Study on Security of 5G and Satellite Converged Communication Network

YAN Xincheng[1,2], TENG Huiyun[2], PING Li[2], JIANG Zhihong[2], ZHOU Na[1,2]

(1. State Key Laboratory of Mobile Network and Mobile Multimedia Technology, Shenzhen 518055, China;
2. ZTE Corporation, Shenzhen 518057, China)

DOI: 10.12142/ZTECOM.202104009

http://kns.cnki.net/kcms/detail/34.1294.TN.20211022.1252.002.html, published online October 22, 2021

Manuscript received: 2021-08-09

Abstract: The 5G and satellite converged communication network (5G SCCN) is an important component of the integration of satellite-terrestrial networks, the national science, and technology major projects towards 2030. Security is the key to ensuring its operation, but at present, the research in this area has just started in our country. Based on the network characteristics and security risks, we propose the security architecture of the 5G SCCN and systematically sort out the key protection technologies and improvement directions. In particular, unique thinking on the security of lightweight data communication and design reference for the 5G SCCN network architecture is presented. It is expected to provide a piece of reference for the follow-up 5G SCCN security technology research, standard evolution, and industrialization.

Keywords: 5G SCCN; non-terrestrial networks; 5G security; satellite security; integration of satellite-terrestrial networks

Citation (IEEE Format): X. C. Yan, H. Y. Teng, L. Ping, et al., "Study on security of 5G and satellite converged communication network," *ZTE Communications*, vol. 19, no. 4, pp. 79 - 89, Dec. 2021. doi: 10.12142/ZTECOM.202104009.

1 Introduction

The development of mobile communication technology has greatly improved the informatization level of all industries in the whole society. However, due to factors such as space and quantity, 5G communication networks are currently deployed in limited areas. Satellites are an ideal choice for wide coverage communications[1], especially for areas where ground transmission towers cannot be deployed (oceans, mountains, islands, etc.) and for scenarios of disaster relief and emergency response. Building 5G and satellite converged communication network (5G SCCN) has become an important direction for future network development, deeply combining the excellent access capabilities and mobility of 5G networks with the extensive coverage capabilities of satellite networks, and giving play to the respective advantages of the networks to achieve global wide-area full coverage and seamless high-speed interconnection. However, the satellite network has the characteristics of environmental openness, time-varying topology, and limited computing resources, bringing 5G and satellite networks more complex security challenges; meanwhile, 5G SCCN will carry more critical and urgent communication services for industries, individuals, and public affairs, which makes it particularly important to ensure the security of 5G SCCN.

A wave of satellite Internet constellation construction is underway around the world. At present, at least 15 companies around the world have announced low-orbit communication satellite plans, and many have carried out research and practice related to 5G and satellite converged networks[2]. In 2017, the European Union funded the Satellite and Terrestrial Network for 5G (SaT5G) alliance to promote solutions that integrate satellite communications with 5G, software-defined networking/network functions virtualization SDN/NFV, and other technologies[3-4]. In 2018, the European Space Agency (ESA) launched the ALIX project to promote the standardization of 5G satellite components and its interfaces with other networks[5]. In 2019, Telesat verified that low-orbit satellites provided effective solutions to 5G base station relays[6]. In April 2021, the China Satellite Network Group was established. It plans to provide satellite communication services including 5G satellite converged networks to ground and air terminals. In July 2021, Beijing University of Posts and Telecommunications completed a low-orbit satellite and 5G private network integration test between two cities.

The academia has researched on early development of satellite communications[7-9]. In recent years, institutions and univer-

sities have gradually carried out technical research on satellite-terrestrial converged communications[10 - 15] and its security, such as dual access through satellite and ground base stations, 5G New Radio (NR) and satellite network convergence, and satellite networks and 5G core network heterogeneous convergence. In the security aspect, the National Digital Switching System Engineering & Technological R&D Center has researched on satellite communication security[16 - 17]. The Ph. D. thesis "Research on Security Protocol of Broadband Satellite Network" improves security protocols such as IP Security (IPSec) and Internet key exchange (IKE) for satellite communications[18].

Standard organizations such as International Telecommunication Union (ITU) and the 3rd Generation Partnership Project (3GPP) proposed that satellite networks can be used as extensions of terrestrial networks[19 - 24], and research in this area has been carried out. Among them, ITU-R M.[NGAT_SAT][19] defines and discusses the key technical issues, service characteristics, network structure, and deployment scenarios regarding satellite networks integration into 5G networks. 3GPP's research on 5G and satellite converged networks is mainly carried out in two projects, TR 38.811[20] and TR 22.822[21]. Among them, "Study on Using Satellite Access in 5G" (TR22.822) analyzes the functional requirement of 5G satellites and introduces 12 functional requirements and their corresponding usage scenarios. While "Study on NR to Support Non-Terrestrial Networks" (TR 38.811) proposes three functions of satellite communications for 5G networks. It serves as a supplementary coverage for terrestrial 5G networks, provides continuous communications for high-speed mobile carriers, and uses new services such as satellite multicast and broadcast. The project also introduces service characteristics, network structures, deployment scenarios, and non-ground-based network channel models of 5G and satellite converged networks and proposes a variety of non-terrestrial network architecture options.

However, although 3GPP defines the network form of 5G SCCN, its security issues have not been considered. At present, there is also a lack of technical requirements in this area, and standards are also absent. This paper intends to analyze and discuss the security requirements and key security technologies of 5G SCCN. On the one hand, it is a reference for future research on 5G and satellite converged network security technology, standard promotion, and industrialization; On the other hand, based on the concept of "security-synchronized design", it is hoped that the security design can provide a reference for 5G SCCN design.

2 Security Challenges and Requirements

2.1 Security Challenges

5G SCCN has different network characteristics from terrestrial 5G networks. These characteristics are mainly derived from satellite networks. Meanwhile, the cross-network and cross-domain integration of 5G and satellite networks, and the introduction of 5G diversified services will jointly constitute new features of the converged network, making 5G SCCN face new security challenges.

1) Borderless security issues are caused by the open network environment.

Different from the terrestrial network, the satellite network nodes are exposed and channels are open, and the satellite node runs in the exposed space orbit for a long time. Thus, new threats emerge. For example, the inter-satellite and satellite-to-ground wireless communication links are more susceptible to the adverse natural environment and malicious users; network nodes are more susceptible to forgery and hijacking; communication links are more susceptible to human interference, eavesdropping, replay attack, and wireless resource occupation. Therefore, higher risks of confidentiality, integrity, availability and reliability of the network are posed.

2) Dynamic changes in network topology lead to changes in security policies.

The 5G SCCN includes satellite nodes and ground nodes. Satellite nodes are always in high-speed operation and may frequently join or exit the network. This makes the network topology change dynamically, and the communication objects change as a consequence, which leads to network security function switching and security strategy migration, such as the update and synchronization of the original authentication policy, or the renegotiation of the original IPSec/transport layer security (TLS) tunnel.

