Hindawi
Security and Communication Networks
Volume 2022, Article ID 2200546, 14 pages
https://doi.org/10.1155/2022/2200546

Research Article

An Efficient Authentication and Key Distribution Protocol for Multicast Service in Space-Ground Integration Network

Wenlong Kou,[1] Wei You ,[1] Sheng Li,[1] Xiaoping Shi,[1] Ruhui Ma,[1] and Chao Guo [2,3]

[1]*School of Cyber Engineering, Xidian University, Xi'an 710126, China*
[2]*The State Key Laboratory of Integrated Services Networks, Xidian University, Xi'an 710126, China*
[3]*Communication Engineering Department, Beijing Electronic Science and Technology Institute, Beijing 100070, China*

Correspondence should be addressed to Wei You; wyou@xidian.edu.cn

Received 25 January 2022; Revised 22 February 2022; Accepted 8 March 2022; Published 28 March 2022

Academic Editor: Zhen Wang

Satellite communication technology has attracted the attention of researchers in the study of the sixth-generation (6G) mobile communication network because of its advantages of achieving global coverage with high cost-effectiveness and not being affected by terrain factors and human activities. In order to achieve efficient interconnection between terminals and networks, it is a new development trend of communication technology to integrate satellite communication networks and ground communication networks to construct the Space-Ground Integration Network (SGIN). Multicast service is widely used by network service providers to provide business services to users. Due to the characteristics of higher delay of space communication and unstable link compared with the ground network, if the ground multimedia multicast security protocol is directly applied to the space communication, it is difficult to guarantee the efficiency of the corresponding business service. The existing security protocols in the space information network are usually designed to ensure the security of end-to-end communication, and there are few studies on the security of multimedia multicast services. In view of the above situation, we design a new multicast service security protocol for the SGIN to realize the secure and efficient transmission in multicast services. In the protocol, we first design a key derivation scheme for the shared key between UE and BM-SC based on the existing 5G-AKA mechanism. Then, we propose a group-based multicast service registration mechanism. Finally, we propose a secure and efficient key distribution and update process of multicast service group key based on China Remainder Theorem (CRT). The formal verification tool Scyther is employed to analyze the security of the proposed protocol, and the results show that our scheme has valid security properties. We analyze the performance of the scheme by comparing it with the existing schemes in three aspects, such as signaling overhead, computational overhead, and bandwidth overhead. The comparison results show that our scheme is superior to other existing schemes. Finally, we build an experimental environment and test the delay, transmission rate, and CPU usage of the proposed system. The results show that our scheme improves the efficiency of multicast services while ensuring network security.

1. Introduction

With the rapid development of ground communication network technology for large-scale applications, users not only have more diversified demands on network service types but also have higher requirements on service of quality. Since the coverage of ground network is limited based on the construction conditions and maintenance costs of ground infrastructure in different regions, satellite communication technology has attracted extensive attention in the planning of the 6G mobile communication network for its features of easy global coverage, negligible impact of terrain and human activities on the ground, and low cost of global coverage compared with ground networks [1].

At present, high throughput Geosynchronous Earth Orbit (GEO) satellite is the main carrier of satellite communication services. GPS, GLONASS, BeiDou, Galileo, and other satellite navigation systems mainly use the Middle Earth Orbit (MEO) satellites to provide positioning and navigation services for ground mobile terminals. Since SpaceX launched the first batch of Starlink satellites in 2019, the large-scale satellite network technology in Low Earth

Orbit (LEO) has become a new technology solution to provide efficient communications around the world. To realize the efficient interconnection of any time, any space, and any terminal, it is a new development trend of communication technology to construct the Space-Ground Integration Network (SGIN) by integrating multilayer satellite communication network and ground communication network [2–5].

In the case of transnational, cross-domain, or lack of ground network coverage, ground network service providers usually choose the satellite network to relay and then send to the authorized ground users in the way of multicast communication, to provide services for the global ground users. However, as the global network of LEO satellites rapidly builds up in orbit and the number of low-cost satellites proliferates, small satellites are increasingly exploring the use of software-defined capabilities to enable in-orbit reprogramming, which brings a host of security concerns from privacy theft to satellite control [6]. A higher level of security is needed between satellites and Earth stations to protect them from attackers. Once an attacker takes control of a satellite, it could easily shut it down and deny service. Satellite signals can also be interfered with or spoofed by attackers, causing serious impacts on critical infrastructure such as power grids, water supply networks, and transportation systems [7]. The security of multicast service in the terrestrial mobile communication system is regulated by 3GPP standards. However, due to the high communication delay and poor link stability in the SGIN, it is difficult to guarantee service efficiency if the ground multimedia multicast security protocol is directly applied. The existing security protocols in space information networks are usually designed to ensure the security of end-to-end communication, but the security of multimedia multicast services is seldom considered.

The multicast service security protocol of the SGIN not only needs to satisfy the accuracy and efficiency of user identity authentication by service providers but also needs to guarantee the confidentiality and integrity of service content. At the same time, it should be convenient for new users to join and leave. In this paper, based on the Security of Multimedia Broadcast/Multicast Service (MBMS) in 3GPP TS 33.246 V16.0.0 [8], a new multicast service security protocol for the SGIN is designed, aiming at the network characteristics of long delay and high jitter. By optimizing the process of multikey protection, integrating the process of the access authentication protocol, and using predistribution key instead of Generic Bootstrapping Architecture (GBA) interactive key generation [9], the balance between network security and efficiency is finally achieved. The contributions are summarized as follows:

(1) With the help of the existing 5G Authentication and Key Agreement (AKA) mechanism [10], the secure derivation and distribution of the shared key of multicast service between User Equipment (UE) and Broadcast-Multicast Service Centre (BM-SC) is completed. The proposed protocol simplifies the multiround interaction process through the GBA mechanism in 4G MBMS.

(2) A group-based multicast service registration mechanism is proposed. Massive users can initiate multicast service registration requests to BM-SC at the same time, which largely reduces computational overhead and bandwidth overhead. In addition, the signaling conflicts can be avoided when massive users access the BM-SC to obtain multicast services at the same time.

(3) The secure and efficient distribution of the multicast service group key is completed by using the China Remainder Theorem (CRT). It simplifies the key layering mechanism, improves the efficiency of key management, and ensures the security of multicast service data transmission.

(4) A dynamic update mechanism for multicast service group key is proposed to ensure that the newly added member cannot obtain the previous multicast service data, and the exiting member cannot obtain the subsequent multicast service data.

(5) We use the formal verification tool Scyther to analyze the security of the scheme, and the results show that our scheme has good security properties.

(6) Compared with the existing schemes in terms of signaling overhead, computational overhead, and bandwidth overhead, the comparison results show that our scheme has superiority in performance.

