, the solution can greatly reduces the content transmission of the backbone network and provide a security guarantee for the frequent switching and access of the Space Internet.

3.3 Encryption algorithm design

The current ground communication protocols and the cryptographic technologies involved often require the use of public key infrastructure. If the ground scheme is directly applied to the Space Internet, huge communication overhead will be generated, which will lead to network performance degradation [16]. Therefore, for Space Internet nodes with limited resources, researchers have proposed some lightweight cryptographic algorithms to improve computing efficiency and reduce time overhead and computing burden on the basis of ensuring encryption strength.

In [16], Xu et al. proposed a lightweight identity-based cryptographic algorithm that adapts to the

Table 3: **Summary of related works on access security of Space Internet**

Reference	Features/Advantages	Proposed algorithm/scheme
[14]	Guaranteed the security of roaming authentication and significantly reduced the calculation and communication overhead of the authentication and key negotiation process	Proposed a two-way token-based roaming authentication scheme
[15]	Provided essential security properties and achieved reasonable accounting	Proposed a secure authentication enhancement scheme for seamless handover and roaming in space information network
[16]	Realized identity anonymity, forward secrecy, mutual authentication, and secure link negotiation	Designed a reliable identity anonymity authentication mechanism against tracing
[17]	Reduced long authentication delay and avoided a single point of bottleneck in the network control center	Designed a secure and efficient access and handover authentication protocol for Internet of Things in Space Information Networks
[18]	Provided the required security features and a small authentication delay	Designed an anonymous and fast roaming authentication scheme for the Space Information Network
[19]	Proposed the reinforcement learning(RL) framework in the space-air-ground integrated networks	Showed the method of applying deep RL(DRL) for the intelligent access network selection in the space-air-ground integrated networks

Table 4: **Summary of related works on encryption algorithm design of Space Internet**

Reference	Features/Advantages	Proposed algorithm/scheme
[16]	Suitable for limited communication resources	Proposed a lightweight identity-based cryptographic algorithm
[20]	High security level and tolerance to Single Event Upsets (SEU)	Proposed an efficient image encryption method based on chaotic maps and the Advanced Encryption Standard (AES)
[21]	Good performance in terms of high level of security, large enough key-space, tolerance to Single Event Upsets (SEU) as well as low time complexity	Proposed a novel satellite image encryption algorithm based on hyperchaotic systems and Josephus problem

integrated network of heaven and earth, which includes the initialization of the domain parameters of the bilinear pairing on the elliptic curve, based on the trusted identity The private key generation algorithm, two-line encryption and decryption algorithm, two-line signature and verification algorithm are used to ensure confidentiality and availability through the above-designed algorithm. The reliability and security of the algorithm are formally proved. At the same time, three IBOOE algorithms are compared through experiments, which proves that each stage of the proposed algorithm has higher performance and lower resource overhead.

In [20], Youcef Bentoutou et al. proposed a new satellite image encryption algorithm, which combines the CTR mode of AES and chaotic cryptography, and uses 2D-LAS Map as a chaotic selector to distribute chaotically the location of the ciphertext block and the key to improve security. Through the analysis of the key space, information entropy, local Shannon entropy, correlation coefficient and other indicators of the algorithm, it is proved that the cryptographic algorithm can resist exhaustive, selected plaintext, known plaintext attacks and differential attacks, and can effectively tolerate single event disturbance (Single Event Upsets, SEU). At the same time, the author has deployed the algorithm on the FPGA board, which further proves that the proposed algorithm is more efficient and less computationally expensive, and can be effectively applied to low-orbit satellites.

In [21], M. Naim et al. proposed a new type of satellite image encryption algorithm based on linear feedback shift register generator, SHA-512, hyperchaotic system and Josephs problem. The use of hyperchaotic systems is to obtain a better diffusion process. The Josephus problem can improve the security level of the cryptosystem during the obfuscation process without losing the advantages of the hyperchaotic system. Experimental and analysis results show that the algorithm has high security, has a large enough key space, has a high tolerance for SEU, and can complete satellite image encryption with low time complexity.

3.4 DDoS attack defense strategy

Due to the limitation of bandwidth resources, Space Internets are more likely to become victims of DDoS attacks than terrestrial networks. Resource-constrained satellite nodes have a low tolerance for DDoS attacks. Attacks can use high-throughput DDoS attacks to quickly exhaust the resources of the Space Internet, thereby paralyzing regional services. Therefore, researchers have proposed various solutions to detect and prevent or mitigate various DDoS attacks, some of which focus on the use of deep learning solutions to distinguish between normal traffic and malicious traffic.