3) Heterogeneous interconnection causes security applicability issues.

5G and satellite converged communications are based on different forms of physical resources and present a "chimney-like" development model. Different satellite systems are relatively independent and dedicated, lacking a unified network protocol specification. This may also make the mature security protocols applicable to terrestrial networks while inapplicable to satellite networks. In addition, the heterogeneous interconnection and long-distance communication of the 5G SCCN make it more difficult to protect data in transmission, and the risk of user data being stolen, tampered with, and damaged increases.

4) Insufficient security computing power is caused by low on-board processing capability.

Satellites usually use aerospace-grade chips to cope with the complexity and harshness of the space environment. In order to improve the reliability of the chip, it is necessary to reduce the density of computing units on the chip, and strictly control the amount of computing of the software carried by the satellite, which makes the computing power of the satellite far lower than that of the ground communication node. Therefore, satellite nodes are more susceptible to availability attacks from asymmetric computing power, such as distributed denial

of service (DDoS) attacks. Meanwhile, some traditional computationally intensive encryption algorithms cannot run on satellites. All these make the security of satellite nodes face greater challenges, and therefore, it is necessary to research on a new type of 5G security architecture and security technology suitable for satellite networks.

2.2 Security Requirements

Based on the above analysis of the 5G SCCN characteristics and security challenges, four security requirements can be summarized: identity authentication, lightweight communication security, enhanced availability protection, and fine-grained resource sharing and isolation.

1) Universal identity authenticity needs

Terrestrial communication networks usually adopt physical isolation or physical dedicated lines. Network nodes are usually in the same physical or logical trust domain, and there is a default trust relationship among network nodes. However, the 5G SCCN conducts ultra-long distance communication in an open space environment, and the satellite network has a time-varying topology, which makes the communication objects highly dynamic. Therefore, ensuring the authenticity of communication nodes, especially the authenticity of network equipment, is a key requirement for 5G SCCN. Through the access authentication of the terminal and the authentication between the network nodes, a communication system with an open external environment and trustworthy internal communication can be established.

2) Lightweight communication security requirements

In the 5G SCCN, the service link, inter-satellite link, and feeder link all use wireless links for communication, making it more vulnerable to eavesdropping, tampering, and replay attacks. Therefore, the confidentiality and integrity protection of the transmitted data is especially necessary. On the other hand, due to the limited processing resources on the satellite, it is necessary to avoid running computationally intensive encryption algorithms on the satellite as much as possible. The 5G SCCN consequently needs to design and adopt lightweight communication security architecture and technology to ensure the security of communication data while avoiding excessive computational burden on the satellite network.

3) Enhanced availability protection requirements

Availability attacks on existing networks will still exist in 5G SCCN, such as DDoS attacks and signaling storms. Considering the openness of the satellite network environment, lower processing capacity, and high value of the services, the security risks are severer. Therefore, more systematic and efficient technical measures need to be adopted to ensure the availability of functions and services on satellite nodes.

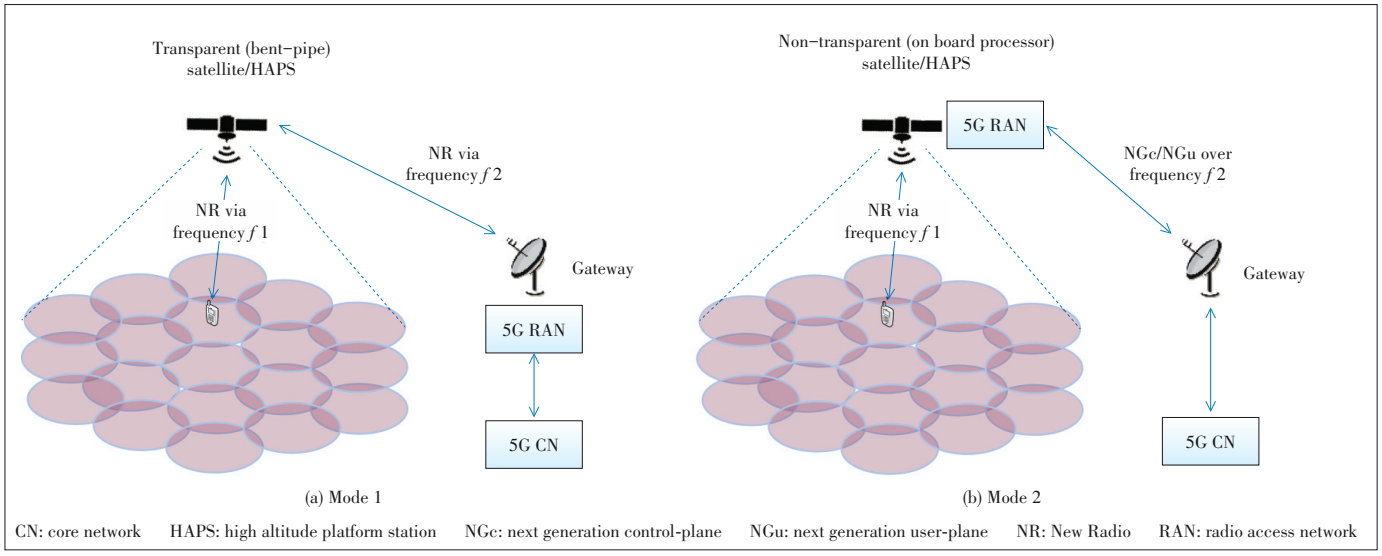
4) Fine-grained resource sharing and isolation requirements

The 5G SCCN will provide differentiated network services for public users, industry users and special users on shared network infrastructure. Therefore, it is necessary to isolate shared resources securely and effectively to prevent side-channel attacks and threats from spreading. Limited satellite network resources put forward higher requirements on the granularity of resource sharing, and more refined network resource management technologies are required.

3 Network Security Architecture

3.1 Service Architecture

3GPP TR 38.811 defines two typical 5G and satellite converged network modes (excluding relay nodes), as shown in Fig. 1. In mode 1, 5G RAN is still deployed on the ground, and the satellite network is used as a transparent forwarding channel for the 5G access network; In mode 2, 5G radio access network (RAN) is deployed on the satellite and connected



▲**Figure 1. Typical access network mode of 5G and satellite integration (Source: 3GPP TR 38.811)**

to the ground core network through non-terrestrial networks (NTN) gateway.