(7) Finally, we built an experimental environment according to the proposed scheme and tested the delay, transmission rate, and CPU usage of the system. The results show that our scheme improves the efficiency of multicast services on the premise of ensuring network security.

This work is structured as follows. Section 2 mainly describes the existing research related to the security protocol of the SGIN. Section 3 introduces the knowledge of the Chinese Remainder Theorem. Section 4 establishes the system model according to the requirement of the network multicast service. In Section 5, a new security protocol for network multicast service in the SGIN is designed. The security analysis of the proposed protocol is described in Section 6. In Section 7, we present the performance analysis. The conclusion is outlined in Section 8.

2. Related Work

SGIN security not only involves the security strategies adopted by the ground segment and the space segment respectively but also includes the fusion of security protocols when information is transmitted across domains. The service security protocols in the ground mobile network are relatively mature by mainly using the 4G MBMS security protocol and 5G-AKA mechanism released by 3GPP committee. The security technology of satellite communication is relatively slow in development. The security protocols published mainly include the Space Communication Protocol Specification-Security Protocol (SCPS-SP) [11] and Space Data Link Security (SDLS) [12] formulated by the Consultative Committee for Space Data Systems

(CCSDS), the Digital Video Broadcasting (DVB) series security protocols [13] proposed by the European Telecommunication Standards Association (ETSI), the Bundle Security Protocol (BSP) in Delay-Tolerant Network (DTN) [14], and the GEO-Mobile Radio (GMR) [15] security design mainly for high orbit narrow-band satellite mobile communication system. Since the communication frequency, bandwidth, and power resources of satellite networks are severely limited, it is necessary to reduce protocol redundancy while increasing network security. Therefore, designing a multicast service security protocol for the SGIN characterized by large-scale, heterogeneous, and highly dynamic topology is challenging.

The existing classical satellite network security protocols mainly design security strategies for data encryption, authentication, access control, and privacy protection at the data link layer or network layer to achieve the confidentiality and integrity of data and prevent the illegal use of network resources. SCPS-SP is applied between the network layer and the transport layer in the system. After processing the Transport-Protocol Data Unit (T-PDU), it is encapsulated into Security-Protocol Data Unit (S-PDU). According to the different security requirements of users, it provides end-to-end data confidentiality, integrity, and authentication security services for these T-PDUs. However, the single encryption algorithm and security protection measures of the same level in SCPS-SP are difficult to adapt to the data security guarantee of multinetwork integration. SDLS is implemented through an additional security sublayer between the data link layer and the network layer. It provides security services including authentication, encryption, and authentication encryption but does not provide security guarantees against denial of service and traffic analysis.

The DVB-RCS2 protocol standard [16], as the first industry standard proposed for satellite interactive application, defines a security architecture that can provide channel activity information protection, control, and management information protection, Network Control Centre (NCC), and Return Channel via Satellite Terminal (RCST) authentication, antijamming, and ground intercept probability functions. However, the protocol has a hidden danger of man-in-the-middle attack. The DTN research group proposed a delay-tolerant message-oriented overlay architecture, which is the Bundle layer between the transport layer and the application layer. The Bundle Security Protocol (BSP) provides DTN with a basic security mechanism including end-to-end security and hop-by-hop security. Because the DTN network cannot establish a path from the source node to the destination node before data transmission, it is difficult to achieve routing security and multicast security by using BSP. GMR standard protocol refers to the 2G/3G system protocol of the ground cellular network. The GMR standard protocol mainly includes the following secure functions: International Mobile Subscriber Identity (IMSI) confidentiality, IMSI authentication, user data confidentiality, signaling information element confidentiality, and International Mobile Equipment Identity (IMEI) confidentiality. The rapid iteration of ground mobile communication technology makes satellite mobile communication adapt to the new 5G or the future 6G mobile communication system protocol.

In recent years, several key technologies such as encryption, authentication, and key management have been improved in satellite security protocols [17–28]. Arezou et al. proposed a three-factor user authentication and session key protocol based on elliptic curve cryptography [17]. The scheme provided reliable temporary secret, antileak attack, and perfect forward secret in satellite networks, but it has relatively high computational complexity. Izwa et al. proposed a lightweight authentication and key agreement scheme for LEO satellite communication by using a one-way hash function to improve the security of the protocol [18]. It protected against offline password guessing, replay, stolen verifier, impersonation, and denial of service attacks. An authentication and key update scheme was proposed by Zhang et al. which achieved user anonymity and reduced the protocol overhead by adopting the hash algorithm [19]. However, Qi et al. analyzed that Zhang's schemes could not resist the stolen verifier attack and the denial of service attack and lacked the invalid user update process, and the database query was complicated in practice. Therefore, they proposed an enhanced authentication scheme to resist these two attacks, in which users must hold a legal smart card to complete the authentication, and did not need to maintain the verifier table [20]. Subsequently, a secure authentication mechanism based on elliptic curve cryptography and symmetric cryptography was proposed by Qi et al. [21]. Different from the previous two schemes, the ground control center in this scheme would not obtain the user's password information, and it allowed the user side to update the password information according to their own needs, giving them a better user experience. Yang et al. realized the user's identity anonymous roaming authentication under Space Information Network (SIN) [22]. They verified the legitimacy of user identity using group signatures, using the elliptic curve signature algorithm to verify satellite and ground station identity. In addition, physical layer security [23, 24], blockchain [25, 26], and quantum technology [27, 28] are hot topics in solving the security problems of satellite networks. However, physical layer security technology is more suitable for the point-to-point communication security guarantee, blockchain technology requires high computing, storage, energy resources, and quantum key distribution, and other security technologies are in the exploration stage. Most of the above research are devoted to improving the security and communication efficiency of satellite or ground network, but it is difficult to solve the problem of secure and efficient transmission across domains in the SGIN.

To provide secure and efficient multicast services in the SGIN, it is necessary to design a simple and reliable protocol flow based on existing ground and satellite network security protocols. According to the characteristics of network services, key technologies such as shared key derivation and distribution, group multicast service registration, group key distribution, and group key dynamic update should be optimized. Finally, the secure transmission of multimedia multicast service between ground segment and space segment is realized.

3. Preliminary

The Chinese Remainder Theorem is an important theorem in number theory, which is used to solve the system of linear congruence equations [29]. In order to solve the answer quickly, mathematicians use the structured approach to give the specific form of the general solution. Let $m_1, m_2, \ldots, m_k$ be a set of pairwise relatively prime positive numbers; then, for any given k positive integers, $a_1, a_2, \ldots, a_k$, the system of linear congruence equations, $x \equiv a_1 \,(\mathrm{mod} m_1), x \equiv a_2 \,(\mathrm{mod} m_2), \ldots, x \equiv a_k \,(\mathrm{mod} m_k)$, has a general solution. Let $m = m_1 m_2 \ldots m_k$ be the product of the moduli.