In [22], Shaaban A R et al. believed that the mission control center is responsible for controlling the operation of satellites and spacecraft, so the mission control center network must maintain availability and be able to resist DDoS attacks. The paper proposes to use convolutional neural networks to classify correct traffic and malicious traffic. Part of the traffic information is captured by Wireshark in the mission control center network to simulate the attack status and normal status, and the other part comes from the open source data set NSL KDD. In the end, the detection success rate of the model proposed in the article reached 99

In [23], Usman M et al. proposed a DDoS mitigation technology, which can be used on the ground base station side of Space Internets. The author simulated the Ping flooding attack in the Space Internet and proved that the proposed solution can proactively prevent DoS and DDoS attacks. In the plan, the Space Internet will be continuously monitored and the average number of ICMP echo requests flowing through the ground base station network will be observed. If the number of requests starts to deviate from the observed average, precautions will be taken to block these requests in the network operations center. The simulation results show that the solution can easily mitigate DDoS attacks without placing too much burden on entities in the Space Internet in terms of communication and data processing capabilities.

In [24], Li et al. carried out research on the intrusion detection system (Network Intrusion Detection

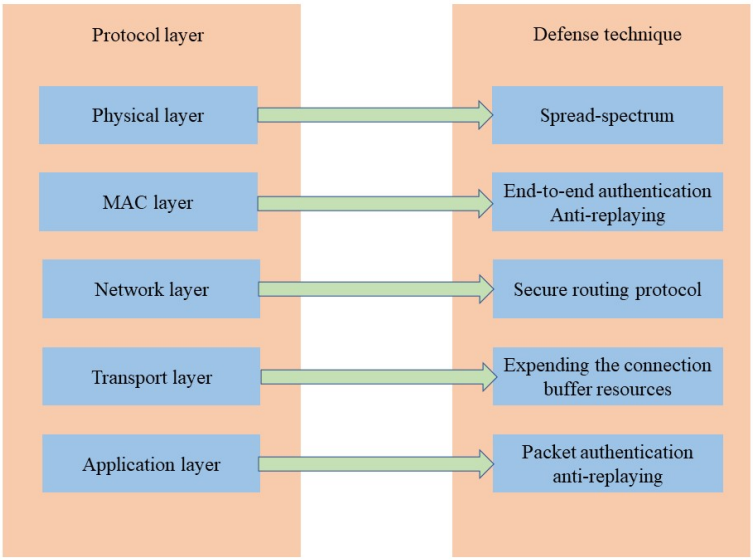

Figure 2: DDoS attacks on wireless communication networks in Space Internet

Systems, NIDS) in the satellite-ground integrated network, and proposed a distributed NIDS based on federated learning and a Space Internet topology Optimize the algorithm and implement it based on the Linux system. The NIDS analyzes and prevents malicious attacks, especially DDoS attacks, by reasonably allocating resources from various domains. In the simulation, the author set up 40 nodes and randomly launched DDoS attacks on these nodes to evaluate the performance of the model. The experimental simulation results show that compared with the traditional method, the distributed NIDS using FL has a higher rate of malicious traffic recognition. Lower packet loss rate and lower CPU utilization.

3.5 Routing strategy

The inter-satellite link is relatively complicated, and the satellite nodes are susceptible to failure due to the complex space environment. Traditional routing protocols such as RIP and OSRF will cause excessive routing control messages and high message exchange frequency if they run in a Space Internet. The slow convergence of the route makes the satellite node paralyzed [25], and it is more likely to be coveted by attackers. Therefore, a new routing protocol must be proposed in accordance with the characteristics of the Space Internet. On the other hand, if a satellite fails, it will not only invalidate the route through it, but also affect the service in the geographical area covered by its movement. Therefore, the real-time monitoring capability of Space Internet link failures, effective redundancy and fault tolerance, appropriate routing capability, and rapid failure recovery capability are also the focus of Space Internet security research.

In [25], Li et al. proposed a dynamic routing protocol with security mechanism, which integrated the static configuration and dynamic configuration strategy of the satellite to realize the dynamic adjustment of the routing, and introduced the reputation value measurement of the satellite node. Enables the network to detect and respond to internal and external malicious attacks. The author proves through experiments that the proposed protocol can deal with network failures well and establish a suitable backup path, which has a low impact on network throughput. In terms of security, the protocol can resist routing table overflow attacks and black hole attacks. When an attack occurs, the protocol can quickly shield

Table 5: **Summary of related works on routing strategy of Space Internet**

Reference	Features/Advantages	Proposed algorithm/scheme
[25]	Added the security mechanism based on the credence model	Proposed a security routing algorithm
[26]	Greatly reduced the route convergence time and the amount of protocol control messages	Designed an inter-satellite secure routing protocol, called Sat-OSPF.
[27]	Reduced the capital expenditures and operational expenditures, and improved the interoperability of satellite network devices	Presented a new software-defined architecture for next-generation satellite networks, called SoftSpace

malicious nodes and has good security performance.