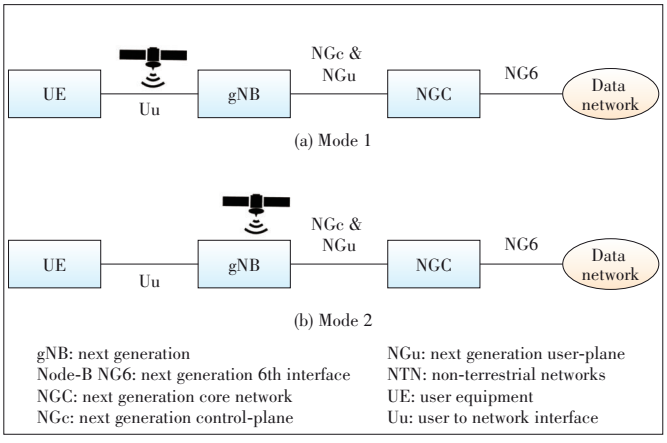
Fig. 2(a) shows NTN featuring access network serving user equipment (UE), based on a satellite/aerial with bent pipe payload and gNB on the ground (satellite hub or gateway level). Fig. 2(b) shows NTN featuring an access network serving UE, based on a satellite/aerial with gNB on board.

In contrast, Mode 2 is easier to inherit the existing 5G access technologies, including air interface scheduling technology, mobile handover technology, terminal secure access technology, etc., and it is also easier to achieve the goal of mobile terminal access everywhere with one device, which has better industrialization foundation and better serviceability. Therefore, the follow-up technical research herein mainly focuses on the second service model, which is about the gNB on board the satellite network.

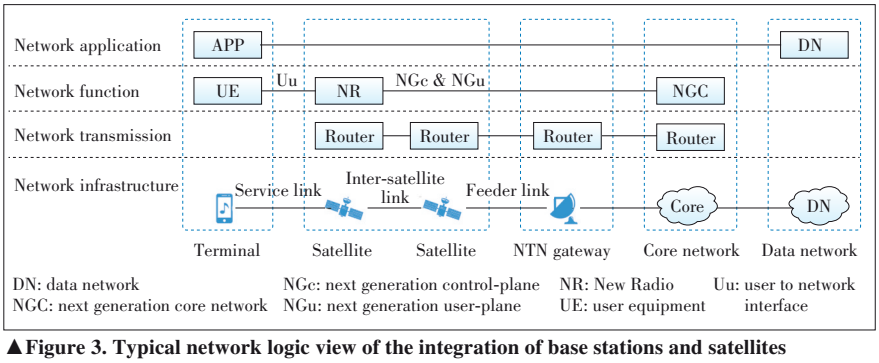
Fig. 3 shows the service architecture in Mode 2 of 3GPP TR 38.811. A mobile phone terminal accesses Internet services through a 5G SCCN. From left to right, the terminal UE located on the ground or in the air communicates with the base station NR on the low-orbit satellite. The inter-satellite link is routed to the ground satellite gateway station, then reaches the core network, and finally accesses Internet services.

In the vertical dimension, the entire service model can be abstracted into four levels, from bottom to top including the network infrastructure layer, the network transmission layer, the network function layer, and the network application layer. The network transmission layer and the network function layer realize respectively the forwarding of IP packets and the communication of the mobile network. At the network transmission layer, assuming that satellites and satellite gateways have basic routing functions and follow the basic IP routing protocol to realize the transmission and forwarding of messages on inter-satellite links and the satellite-to-ground links, and at the network function layer, assuming that the base station is on the satellite, a 5G communication network is therefore formed consisting of network functions such as the terminal, the on-board base station and the terrestrial core network, which has the basic features and capabilities of a 5G network.

Through the service architecture, we can decompose the capabilities of each communication facility, and thus map more clearly the requirements and capabilities of the traditional 5G network and bearer network to the NTN network. For example, the NGc&NGu port in the 5G network is composed of inter-satellite links, feeder links, and the ground bearer network between satellite gateways and the core network in the NTN network. As another example, because the satellite has the capability of a base station at the network functional layer, the UE's access guarantee can be enhanced with the help of existing 5G access technologies to a large extent.



▲Figure 2. Network logical view of two modes



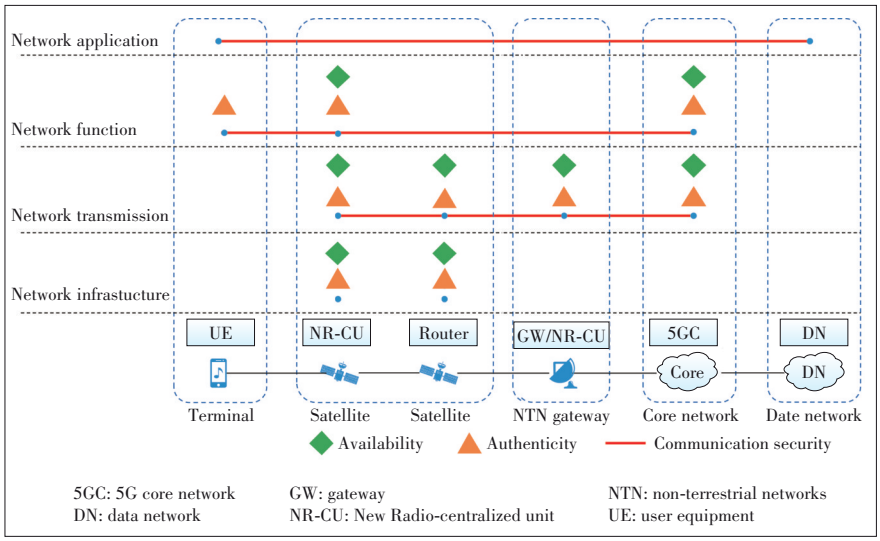
▲Figure 3. Typical network logic view of the integration of base stations and satellites

3.2 Security Architecture

Due to the openness, mobility, and low power consumption of satellite links, the offensive and defensive situations of 5G SCCN and terrestrial 5G networks are quite different. But many similar technologies can be used and referenced. As shown in Fig. 4, based on the service architecture, the security of the 5G SCCN is analyzed layer by layer, focusing on the three types of security attributes of availability, authenticity, and communication security (confidentiality, integrity, and communication isolation) for key communication nodes and interfaces.

In the 5G SCCN, in addition to the general security attributes and technologies of the 5G network, it is important to consider the security issues caused by the characteristics of the satellite network and its integration with the 5G network. Given the different service characteristics and security attributes of each layer, the required security technologies are also different.

At the infrastructure layer, considering the difficulty of upgrading and maintaining the equipment on the satellite, it is necessary to establish an active immune mechanism for the satellite node through the trusted boot to resist attacks from unknown threats to ensure the authenticity of a single node. The infrastructure protection method for other nodes is similar to that of the 5G network. In the radio frequency part, con-



▲Figure 4. 5G satellite converged communication network (SCCN) security architecture

sidering the power asymmetry between the satellite and the ground attacker, the availability of satellite nodes needs to be paid more attention.

At the network transmission layer, in order to ensure the confidentiality and integrity of the information transmission of the inter-satellite link and the back-haul network, the bearer network communication security technology is needed to be in place. Considering the limited resources of satellite networks, lightweight attack detection methods can be used to defend against DDoS attacks on satellite networks. In addition, with the slice isolation technology of the bearer network, the satellite network-related traffic is isolated from other 5G network traffic to avoid mutual influence.