For each i with $1 \leq i \leq k$, let $M_i = m/m_i$. Notice that since the moduli are relatively prime and M_i is the product of all the moduli other than m_i, M_i has an inverse element modulo m_i, say M_i^{-1}, which meets the condition $M_i M_i^{-1} \equiv 1 \,(\mathrm{mod} m_i)$. Then there is the unique $x \,(\mathrm{mod} m)$ such that $x \equiv M_1 M_1^{-1} a_1 + \cdots + M_i M_i^{-1} a_i + \cdots + M_i M_k^{-1} a_k \,(\mathrm{mod} m)$ for all $1 \leq i \leq k$.

4. System Model and Design Objectives

4.1. System Model. As shown in Figure 1, our Space-Ground Integration Network model consists of 6 parts: ground-based node networks, space-based node networks, gateway, content provider, Home Subscriber Server (HSS), and BM-SC. Through this integrated system, a UE can connect to the BM-SC via the satellite and obtain multicast services.

(1) Ground-based node networks, which consist of different types of UEs, are requesters/initiators of multicast services.

(2) Space-based node network, which consists of multiple satellites, is the access network in the architecture. It is mainly responsible for forwarding and processing messages between the UE and the core network.

(3) Content provider is the provider of data in the system.

(4) HSS is a core network element that stores the mapping relationship between User Security Settings (USSs) and user identity identifiers, that is, IMSIs. In our model, the HSS will provide the user's USS and IMSI to the BM-SC.

(5) BM-SC is an organization with functions such as key distribution, key update, data transmission, and member authority management.

4.2. Design Objectives. The proposed scheme is to realize the access authentication of UE in multicast services and the group key agreement between users and the BM-SC. Our scheme should meet the following security requirements:

(1) Mutual authentication: The scheme needs to complete entity identity authentication between the UE and the BM-SC. Based on this, the scheme realizes that only authorized legal users can use multicast services, and only legal BM-SCs can provide users with real and reliable data information.

(2) Resistance to protocol attacks: Our scheme is expected to resist entity impersonation attacks, replay attacks, man-in-the-middle attacks, and so on.

(3) Conditional anonymity: Our scheme is expected to realize the anonymity of user identity to protect the privacy of users; that is, users do not use their real identity to interact in the network but through temporary identification,

(4) Unlinkability: Unlinkability means that an attacker cannot determine whether two messages are sent by the same user.

5. The Proposed Authentication Scheme

In this section, we introduce the shared key agreement process which improves the 5G AKA mechanism [30], the group-based multicast service registration process, the group key distribution process, and the key update process based on the CRT. In these processes, we implement the mutual authentication and key agreement between the UEs and the BM-SC in multicast service and update keys when group membership changes. Specifically, our scheme includes the following: (1) the shared key agreement process between the UE and the BM-SC, (2) the user multicast service registration process, (3) the multicast key distribution process, and (4) the key update process. We will describe our proposed scheme in detail as follows.

5.1. Shared Key Agreement Process in Multicast Service. As shown in Figure 2, our scheme realizes the identity authentication of the UE based on the 5G AKA mechanism at this stage to verify whether the user is authorized to access the network. During this process, we also negotiate a session key K_i, a random prime number Z_i, and the user temporary identity identifier TID_i shared between UE_i and BM-SC. K_i will be used for the generation of the important parameter MRK_i in the multicast service registration process. The key distribution process is implemented by relying on Z_i. The specific steps are described as follows:

(1) First, the UE_i generates a prime number Z_i and uses the public key of Home Network (HN) to encrypt and generate $\{Z_i\}_{pb}$ and sends the access authentication request message $(SUCI, \{Z_i\}_{pb}, (mbs_{req}))$ to the ground Service Network (SN) through the satellite network, where the $SUCI$ is the terminal identity in the 5G AKA authentication process defined by the 3GPP committee, and mbs_{req} is the multicast service request flag and its length is 1 bit.

(2) Subsequently, the SN sends the message $(SUCI, SN - \mathrm{Name}, \{Z_i\}_{pb}, mbs_{\mathrm{req}})$ to the HN, where $SN - \mathrm{Name}$ is the service network name in the 5G AKA authentication process.

(3) The UE performs the access authentication of the integrated space and ground network through the 5G-AKA mechanism.

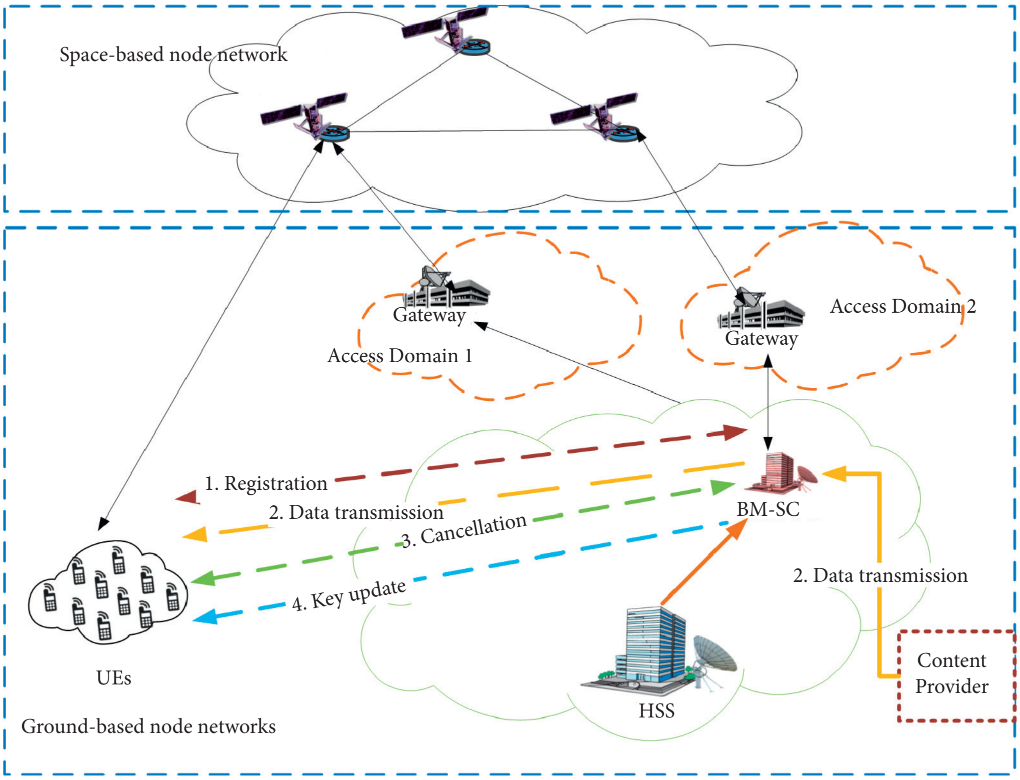
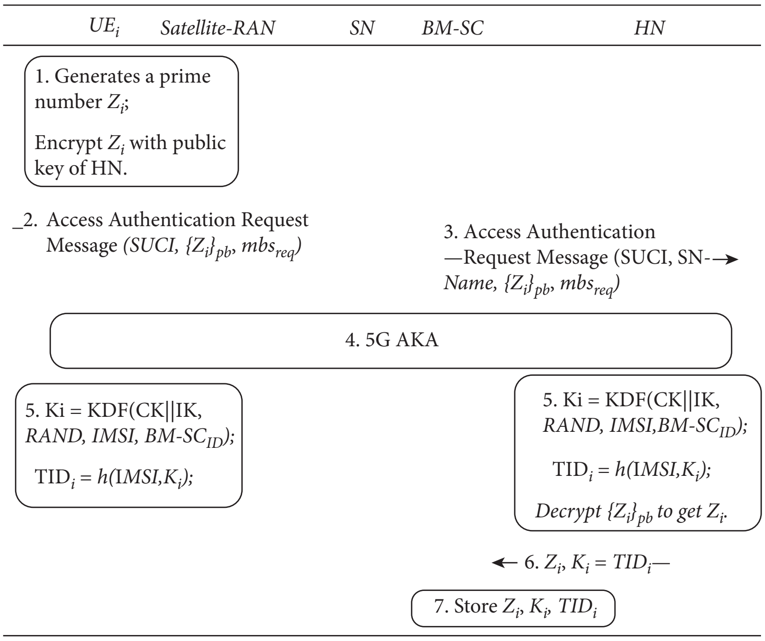