In [26], Zhou et al. proposed a protocol design for inter-satellite secure routing-based on the predictable topology of the Space Internet inter-satellite routing protocol Sat-OSRF, which uses the predictable and changing periodicity of the Space Internet The advantage avoids the disadvantage of traditional OSRF that uses a large number of messages to describe network topology changes. Because the satellite's trajectory will be extracted and planned before launch, it can predict and actively respond to network topology changes. Simulation shows that this scheme can greatly reduce the cost of routing control messages and speed up routing convergence. The author also proposes an ECC-based certificateless signature security enhancement solution to solve the security threats faced by the Sat-OSRF protocol. The solution ensures the authenticity of the routing node identity and the authenticity of the protocol message, and avoids Sat-OSRF. Subject to malicious attacks, experiments also show that the security enhancement scheme has a small impact on the routing convergence speed.

In [27], Xu et al. proposed a new software-defined architecture for the next-generation Space Internet, which the author called SoftSpace. In SoftSpace, network function virtualization and software-defined radio methods are used to promote the integration of new applications, services and satellite communication technologies. This can not only reduce capital expenditures and operating expenditures, but also seamlessly integrate Space Internets with terrestrial networks, and can improve the interoperability of Space Internet equipment. This paper also proposes a hybrid failure recovery mechanism for SoftSpace, which combines the advantages of active failure recovery mechanism and passive response mechanism, reduces failure recovery time, and ensures the best recovery path. Specifically, in the design of the failure scheme in this paper, the working path and the recovery path are calculated by the network controller and installed in the Software-defined LEO satellite at the same time, so that the network controller performs routing when a failure occurs.

4 Conclusion

Based on the analysis of the security threats faced by Space Internet and traditional protection technology, this paper analyzes and sorts out the research directions and technical ideas of existing security protection methods for new security challenges. Overall, the Space Internet will enter a period of rapid development. The security of Space Internet will develop towards endogenous security and unified control.

In the direction of endogenous security, the traditional TCP/IP system is not friendly to the Space Internet system with rapidly changing topology and severely limited on-board processing capacity. The research on the endogenous security mechanism of binding the real identity information of individuals, organizations and equipment owners with network communication identification is a breakthrough di-

rection. In terms of unified management and control, the Space Internet will break the separation and irrelevant status of traditional satellite operation control, measurement and control, network management and network application, and adopt unified security mechanism and security policy standards to lay a solid foundation for building a unified security management and control mechanism between heaven and earth.

References

[1] A.Chen. Satellite communication system security protection. *Network Security Technology and Application*, (9):95–97, September 2019.

[2] W. Zhang, P. Fan, Z. Wu, and C. Zhang. Research on security protection architecture of military satellite system. In *Proc. of the 6th China Command and Control Conference, Beijing, China*, volume 2, pages 243–247. Publishing House of Electronics Industry, July 2018.

[3] D. Benedikt, H. Ralf, W. Carsten, P. Christof, and H. Thorsten. Don't trust satellite phones: A security analysis of two satphone standards. In *Proc. of the 2012 IEEE Symposium on Security and Privacy (S&P'12), San Francisco, CA, USA*, pages 128–142. IEEE, May 2012.

[4] N. O. Tippenhauer, C. Pöpper, K. B. Rasmussen, and S. Capkun. On the requirements for successful gps spoofing attacks. In *Proc. of the 18th ACM Conference on Computer and Communications Security (CCS'11), Chicago, Illinois, USA*, page 75–86. ACM, October 2011.

[5] T. Nighswander, B. Ledvina, J. Diamond, R. Brumley, and D. Brumley. Gps software attacks. In *Proc. of the 19th ACM Conference on Computer and Communications Security (CCS'12), Raleigh, North Carolina, USA*, page 450–461. ACM, October 2012.

[6] K. C. Zeng, S. Liu, Y. Shu, D. Wang, H. Li, Y. Dou, G. Wang, and Y. Yang. All your GPS are belong to us: Towards stealthy manipulation of road navigation systems. In *Proc. of the 27th USENIX Security Symposium (SEC'18), Baltimore, MD, USA*, pages 1527–1544. USENIX Association, August 2018.

[7] S. Narain, A. Ranganathan, and G. Noubir. Security of gps/ins based on-road location tracking systems. In *Proc. of the 2019 IEEE Symposium on Security and Privacy (S&P'19), San Francisco, CA, USA*, pages 587–601. IEEE, May 2019.