At the network function layer, to reduce the burden on the on-board base station, on-demand air interface signaling encryption and decryption and user plane confidentiality and integrity protection functions are considered. To ensure that the satellite access network and related core network resources are not affected by other 5G services, end-to-end slice isolation from the RAN to the core network should be adopted. Regarding the malicious directed call attack that may exist in the case of the asymmetry of space and ground resources, the anti-UE random access technology should be adopted to ensure the regular access of legitimate users. In addition, in order to ensure the legitimate access of mass terminals and dynamic nodes, it is necessary to perform two-way authentication on the terminals and the network nodes.

At the network application layer, in order to protect the confidentiality and integrity of application layer data, end-to-end encryption technology is used between the terminal and the application service. To reduce the processing burden of the satellite, the satellite nodes can implement transparent transmission.

The specific security technologies are referred to in Table 1.

4 Key Protection Technology

Combining the analysis result in Table 1, this section analyzes the key technologies involved in aspects of identity authentication, data communication security, network availability, and network resource sharing. Due to space limitations, we only put forward directional suggestions for each technical requirement, and elaborate the key technical features needed to meet the requirements, the current technologies that can be inherited or learned from, and the improvement suggestions when applying this technology to 5G SCCN. The technical details will not be discussed.

4.1 Identity Authentication

Due to the openness and the time-varying topology of the 5G SCCN, it is necessary to verify the authenticity of the communication node. In addition to the terminal access authorization in the traditional 5G network, the 5G SCCN also needs to authenticate the network nodes. Communications among network nodes should take identity authentication as a prerequisite, and ensure the security and independence of the 5G SCCN system by enabling the identity authentication process. Meanwhile, technologies such as trusted boot and trusted environment can also be used to further ensure the authenticity of hardware devices and their running software.

4.1.1 Terminal Access Authentication

In the 5G SCCN, due to the openness of the service link and the diversity of access terminals, the trusted communication of the service link has received much attention. 3GPP defines a complete user access system for 5G networks. Based on the 5G unified authentication architecture (5G-AKA or EAP-AKA'), the terminal and the service network are mutually authenticated to ensure mutual trust between users and the network. The 5G SCCN can follow this set of access authentication frameworks to ensure the trusted access of wireless terminals and solve the problem of pseudo base stations, pseudo terminals, and pseudo networks. Meanwhile, 5G SCCN also needs to enhance 5G access authentication for new network features. For example, for the weak processing capabilities of satellite nodes and new multicast services, group authentication and lightweight authentication methods[25] need to be considered; The topology of the satellite network is time-varying, and it is necessary to enhance the switching capability of the X*n* ports between the base stations.

4.1.2 Authentication of Network Nodes

Authentication of network nodes is a key feature that distinguishes 5G SCCN from terrestrial 5G networks. In the commu-

▼Table 1. Catalogue of security protection technology

Network Layer	Security Attributes	Categories of Security Technology	Sub-Categories of Security Technology
Network application layer	Communication security	Data communication security	User data communication security
Network function layer	Authenticity	Identity authenticity	Terminal access authentication
			Authentication between network nodes
	Availability	Network availability	Anti-DDoS attack
			Anti-UE random access attack
	Communication security	Network resource sharing	RAN slice isolation
			Core network slice isolation
		Data communication security	Network function communication security
Network transmission layer	Communication security	Network resource sharing	Bearer network slice isolation
		Data communication security	Bearer network communication security
	Availability	Network availability	Anti-DDoS attack
	Authenticity	Identity authenticity	Authentication between network nodes
Infrastructure layer	Availability	Network availability	Anti-wireless communication interference
	Authenticity	Identity authenticity	Trusted boot of satellite nodes

DDoS: distributed denial of service UE: user equipment RAN: radio access network

nication of each layer of the 5G SCCN, whether the communication is between network functions (such as between NR and 5G core network elements) or between transmission nodes (such as on-board routing and forwarding), the authentication of the network node is required as a precondition to prevent attackers from impersonating legitimate network functions to access the 5G network, or impersonating legitimate transmission nodes to establish routing adjacencies with legitimate satellites, thereby stealing or tampering with user data and routing information in the network.

There are two typical authentication methods. One is to use SDN-like technology. The communication forwarding node uniformly authenticates the management node, and the token for network communication is obtained after the authentication is passed. Since there may be blind spots in communication, this method has higher requirements on the topology of the management network. The other way is to carry out mutual authentication between communication nodes. This way has a relatively high technical maturity. For example, two-way authentication between network function nodes can be performed based on the IKE protocol, and the authentication function in the dynamic routing protocol can be enabled to implement identity authentication between routing and transmission nodes. However, in this way, the overhead brought to the satellite node and the system complexity introduced by the dynamic switching of communication objects need to be considered.

4.1.3 Trusted Boot of Satellite Nodes

Satellite nodes run in the space orbit for a long time, making upgrades and maintenance difficult. Software and hardware vulnerabilities are difficult to update in time, and the nodes are more vulnerable to attacks from unknown threats. Therefore, the satellite nodes need stronger self-immunity. Satellite nodes need to be reinforced under the principle of the least privilege, such as shutting down unnecessary processes and ports. Meanwhile, with trusted computing technology, there forms a trusted chain of level-by-level verification to ensure the operation of satellite nodes through digital signature and integrity verification technology. Based on trusted execution environment (TEE) storage device identity fingerprints, combined with technologies such as authentication and remote certification, the authenticity of the 5G SCCN communication system can be further assured.

4.2 Data Communication Security

Due to the openness of the 5G SCCN, the confidentiality and integrity protection of the transmitted data has become particularly important. However, the cryptographic computing used for data confidentiality and integrity protection requires a large amount of computing power, which contradicts the low processing capabilities of satellites. Therefore, the confidentiality and integrity protection of the 5G SCCN needs to be considered systematically, especially to avoid enhancing the overhead of satellite nodes greatly. This section discusses the communication security protection technology of critical data such as 5G signaling, IP routing, and user data in the 5G SCCN, and proposes a framework solution that can effectively avoid the impact on satellite computing resources caused by confidentiality and integrity requirements.

4.2.1 Bearer Network Communication Security

On the ground network, if a section of the bearer network is in an insecure or untrustworthy environment, it is usually recommended to protect its confidentiality and integrity. On the satellite network, although the inter-satellite and satellite-to-ground links use wireless communications, considering the limited processing capabilities of the satellite nodes, we do not recommend this kind of protection. Confidentiality and integrity protection in 5G SCCN communication requires refined

design. For the data transmitted in the network, including 5G signaling and user data, it is recommended that the network function layer and application layer be resolved. This part will be discussed in subsequent sections. The network transmission layer should focus on ensuring the confidentiality and integrity of the routing information exchanged in the network. If each network node in the 5G SCCN has undergone strict authentication, whether it is necessary to protect the confidentiality and integrity of routing information requires further research. If considering the bit error rate of wireless transmission, cyclic redundancy check (CRC) may be more suitable for satellite communications than MD5.