Figure 1: System model.



1. Generates a prime number Z_i;

Encrypt Z_i with public key of HN.

2. Access Authentication Request Message $(SUCI, \{Z_i\}_{pb}, mbs_{req})$

3. Access Authentication Request Message (SUCI, SN-Name, $\{Z_i\}_{pb}, mbs_{req}$)

4. 5G AKA

5. Ki = KDF(CK||IK, $RAND, IMSI, BM\text{-}SC_{ID}$);

$\mathrm{TID}_i = h(\mathrm{IMSI}, K_i)$;

5. Ki = KDF(CK||IK, $RAND, IMSI, BM\text{-}SC_{ID}$);

$\mathrm{TID}_i = h(\mathrm{IMSI}, K_i)$;

Decrypt $\{Z_i\}_{pb}$ to get Z_i.

6. $Z_i, K_i = TID_i$

7. Store Z_i, K_i, TID_i

Figure 2: The shared key establishment process between UE and BM-SC in case of multicast service.

(4) After the UE successfully passes the access authentication, the HN decrypts $\{Z_i\}_{pb}$ to obtain Z_i. The UE and the HN, respectively, derive the shared key $K_i = K\ DF(CK\|IK, RAN\ D, IMSI, BM - SC_{I\ D})$ and user temporary identity $TID_i = h(IMSI, K_i)$, where $K\ DF$ is the key derivation function, h is the one-way hash function, CK, IK, and RAND are the key negotiation parameters shared by the UE and the HN in the 5G AKA process, and $BM - SC_{\mathrm{ID}}$ is the identity of the BM-SC.

(5) Finally, the HN sends Z_i, K_i, and TID_i to the BM-SC.

5.2. Multicast Service Registration Process. In the previous stage, through the improved 5G AKA process, a secure channel has been established between the UE and the Satellite-RAN and between the Satellite-RAN and the BM-SC. As shown in Figure 3, the mutual authentication between multiple UEs and BM-SC is realized based on group authentication at this stage to verify in batches whether multiple users are legitimate users of multicast services. The specific process is as follows:

(1) The UE_i generates a random number r_i and then sends a multicast service registration request message (TID_i, r_i) to the Satellite-RAN.

(2) The Satellite-RAN sends all registration requests $(TID_1, TID_2, \ldots, TID_n,\ r_1, r_2, \ldots, r_n, uG_{\mathrm{id}},\ sRAN_{\mathrm{id}}, R_{\mathrm{sat}})$ received within a certain period of time to the BM-SC, where uG_{id} is used to identify the user group, $sRAN_{\mathrm{id}}$ is the identity of the Satellite-RAN, and R_{sat} is a random number generated by the Satellite-RAN.

(3) The BM-SC generates a random number R after receiving the message and obtains the long-term shared key K_i according to TID_i. Then the BM-SC sequentially calculates and stores the following parameters for the identity authentication of each UE: (1) multicast request key $MRK_i = K\ DF(K_i, \text{“}mbs_{\mathrm{mrk}}\text{”})$; (2) message authentication code $MAC_i = f_1(MRK_i, r_i, R)$; (3) authentication response value $XRES_i = f_2(MRK_i, r_i, R)$; (4) aggregated expected authentication response value $XRES_0 = XRES_1 \oplus XRES_2 \oplus \cdots \oplus XRES_n$; and (5) $HXRES = h(R, XRES_0)$. Finally, the BM-SC returns $(AUTN, HXRES, uGi\ d, R_{\mathrm{sat}})$ to the Satellite-RAN as a response to the service registration message, where $AUTN = R\|MAC_1\|\ldots\|MAC_n$. Note that f_1 and f_2 are one-way hash functions.

(4) The Satellite-RAN sends $AUTN_i = R\|MAC_i$ to the corresponding UE_i after receiving message.

(5) UE_i generates MRK_i, calculates $XMAC_i = f_1(MRK_i, r_i, R)$, and checks whether MAC_i is correct. If the verification is passed, UE_i calculates the message response value $RES_i = f_2(MRK_i, r_i, R)$ and returns it to the Satellite-RAN.

(6) After the Satellite-RAN receives the message, it calculates the aggregated response value $RES_0 = RES_1 \oplus RES_2 \oplus \cdots \oplus RES_n$ and $HRES = h(R, RES_0)$ and checks whether $HRES$ is equal to $HXRES$. If the two values are equal, it sends $(RES_0, uG_{\mathrm{id}})$ to the BM-SC.

(7) After the BM-SC receives the message, it verifies whether RES_0 is equal to $XRES_0$. If the verification is passed, UE_i's multicast service registration is completed.

5.3. Multicast Key Security Distribution Process. After successful registration, the BM-SC uses Z_i to realize the secure distribution of multicast group key based on the CRT. As shown in Figure 4, the specific process is as follows:

(1) Firstly, the BM-SC generates a random number GK as the group key, and executes the following process.

Step 1: $\partial g = \prod_{i=1}^{n} Z_i$.
Step 2: $X_i = \partial g / Z_i$.
Step 3: $Y_i \equiv X_i^{-1} (\mathrm{mod} Z_i)$.
Step 4: $\partial x_i y_i = X_i Y_i$.
Step 5: $a \equiv \sum_{i=1}^{n} \partial x_i y_i (\mathrm{mod}\ \partial g)$.
Step 6: $b = a \times GK$.