[8] W. Meng. *Study on the Authentication Mechanism for the Security Access of the World-Earth Integrated Information Network*. PhD thesis, University of Science and Technology of China, 2019.

[9] K. Gorkem, M. Hossen, W. Yan, C. Yingying, X. Wenyuan, G. Marco, and V. Tam. Detection of on-road vehicles emanating gps interference. In *Proc. of the 21st ACM Conference on Computer and Communications Security (CCS'14), Scottsdale, Arizona, USA*, pages 621—-632. ACM, November 2014.

[10] Z. Kewei and P. Panos. Secure multi-constellation gnss receivers with clustering-based solution separation algorithm. In *Proc. of the 2019 IEEE Aerospace Conference (AERO'19), Big Sky, MT, USA*, pages 1–9. IEEE, March 2019.

[11] X. Ji, H. Liang, and H. Hu. New thoughts on information network security protection technology for integrated space and earth. *Telecommunications Science*, 33(12):24–35, December 2017.

[12] F. Li, L. Zhang, Y. Lu, K. Geng, and Y. Guo. Study on the technology of world network security assurance. *World Integrated Information Network*, 1(1):17–25, December 2020.

[13] G. Wei, H. Li, Y. Bai, G. Li, and K. Xing. World integration endogenous security multi-identification network system. *World Integration Information Network*, 1(2):66–72,80, December 2020.

[14] K. Xue, Y. Ma, J. Hong, J. Xu, and Q. Yang. Token-based secure and efficient roaming authentication scheme in world-earth integrated networks. *Journal of Communications*, 39(5):48–58, May 2018.

[15] K. Xue, H. Zhou, W. Meng, and S. Li. A security authentication enhancement scheme in the scenarios of seamless handover and cross-domain roaming in integrated world-ground networks. *Journal of Communications*, 40(6):138–147, June 2019.

[16] J. Xu. *Research on the Trusted Identity Authentication Mechanism of the Integrated World and Earth Network*. PhD thesis, Beijing University of Posts and Telecommunications, 2019.

[17] K. Xue et al. A secure and efficient access and handover authentication protocol for internet of things in space information networks. *IEEE Internet of Things*, 6(3):5485–5499, June 2019.

[18] Q.Yang, K.Xue, J.Xu, J.Wang, F.Li, and N.Yu. Anfra: anonymous and fast roaming authentication for space information network. *IEEE Transactions on Information Forensics and Security*, 14(2):486–497, February 2019.

[19] X. Shen, N. Cheng, H. Zhou, W. Quan, W. Shi, H. Wu, and Z. Zhou. Space-air-ground integrated networks:review and prospect. *Journal of the Internet of Things*, 4(3):3–19, September 2020.

[20] Y. Bentoutou, E.-H. Bensikaddour, N. Taleb, and N. Bounoua. An improved image encryption algorithm for satellite applications. *Advances in Space Research*, 66(1):176–192, July 2020.

[21] M. Naim, A. A. Pacha, and C. Serief. A novel satellite image encryption algorithm based on hyperchaotic systems and josephus problem. *Advances in Space Research*, 67(7):2077–2103, April 2021.

[22] A. R. Shaaban, E. Abd-Elwanis, and M. Hussein. Ddos attack detection and classification via convolutional neural network (cnn). In *Proc. of the 9th International Conference on Intelligent Computing and Information Systems (ICICIS'19), Cairo, Egypt*, pages 233–238. IEEE, December 2019.

[23] M. Usman, M. Qaraqe, M. R. Asghar, and I. S. Ansari. Mitigating distributed denial of service attacks in satellite networks. *Transactions on Emerging Telecommunications Technologies*, 31(6):e3936, March 2020.

[24] K.Li, H.Zhou, Z.Tu, W.Wang, and H.Zhang. Distributed network intrusion detection system in satellite-terrestrial integrated networks using federated learning. *IEEE Access*, 8:214852–214865, December 2020.

[25] Z. Li and J. Liu. Research on satellite network security routing. *Journal of Communications*, 4(8):113–119, August 2006.

[26] Y. Zhou. *Inter-satellite Security Routing Protocol Design and Simulation Verification*. PhD thesis, Chongqing University of Posts and Telecommunications, 2020.

[27] S. X.Wang and M.Huang. Software-defined next-generation satellite networks: Architecture, challenges, and solutions. *IEEE Access*, 6:4027–4041, January 2018.

Author Biography

Cheng Gong is a postgraduate student at the School of Computer, National University of Defense Technology, China. His current research interests include communication technology and Identity authentication.

Tongwei Liu is a postgraduate student at the School of Computer, National University of Defense Technology, China. His current research interests include communication technology and Network addressing.