4.2.2 Network Function Communication Security

This section focuses on the security of signaling communications between 5G network functions, and the security of user data communication carried by the 5G network is discussed in the next section. In order to ensure the security of 5G air interface communication and UE access signaling, 3GPP has standardized the confidentiality and integrity protection of radio resource control (RRC) signaling between UE and NR, and non-access stratum (NAS) signaling between UE and 5GC. In order to enhance the communication security of the 5G SCCN, it is recommended to enable transmission protection for RRC and NAS signaling. However, the opening of the confidentiality and integrity of RRC signaling means that the load on the on-board base station will increase significantly.

In view of the limited computing resources of satellites, confidentiality and integrity computing on the satellite should be avoided. As shown in Fig. 5, we recommend the Control and User Plane Separation technology, to adopt the deployment method of distributed unit-centralized unit (DU-CU) separation. Among them, the DU is deployed on the satellite, and the CU is deployed on the ground. The physical layer, media access control (MAC) layer, and radio link control (RLC) layer with high real-time requirements are placed in the DU for processing, while the packet data convergence protocol (PDCP) and RRC layers with relatively low real-time requirements are placed in the CU for processing. Since the confidentiality and integrity of the RRC signaling are completed at the PDCP layer by the DU located on the ground, it is possible to effectively avoid heavy-duty cryptographic computing on the satellite nodes.

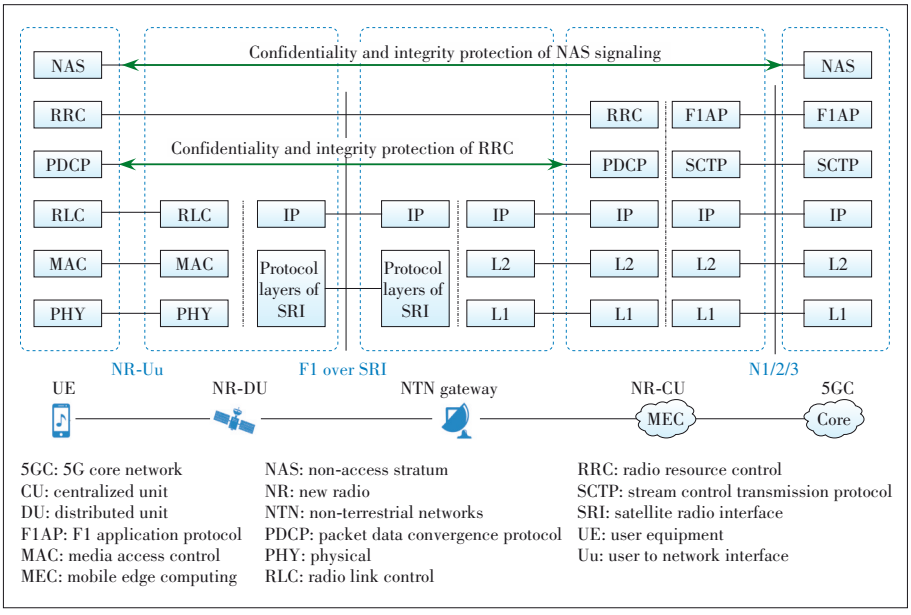
4.2.3 User Data Communication Security

In Fig. 6, there are requirements for communication security assurance at the network transmission layer, network function layer, and network application layer. In traditional network protection, the idea of in-depth multi-level protection is usually adopted, that is, each system and each protocol layer is protected independently. When the internal system is protected, the assumption that the external system has been protected cannot be made. This may result in the network transmission layer, network function layer, and network application layer protecting the confidentiality and integrity of user data on their own. However, in satellite communications, this idea cannot be fully applied, instead, the principles of minimalism and optimality should be adopted.

To solve the contradiction between the security protection of data communication and the weak processing capability of satellite nodes, we can use the idea of "transmitting on-satellite, processing off-satellite" and place the encryption, decryption and integrity check of high computing costs on the ground node for processing. The satellite is mainly responsible for the forwarding of encrypted user plane data to achieve a balance between performance and security. The higher layer the encryption is applied to, the closer to the end-to-end encryption and the higher level of the security is achieved. Based on this idea, we propose two security solutions to data communication, which are discussed below.

1) Solution 1: UE-DN's end-to-end security

Users and providers of 5G SCCN usually belong to different trust subjects, especially for some high security level services. Network users do not fully trust the protection mechanism of the network provider, and tend to provide end-to-end data encryption by themselves. Performing user data confidentiality and integrity protection between the UE and the Internet can effectively prevent user data from being eavesdropped and tampered with. At the same time, security functions such as



▲**Figure 5. 5G control plane encryption and integrity protection**

encryption, decryption, and integrity verification are performed on the terminal and the ground network. The satellite node does not participate in cryptographic computing but only performs transparent forwarding, which greatly saves the computing power of the satellite node.

However, end-to-end encryption also introduces additional problems, such as illegal interception, and the inability of the IP Multimedia Subsystem (IMS) network to recognize voice over Long-Term Evolution (VoLTE) or guarantee the voice quality. The trusted third-party key management server (KMS) or the deployment of encryption and decryption agents in the core network can help solve the problem of legal interception of encrypted communications and the problem of VoLTE voice recognition after multiple encryptions.