Then, the BM-SC sets the validity period of the group key ET_{GK} and then calculates $MAC_{GK} = h(b, ET_{GK}, GKI\ D)$, where $GKI\ D$ is the group key identifier.

(2) The BM-SC sends the message $(b, ET_{GK}, GKI\ D, MAC_{GK})$ to UE_i via the Satellite-RAN.

(3) After UE_i receives the message, MAC_{GK} is used to verify the integrity of the message, and $GK \equiv b(\mathrm{mod} Z_i)$ is obtained by one modulo division operation.

Then, the content provider transmits the multimedia multicast service (MMS) data to the BM-SC, and the BM-SC uses the group key GK corresponding to each service to encrypt the data and transmit the data to the users of the multicast service.

5.4. Group Key Update Process. In view of the situation that users of multicast services leave or join the group, we need to design the corresponding key update schemes. In section 5.3, we can see that b is the most important factor in the group key agreement request message, and UE_i can calculate the group key GK based on b and known Z_i. Therefore, we focus on the update of b, and the specific process is designed in four scenarios as follows:

(1) Group key update when a single user leaves

When UE_i leaves the group, the BM-SC reselects a group key GK' and calculates b according to the following steps:

Step 1: $a' \equiv a - \partial x_i y_i (\mathrm{mod}\ \partial g)$.
Step 2: $b' = a' \times GK'$.

(2) Group key update when a single user joins

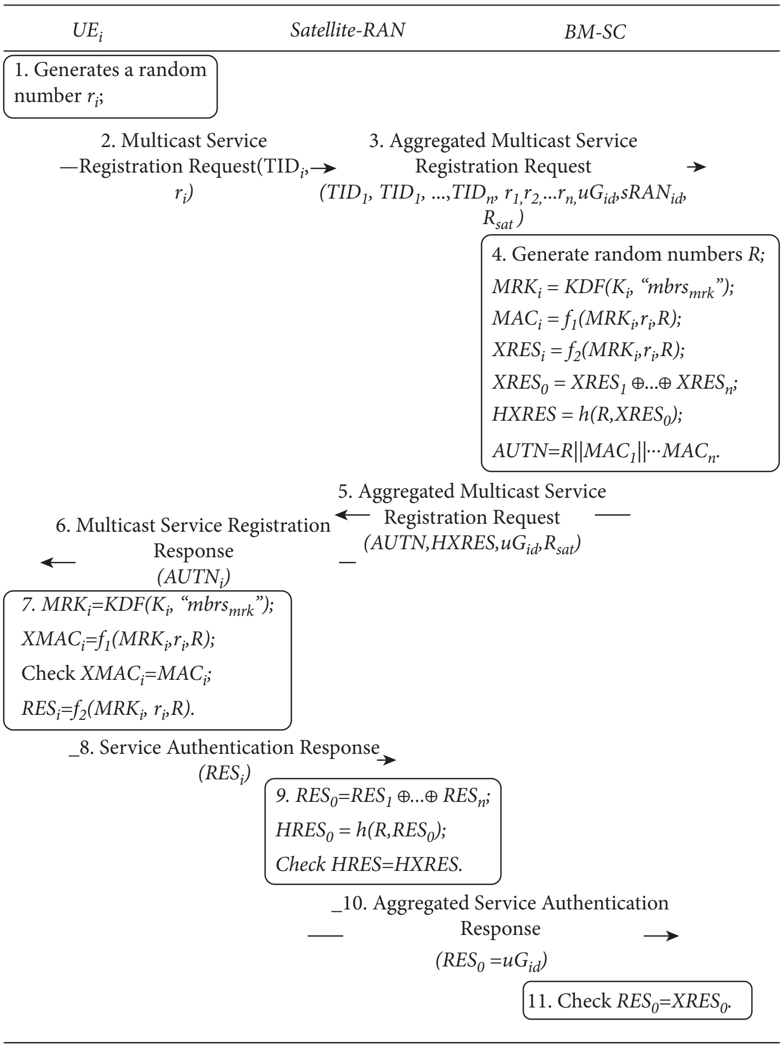

UE_i
Satellite-RAN
BM-SC
1. Generates a random number r_i;
2. Multicast Service Registration Request(TID_i, r_i)
3. Aggregated Multicast Service Registration Request
$(TID_1, TID_1, \ldots, TID_n, r_1, r_2, \ldots r_n, uG_{id}, sRAN_{id}, R_{sat})$
4. Generate random numbers R;
$MRK_i = KDF(K_i, \text{“}mbrs_{mrk}\text{”})$;
$MAC_i = f_1(MRK_i, r_i, R)$;
$XRES_i = f_2(MRK_i, r_i, R)$;
$XRES_0 = XRES_1 \oplus \ldots \oplus XRES_n$;
$HXRES = h(R, XRES_0)$;
$AUTN = R \| MAC_1 \| \cdots MAC_n$.
5. Aggregated Multicast Service Registration Request
$(AUTN, HXRES, uG_{id}, R_{sat})$
6. Multicast Service Registration Response
$(AUTN_i)$
7. $MRK_i = KDF(K_i, \text{“}mbrs_{mrk}\text{”})$;
$XMAC_i = f_1(MRK_i, r_i, R)$;
Check $XMAC_i = MAC_i$;
$RES_i = f_2(MRK_i, r_i, R)$.
8. Service Authentication Response
(RES_i)
9. $RES_0 = RES_1 \oplus \ldots \oplus RES_n$;
$HRES_0 = h(R, RES_0)$;
Check $HRES = HXRES$.
10. Aggregated Service Authentication Response
$(RES_0 = uG_{id})$
11. Check $RES_0 = XRES_0$.

FIGURE 3: The service registration process.

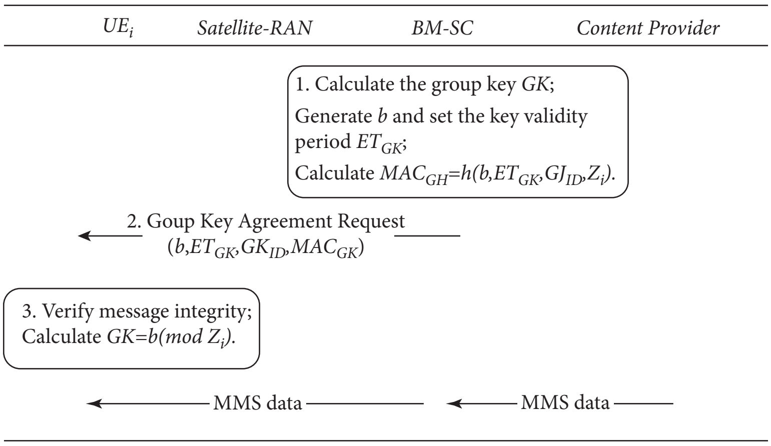

UE_i
Satellite-RAN
BM-SC
Content Provider
1. Calculate the group key GK;
Generate b and set the key validity period ET_{GK};
Calculate $MAC_{GH} = h(b, ET_{GK}, GJ_{ID}, Z_i)$.
2. Goup Key Agreement Request
$(b, ET_{GK}, GK_{ID}, MAC_{GK})$
3. Verify message integrity;
Calculate $GK = b(mod\ Z_i)$.
MMS data
MMS data

FIGURE 4: The multicast key security distribution process.

When UE_i joins the group, the BM-SC reselects a group key GK' and calculates b according to the following steps:

Step 1:

$$\begin{cases} a' \equiv a(\bmod \partial g), \\ a' \equiv 1(\bmod Z_i). \end{cases} \tag{1}$$

According to Equation (1), we can calculate

$$a' \equiv aZ_iZ_i^{-1}{}_{\bmod \partial g} + \partial g\, \partial g^{-1}{}_{\bmod Z_i}(\bmod \partial g\ Z_i). \tag{2}$$

Step 2: $b' = a' \times GK'$.

(3) Group key update when multiple users leave

When K UEs leave the group, the BM-SC reselects a group key GK' and calculates b according to the following steps. Here, K UEs are represented as $(UE_1, UE_2, \ldots, UE_k)$.

Step 1: $a' \equiv a - \sum_{i=1}^{k} \partial x_i y_i (\bmod \partial g)$.
Step 2: $b' = a' \times GK'$.

(4) Group key update when multiple users join

When K UEs join the group, the BM-SC reselects a group key GK' and calculates b according to the following steps. Here, K UEs are represented as $(UE_{n+1}, UE_{n+2}, \ldots, UE_{n+k})$.

Step 1: We set $Z_0 = \partial g$, $\partial g' = Z_0 \times \prod_{i=n+1}^{n+k} Z_i$.
Step 2:

$$X_i = \begin{cases} \dfrac{\partial g'}{Z_0}, & i = 0, \\ \\ \dfrac{\partial g'}{Z_i}, & i = n+1, n+2 \ldots n+k. \end{cases} \tag{3}$$

Step 3:

$$Y_i \equiv \begin{cases} X_i^{-1}(\bmod \partial g), & i = 0, \\ X_i^{-1}(\bmod \partial Z_i), & i = n+1, n+2 \ldots n+k. \end{cases} \tag{4}$$

Step 4: $\partial x_i y_i = X_i Y_i$.
Step 5: $a' \equiv a\ \partial x_i y_i + \sum_{n+1}^{n+k} \partial x_i y_i (\bmod \partial g')$.
Step 6: $b' = a' \times GK'$.

5.5. Key Layering Mechanism. Figure 5 shows our key layering mechanism. Based on the derived CK, IK in the 5G AKA mechanism and random prime number Z_i, we obtain the shared key K_i and random prime number Z_i between a UE and the BM-SC in the shared key agreement process of multicast service. The two keys are used in the multicast service registration and key distribution phases, respectively. The details are as follows:

(1) CK, IK: CK, IK are generated during the access authentication process between the UE and the HN based on the 5G AKA mechanism.

(2) Z_i: The random prime number Z_i is sent by the UE to the HN during the shared key agreement process of multicast service and forwarded by the HN to the BM-SC.

(3) K_i: K_i is derived by the UE and the HN according to CK and IK in the shared key agreement process of multicast service.

(4) MRK_i: MRK_i is derived by the UE and the BM-SC according to K_i in the multicast service registration stage and is used to realize the mutual authentication between the UE and the BM-SC.

(5) GK: In the key distribution stage, GK is the group key selected by the BM-SC, and the UE calculates GK according to Z_i.

6. Security Analysis

The proposed scheme includes user access authentication and shared key establishment, service registration, and group key distribution in multicast scenarios. Among them, the security of access authentication is guaranteed by the 5G AKA protocol securely, and the security of group key distribution is guaranteed by the CRT. In this section, we conduct the formal and informal security analyses for the service registration process.

6.1. Scyther Simulation. In this paper, we use the Scyther tool [31, 32] to verify the security of the service registration process. Scyther is an automated protocol analysis tool that is widely used in protocol security analysis. The security analysis using Scyther is based on the assumption of perfect cryptography; that is, the long-term shared key or private key is not leaked. During the security analysis, researchers can choose multiple security models such as Dolev-Yao and Canetti-Krawczyk. Scyther is suitable for fewer participating roles in the protocol, and the protocol itself relies on a third-party encryption protocol.

Researchers can analyze the proposed protocol through the following process based on the SPDL language. Firstly, the protocol is described by events such as sent and recv, so as to realize the modeling of the protocol. Secondly, Scyther uses the claim event to declare the expected security properties, such as Alive, Weakagree, Niagree, Nisynch, Commit, and Secret, to verify whether the protocol is resistant to replay attacks, man-in-the-middle attacks, and tampering and forgery.

During the analysis process, the Scyther tool explores all possible evidence trees for protocol attacks. By default, the space of the search tree is bounded, but the search range can be expanded by changing the parameters. Therefore, the protocol tool can achieve unbounded verification. If the search range is reached or all verifications are completed, Scyther will display the verification results on the graphical interface. If the verification is passed, the graphical interface will display "ok"; otherwise, the security attribute will display "fail" and give the existing attack graph.

Figure 6 shows the security simulation result of the service registration process. It can be seen from the figure

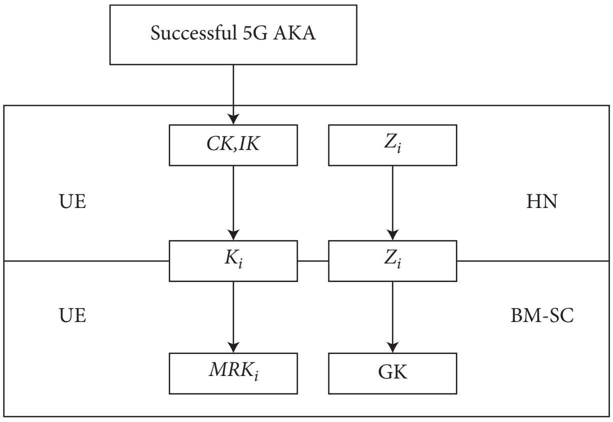
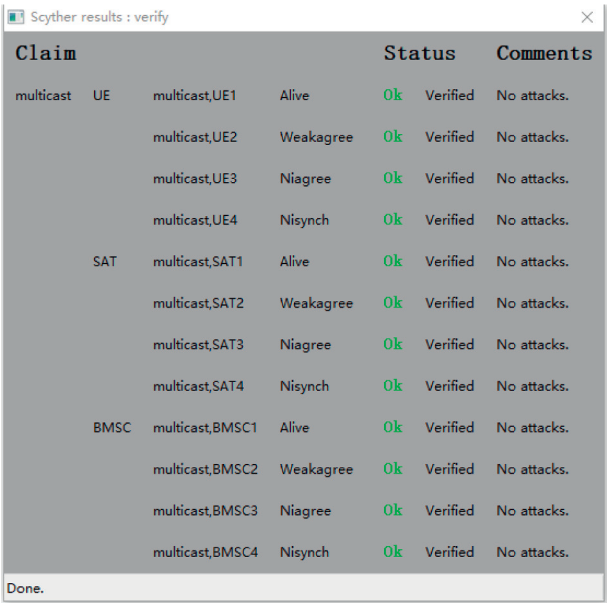