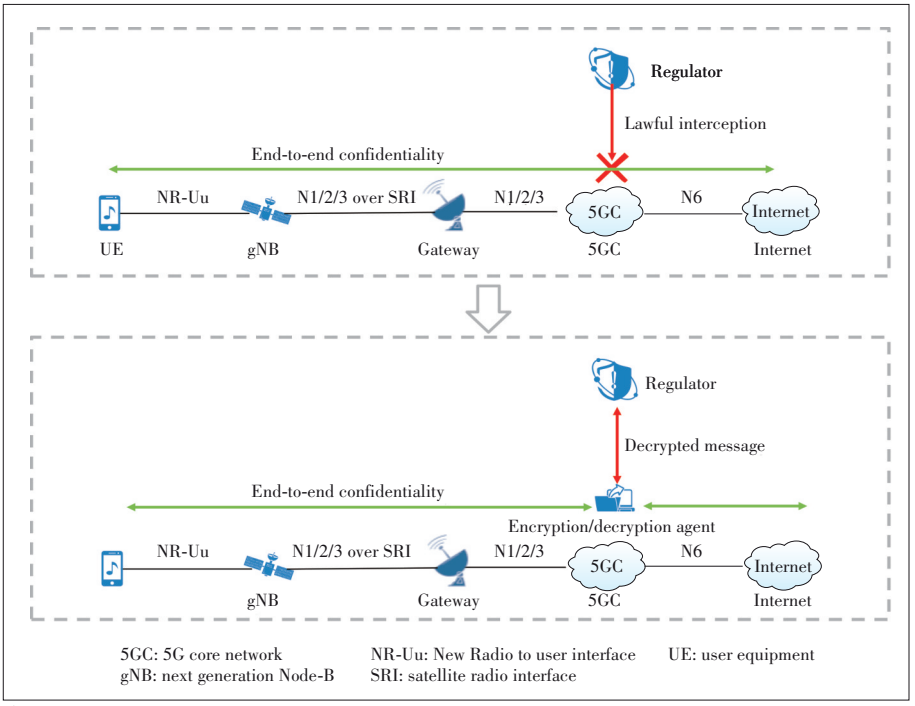
2) Solution 2: UE- NR CU security

The separate deployment of CU-DU can also effectively solve the contradiction between the protection of user data transmission and the weak processing capability of satellite nodes. As shown in Fig. 7, using the segmented encryption transmission scheme, the air interface enables PDCP-based confidentiality and integrity protection, and the N1/2/3 ports of the backhaul network and the N6 port of the data network can enable IPSec or DTLS protection as needed. The advantage of this solution is that the confidentiality and integrity of user data are processed on the UE and CU on the ground and the DU on the satellite does not participate in the process, so the transmission security of user data can be protected without increasing the cryptographic computing overhead of satellite nodes.

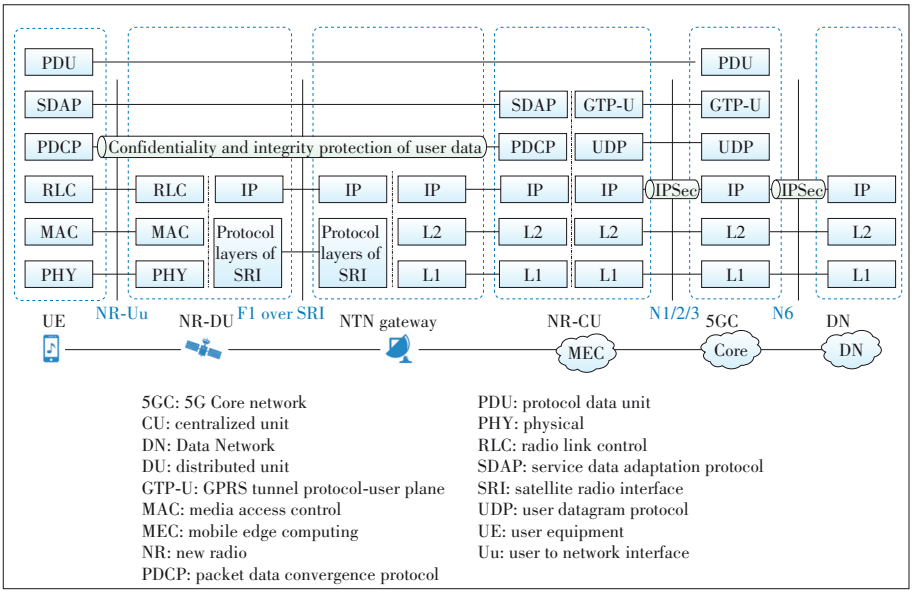
3) Solution comparison

The comparison between Solutions 1 and 2 is shown in Table 2.

The above two solutions can help 5G SCCN solve the contradiction between user data transmission protection and the weak processing capability of satellite nodes, so that the satellite nodes can avoid heavy cryptographic computing. Solution 1 realizes end-to-end



▲Figure 6. Schematic diagram of end-to-end encryption in user plane



▲Figure 7. Schematic diagram of CU-DU separated user plane encrypted communication

▼Table 2. Comparison of on-board security solutions without user plane encryption

Solution	Advantages	Disadvantages
Solution 1	1) End-to-end encryption 2) The intermediate network cannot obtain data and the level of privacy and security are high	1) The legal interception function is affected 2) VoLTE service quality is affected
Solution 2	1) Segmented encryption easy for security supervision 2) IMS service is not affected	It is possible for the network provider to obtain confidential user data

IMS: IP multimedia subsystem VoLTE: voice over Long-Term Evolution

encryption and integrity protection from terminal to service. Although it achieves higher security and privacy, it has a certain impact on legal monitoring and VoLTE services. While Solution 2 uses segmented encryption and decryption and integrity protection, posing requirements for network deployment.

The two solutions are not contradictory and can be used in combination. For general services, Solution 2 is recommended; for high confidential services, Solutions 1 and 2 can be activated simultaneously, so that critical data can be double protected.

4.3 Network Availability

Availability attacks on existing networks will still exist in 5G SCCN, such as electromagnetic interference, DDoS attacks and signaling storms. Considering the openness of the satellite network environment, lower processing capacity, and high value of the services carried, the security situation is severer.

In addition to the impact of unconscious group behavior on key resources, it is also necessary to combine the characteristics of 5G SCCN global coverage, focusing on the possibility of satellites suffering from availability attacks over the sea or in the air and enhancing the protection of signaling resources at each protocol layer. At present, the industry's protection measures for the availability of satellite networks are not yet systematic or effective, and research needs to be strengthened.

4.3.1 Anti-DDoS Attack

Although identity authentication can make the network reject a large number of unauthorized communications, there are still a certain number of protocol interactions without authentication, or authentication itself can also cause DDoS attacks.

DDoS attacks on the user plane can be effectively prevented by strengthening access authentication and single-session traffic rate limit. DDoS attacks on the control plane can use conventional security defense mechanisms, such as prohibiting Internet control message protocol (ICMP) packets and broadcast packets, adding access control list (ACL) filtering, and adding black and white lists. At the same time, there are still DDoS first-packet attacks on the control plane. A single-packet authorization mechanism can be considered. Meanwhile, special modules and cryptographic chips can be used on the user plane to reduce the consumption of CPU resources.

Considering the limitations of satellite network resources and complex defense strategies, new challenges have been posed to satellite resources. We can consider lightweight DDoS attack detection methods, such as self-organizing map (SOM)[26] and support vector machine (SVM)-SOM[27] technologies, building an unsupervised artificial neural network trained by traffic characteristics to detect DDoS attacks, or combining LSTM deep learning models and SVM technologies[28–29] to perform DDoS detection in spatial networks.

4.3.2 Anti-UE Random Access Attacks

Random competitive access of 5G NR may cause a signaling storm. For example, a base station malfunctions due to mass activities or large-area calls caused by disasters, which can usually be avoided by speed limiting. However, misuse of random access resources or malicious competition access, such as using a UE simulator to make a directional analog call to a specific satellite, will also make the satellite fail to access real and effective calls. Due to the asymmetry of space-ground computing resources, the possibility of such problems erupting in insecure areas also exists.

In order to avoid the aforementioned UE random access attack, the response message can be scrambled. For example, the satellite base station response message can be scrambled, so that the attacker cannot decode it correctly and no longer sends the radio resource request message to avoid occupying resources.