Figure 5: Key layering mechanism.



```
Claim                                          Status        Comments
multicast  UE     multicast,UE1     Alive       Ok  Verified  No attacks.
                  multicast,UE2     Weakagree   Ok  Verified  No attacks.
                  multicast,UE3     Niagree     Ok  Verified  No attacks.
                  multicast,UE4     Nisynch     Ok  Verified  No attacks.
           SAT    multicast,SAT1    Alive       Ok  Verified  No attacks.
                  multicast,SAT2    Weakagree   Ok  Verified  No attacks.
                  multicast,SAT3    Niagree     Ok  Verified  No attacks.
                  multicast,SAT4    Nisynch     Ok  Verified  No attacks.
           BMSC   multicast,BMSC1   Alive       Ok  Verified  No attacks.
                  multicast,BMSC2   Weakagree   Ok  Verified  No attacks.
                  multicast,BMSC3   Niagree     Ok  Verified  No attacks.
                  multicast,BMSC4   Nisynch     Ok  Verified  No attacks.
Done.
```

Figure 6: Security simulation result.

that there are three roles in our established model: UE, SAT, and BM-SC, which represent UE, Satellite-RAN, and BM-SC in the protocol, respectively. We use four claim types, Alive, Weakagree, Niagree and Nisynch, to describe our expected security properties. Meanwhile, in terms of security model, we choose the Dolev-Yao model. According to the analysis results, the security properties of our protocol are verified under the test; that is, the protocol can complete entity identity authentication and can resist replay attacks, message tampering and forgery, man-in-the-middle attacks, and so forth.

6.2. Informal Security Analysis. In this section, we analyze the security of the protocol from the perspective of the security requirements that the scheme needs to meet.

(1) Mutual authentication: In this scheme, on the one hand, the UE verifies the identity of the BM-SC by checking MAC_i in $AUTN_i$. On the other hand, the satellite network and the BM-SC perform the identity authentication on the UE, respectively. Specifically, the Satellite-RAN aggregates the authentication response value of the group user to obtain RES_0 and then generates $HRES = h(R, RES_0)$ and realizes the authentication of the UE by comparing whether $HRES$ and $HXRES$ are equal. After the authentication, the Satellite-RAN forwards the aggregated message RES_0 to the BM-SC to authenticate the UE.

(2) Conditional anonymity: The anonymity of the UE is achieved through the temporary identity $TI\ D$. The Satellite-RAN and the BM-SC do not store the mapping table of the user's real identity and temporary identity, and the one-way hash algorithm makes it impossible to obtain the user's real identity through reverse operation. Therefore, the UE can realize the identity anonymity for the Satellite-RAN, the BM-SC, and other users and adversaries. At the same time, this anonymity is conditional. The HN locally stores the IMSI corresponding to the TID, so the HN can obtain the real identity of the UE.

(3) Resistance to replay attacks: In our scheme, we employ a double random number mechanism. Each entity will add random numbers when sending messages, such as R_{sat}, R. If a received message contains a previously received random number, then the message will be ignored, which prevents replay attacks.

(4) Resistance to impersonation attacks: Impersonation attack refers to an attacker impersonating the identity of a legitimate authorized user. In our solution, the access authentication is implemented for users based on the 5G AKA process in the first stage, and the mutual authentication between the UE and the BM-SC is implemented for users in the registration process. If an attacker wants to impersonate an identity, he needs to calculate RES, but the lack of K_i makes him unable to succeed.

(5) Resistance to man-in-the-middle attacks: A man-in-the-middle attack means that an attacker needs to

pretend to be both sides of the conversation so that they think they are communicating with each other directly. In our scheme, the mutual authentication is achieved between the UE and the BM-SC, so there is no possibility of attackers masquerading successfully.

(6) Unlinkability: The one-way hash function and random number RAND are used in the generation of the user's temporary identity, which makes it impossible for an attacker to determine that two $TI\ Ds$ belong to the same user and that two messages belong to the same user.

7. Performance Analysis

In this section, we evaluate the performance of our scheme by comparing it with existing schemes [18–22] in terms of computational overhead, bandwidth overhead, and signaling overhead, which are three important aspects for evaluating the performance.

In addition, we built an experimental environment based on our scheme and measured the delay of the registration and key distribution process, the data transmission rate, and the CPU usage to further evaluate the performance of our scheme.

7.1. Signaling Overhead. Since multiple users are often involved in multicast service registration, we compare the signaling overhead of our proposed scheme and the previous scheme when n users perform the registration process. Table 1 shows that the signaling overhead of our scheme is only slightly higher than that of the scheme in [22] and lower than those of other schemes because our scheme adopts the way of aggregating messages. With the increasing of the number of users, our scheme has more significant advantages in signaling overhead, which shows that our scheme can effectively alleviate the signaling conflict when a large number of users concurrently execute the service registration process.

7.2. Computational Overhead. In terms of the computational cost of the registration process, it involves the time cost of various operations: XOR operation T_x, concatenation T_c, exponential operation T_e, dot product T_{pm}, bilinear pairing operation T_p, point addition operation T_{pa} , one-way hash operation T_h, and symmetric encryption and decryption operation $T_{e/d}$. Among them, XOR and concatenation require shorter execution time, so these two types of operations are ignored in the computational overhead. The rest of the operations follow the calculation rules and data given in [33], and Table 2 lists the time overhead required for each calculation.

As shown in the third column of Table 1, we calculated the computational overhead of our scheme and the previous schemes. Figure 7 shows how the computational overhead of each scheme changes as the number of authenticated users increases. It can be clearly seen from the figure that the computational overhead of our scheme is much smaller than those of other schemes in [18–22], so it is more suitable for large-scale user multicast service registration. This is because our scheme mainly relies on the hash operation with a small amount of computation operations and adopts the method of processing authentication requests by using satellites to aggregate multiple messages.