4.3.3 Anti-Wireless Communication Interference

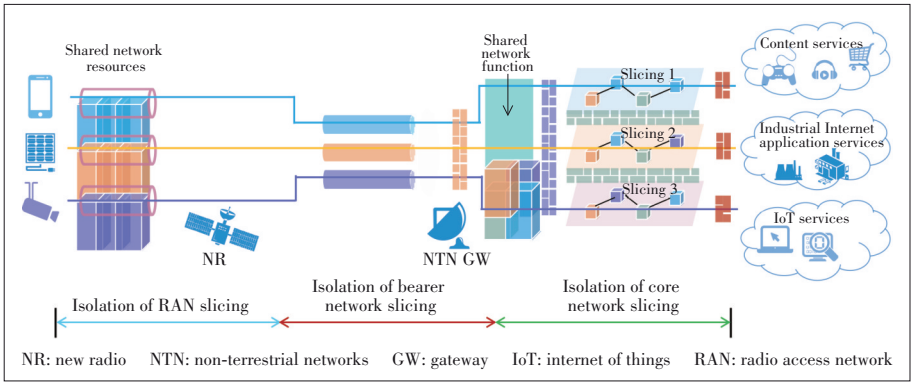
In the sea and sky environment, frequency band suppression attacks may occur. Since the ground transmission power can be several times that of the satellite, the attacker can track and aim the communication satellite and launch strong interference signals to the satellite, including blocking interference and noise interference, which greatly deteriorates the signal-to-noise ratio of the wireless channel. Meanwhile, the 5G frequency band is public, and it is easier for attackers to implement targeted frequency band suppression instead of full frequency band suppression, which will further increase the effectiveness of the attack. Using spot beam and line beam antenna technology to dynamically allocate wireless channels, increasing frequency band guard bands, improving filtering accuracy, and adopting frequency shift can cope with wireless communication interference to a certain extent.

4.4 Network Resource Sharing

Satellite resources are costly and space is limited, so limited satellite resources must be shared among multiple services. 5G SCCN resource sharing can refer to 5G network slicing technology. On the one hand, through the exploration of 5G in the field of Industrial Internet, 5G end-to-end network slicing technology has gradually matured, which provides a good foundation for the feasibility of 5G SCCN resource sharing. On the other hand, the existing 5G network slicing technology shares too large a granularity of resources and is not suitable for direct application on the 5G SCCN. 5G SCCN slicing requires more refined network resource management technology. Meanwhile, the network slicing technology of 5G SCCN also needs to be adaptively designed for other features such as the time-varying topology of satellite communication and network heterogeneity.

The end-to-end security isolation mechanism for network slicing includes RAN slice security isolation, bearer network

slice security isolation, and core network slice security isolation. Fig. 8 compares the 5G SCCN with the slicing technology. It can be seen that even in the manner of separate deployment of CU-DU, the two can be properly mapped. This shows that the 5G network slicing technology has reference significance for the 5G SCCN slicing technology.



▲Figure 8. Schematic diagram of 5G satellite converged communication network (SCCN) slice isolation

4.4.1 RAN Slice Isolation

The core technology of RAN slice isolation is the isolation of wireless spectrum resources, which divides the wireless spectrum into different resource blocks from the time domain, frequency domain, and space domain dimensions for air interface communication. This technology can still be applied in 5G SCCN. According to the requirements of different application scenarios, the use of resource pool reservation and allocation can realize the isolation of the wireless channel for the terminal to access the satellite. Limited by satellite resources, 5G SCCN slicing is likely to be service-oriented rather than industry-oriented.

4.4.2 Bearer Network Slice Isolation

The bearer network in the 5G SCCN includes the backhaul network and the middle-haul network, which will cover both the on-board link and the ground link. Currently, bearer network isolation mechanisms include logical virtual local area network (VLAN) isolation, and the Ethernet fragmentation technology (such as FlexE) to achieve physical isolation at the time slot level. Although FlexE has better security, the granularity of 5 Gbit/s is obviously not suitable for applications on satellite links.

Considering that the movement of satellites causes the network topology to dynamically change, the corresponding network slicing also needs to be dynamically adjusted. Although the satellite behavior can be predicted based on the ephemeris information, and the resources of the 5G SCCN bearer network can be planned and deployed in advance, this is still a complicated technical problem. In addition, issues such as the granularity of scheduling between on-board bearer network slicing and terrestrial bearer network slicing, protocol compatibility, and resource docking are also to be studied.

4.4.3 Core Network Slice Isolation

The core network in 5G SCCN is located on the ground, so it can inherit the existing 5G core network slicing technology. This part is relatively mature. Physical isolation can be used to allocate relatively independent physical resources to the slices with higher security requirements. A logical isolation solution can also be used to manage and orchestrate networks and network functions with the help of the virtualization technology.

5 Conclusions

The 5G network is expected to achieve wide-area coverage and integrated space-ground communications by converging with satellite networks. However, due to the characteristics of openness, dynamics, and low power consumption of satellite networks, 5G SCCN is faced with new security challenges. Based on the network mode proposed by 3GPP TR38.811, this paper conducts a comprehensive analysis from the three dimensions of network structure, network layering and security attributes, and constructs the security architecture of the 5G SCCN, so that readers can get an overall and specific understanding of the 5G SCCN from a security perspective.

By analyzing the security attributes of each layer and segment of the 5G SCCN, four key security technologies can be summarized, namely, strict identity authentication, lightweight data communication security, enhanced network availability, and fine-grained resource sharing and isolation. Based on strict identity authentication, building a relatively independent and trustworthy communication system in an open environment is a key feature that distinguishes the 5G SCCN from the traditional 5G network. Based on the principle of "forwarding on-satellite, processing off-satellite" and NR's CU-DU separate deployment, a lightweight communication security assurance for 5G SCCN can be provided. This is also a reference for the network design that this paper put forward from a security perspective. Based on new radio and signaling protection technologies, the availability of 5G SCCN services over the sea and in the air is enhanced; Based on the refined network resource management technology, fine-grained resource sharing and isolation for 5G SCCN applications is provided.

All in all, the 5G SCCN can inherit the existing security mechanisms and technologies of 5G networks and IP bearer networks to a large extent. There is no need to start anew for its security or design a completely different set of security architecture and protocol, but it should also be seen that the new network after integrating is faced with huge challenges. It is necessary to systematically design the network security architecture. Meanwhile, it is also necessary to fully consider the network security requirements at the architecture design phase.

References

[1] 3GPP. Study on new services and markets technology enablers: 3GPP TR 22.891 V14.2.0 [S]. 2016
[2] XU B Y, HAN M. Study on international standards of satellite communications [J]. Information and communications technology and policy, 2019, (17): 41 - 44
[3] WANG C T, LI N, ZHAI L J, et al. Preliminary study on the integration of satellite communications and terrestrial 5G network [J]. Satellite & network, 2018, (9): 14 - 21
[4] KONSTANTINOS L, ALEXANDER G, RAY S, et al. Use cases and scenarios of 5G integrated satellite-terrestrial networks for enhanced mobile broadband: the SaT5G approach [J]. International journal of satellite communications and networking, 2019, 37(2): 91 - 112
[5] LIU S J, HU Y M, WANG D P. Overview of studies on the satellite-5G integration [J]. Information and communications technology and policy, 2019, (5)
[6] SHEN Y Y. The Development trend of satellite communications in 5G era. Space international [J]. 2020, (1): 48 - 52
[7] CRUICKSHANK H, IYENGAR S, SUN Z L. Securing IP multicast over GEO satellites [C]//IEEE Seminar on Broadband Satellite: The Critical Success Factors Technology, Services and Markets. London, UK: IEEE, 2000. DOI: 10.1049/ic: 20000534
[8] NOUBIR G, ALLMEN LVON. Security issues in Internet protocols over satellite links [C]//50th Vehicular Technology Conference. Amsterdam, Netherlands: IEEE, 1999: 2726 - 2730. DOI: 10.1109/VETECF.1999.800282
[9] ROY-CHOWDHURY A, BARAS J S, HADJITHEODOSIOU M, et al. Security issues in hybrid networks with a satellite component [J]. IEEE wireless communications, 2005, 12(6): 50 - 61. DOI: 10.1109/MWC.2005.1561945
[10] JIANG Y W, ZHANG G X, ZHAO L D, et al. Summary of satellite communication and 5G convergence system development [C]//The 15th Annual Conference of satellite Communication. Beijing, China: CIC, 2019: 56 - 65
[11] CHEN S Z, SUN S H, KANG S L. System integration of terrestrial mobile communication and satellite communication-the trends, challenges and key technologies in B5G and 6G [J]. China communications. 2020, 17(12): 16
[12] KODHELI O, GUIDOTTI A, VANELLICORALLI A. Integration of Satellites in 5G through LEO Constellaions [C]//IEEE Global Communications Conference. Singapore, Singapore: IEEE, 2017: 1 - 6. DOI: 10.1109/GLOCOM.2017.8255103
[13] CHEN T T, WANG W J, DING R, et al. Location-based timing advance estimation for 5G integrated LEO satellite communications [C]//IEEE global communications conference. Taipei, China: IEEE. 2020: 1 - 6. DOI: 10.1109/GLOBECOM42002.2020.9322428
[14] TANG Q Q, XIE R C, LIU X, et al. MEC enabled satellite-terrestrial network: architecture, key technique and challenge [J]. Journal on communications, 2020, 41(4): 162 - 182
[15] ZHANG Z, ZHANG W, TSENG F H. Satellite mobile edge computing: improving QoS of high-speed satellite-terrestrial networks using edge computing techniques [J]. IEEE Network, 2019, 33(1): 70 - 76
[16] LI F H, YIN L H, WU W. Research status and development trends of security assurance for space - ground integration information network [J]. Journal on communications. 2016, (11): 160 - 172
[17] JI X S, LIANG H, HU H C. New thoughts on security technologies for space-ground integration information network [J]. Telecommunications science. 2017, (12): 30 - 41
[18] Huang Zhan. Research on security protocol of broadband satellite network [D]. Harbin Institute of Technology, 2012
[19] ITU-R M. Key elements for integration of satellite systems into next generation access technologies [EB/OL]. (2019-07-02) [2021-04-06]. https://www.itu.int/md/r15-wp5d-c-1263/en
[20] 3GPP. Study on new radio (NR) to support non-terrestrial networks: TR 38.811 V15.4.0 [S]. 2020
[21] 3GPP. Study on using satellite access in 5G: 3GPP TR 22.822 V16.0.0 [S]. 2018
[22] 3GPP. Study on scenarios and requirements for next generation access technologies: 3GPP TR 38.913 V16.0.0 [S]. 2020
[23] 3GPP. Study on architecture for next generation system: 3GPP TR 23.799 V14.0.0 [S]. 2016
[24] 3GPP. Service requirements for the 5G system: 3GPP TS 22.261 V17.2.0 [S]. 2020
[25] ZHANG Z J, ZHOU Q, ZHANG C. New low-earth orbit satellites authentication and group key agreement protocol [J]. Journal on communications. 2018, (6):150 - 158. DOI: 10.11959/j.issn.1000 - 436x.2018102
[26] BRAGA R, MOTA E, PASSITO A. Lightweight DDoS flooding attack detection using NOX/OpenFlow [C]//IEEE Local Computer Network Conference. Denver, USA: IEEE, 2010: 408 - 415. DOI: 10.1109/LCN.2010.5735752
[27] DEEPA V, SUDAR K M, DEEPALAKSHMI P. Detection of DDoS attack on SDN control plane using hybrid machine learning techniques [C]//International Conference on Smart Systems and Inventive Technology. Tirunelveli, India: IEEE, 2018: 299 - 303. DOI: 10.1109/ICSSIT.2018.8748836
[28] JIA M, SHU Y J, GUO Q, et al. DDoS attack detection method for space - based network based on SDN architecture [J]. ZTE communications, 2020, 18 (4): 18 - 25. DOI: 10.12142/ZTECOM.202004004
[29] YANG L F, ZHAO H. DDoS attack identification and defense using SDN based on machine learning method [C]//The 15th International Symposium on Pervasive Systems, Algorithms and Networks (I - SPAN). Yichang, China: IEEE, 2018: 174 - 178. DOI: 10.1109/I - SPAN.2018.00036

Biographies

YAN Xincheng (yan.xincheng@zte.com.cn) received his M.S. degree from Southeast University, China in 2004. He is currently the chief system architect and director of the Security Technology Committee of ZTE Corporation, responsible for network security technology planning. He was the leader of the network security sub-project of the "New Generation Broadband Wireless Network Communication Network" and National Science and Technology Major Project "5G Security Overall Architecture Research and Standardization". He has been awarded a number of scientific and technological awards of Jiangsu Province and Shenzhen.

TENG Huiyun received her M.S. degree from Hohai University, China in 2011. She is currently the senior technical research engineer in ZTE Corporation and has 10 years of professional experience in communication and security.

PING Li received her M.S. degree from Southeast University, China in 2005. She is currently the senior cybersecurity analyst in ZTE Corporation with 8 years of professional experience in cybersecurity policy and technology research and analysis. She got the CISSP in 2018.

JIANG Zhihong received his M.S. degree from Nanjing University of Posts and Telecommunications, China in 2003. He is currently the senior technical research expert in ZTE Corporation.

ZHOU Na received her Ph.D. degree from Nanjing University of Aeronautics and Astronautics University, China in 2004. She is currently the senior technical research expert in ZTE Corporation. She has won Shenzhen Scientific and Technological Award.