7.3. Bandwidth Overhead. On the premise of achieving the same security as AES-128, we make the following settings in order to fairly compare the bandwidth overhead of our proposed scheme with the previous schemes. We assume that the key length based on the symmetric cryptosystem is 128 bits, the lengths of the public key and private key based on finite field are 3072 bits and 256 bits, respectively, the point on the elliptic curve is 320 bits, the output values of the hash functions such as MAC and RES are uniformly 160 bits, the random number is 128 bits, the length of the serial number and AMF identifier in 5G AKA is 48 bits, and the length of the identification and timestamp is 32 bits.

The bandwidth overheads of our scheme and the previous schemes in [18–22] are listed in Table 1. Figure 8 intuitively shows the change of the bandwidth overhead of each scheme as the number of users increases. We can see that the proposed scheme has more advantages in the bandwidth overhead compared with other schemes as the number of users increases, since the request messages are aggregated in the service registration phase.

7.4. Experiment and Analysis

7.4.1. The Experimental Scheme. To verify the validity and reliability of the proposed scheme, an experimental environment is built according to the network topology shown in Figure 9. The experiments simulate the multicast service of three users. Each node is deployed on a physical host that connects through a Gigabit network. The host is configured with Intel(R) Core(TM) i7-2600 CPU @ 3.40 GHz, 3 GB memory, 2 TB hard disk, and CentOS 7.4 operating system.

The experiments are divided into three parts as follows:

(1) In the experimental environment, the delay of establishing shared key between three users and the BM-SC, the delay of user multicast service registration, and the delay of group key security distribution are tested. Each delay is tested several times to observe and analyze the efficiency of key derivation and distribution during the multicasting.

(2) After the group key distribution between the user and the BM-SC is completed, we tested the throughput rate of multicast data transmission. The data transmission adopts the ECB mode of the SM4 algorithm implemented by software for encryption and decryption. The throughput rate is sampled several times to observe and analyze the changes in data transmission performance during the multicasting.

(3) In the above two experiments, the system monitoring tool is used to monitor the CPU usage,

Table 1: Comparison of the overhead of each protocol.

Protocol	Signaling Overhead	Computational Overhead (s)	Bandwidth Overhead (bits)
[18]	$4n$	$(12T_h + 1T_{\mathrm{pm}})n$	$1088n$
[19]	$4n$	$(8T_h)n$	$896n$
[20]	$4n$	$(8T_h + 3T_{\mathrm{pm}})n$	$1120n$
[21]	$6n$	$(10T_h + 6T_{\mathrm{pm}} + 2T_{e/d})n$	$1312n$
[22]	$3n$	$(4T_e + 17T_{\mathrm{pm}} + 7T_p + 2T_h + 7T_{pa})n$	$8348n$
Proposed	$3n + 3$	$(4n + 2)T_h$	$480n + 576$

Table 2: Comparison of the overhead of each protocol.

Operation	Time overhead (μs)
T_e	1.00×10^3
T_{pm}	0.52×10^3
T_p	8.36×10^3
T_{pa}	1.39
T_h	1.21
$T_{e/d}$	1.05

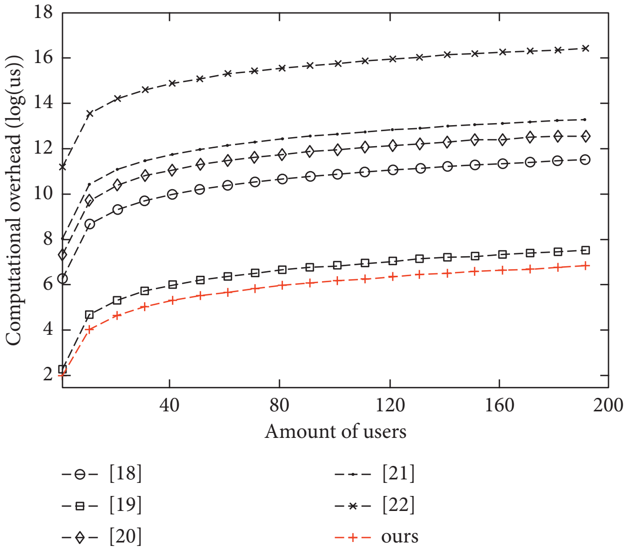


Figure 7: Computational overhead of each scheme.

memory usage, and system load changes of the user system in the process of key derivation, distribution, and data transmission.

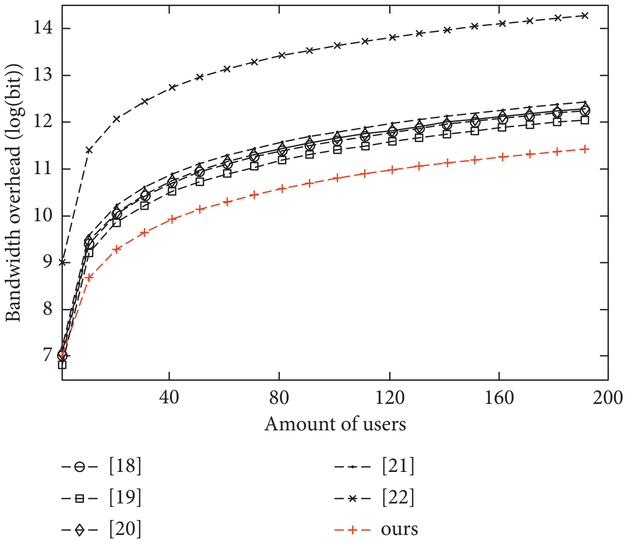


Figure 8: Bandwidth overhead of each scheme.

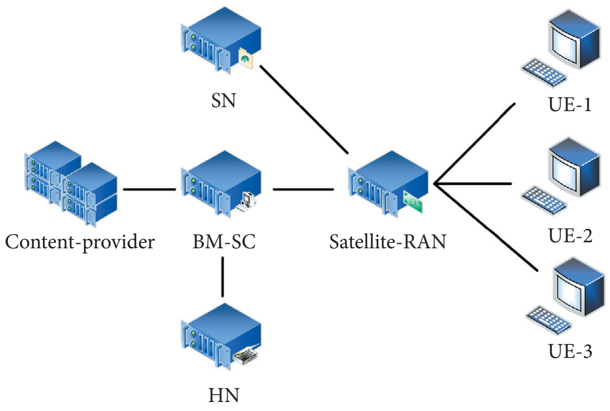


Figure 9: Experimental environment.

7.4.2. Experimental Results and Analysis. The delays of the establishment of the shared key between three users and the BM-SC, the registration of user multicast service, and the group key distribution are described in Figures 10–12, respectively. Each delay is tested 50 times. As shown in Figure 10, the maximum delay of the shared key establishment is less than 2 ms. Compared with the round-trip delay of network transmission in the experimental environment, the delay of the shared key establishment process is basically the same as that of network transmission in the communication process. Therefore, the cost of shared key calculation can be ignored. As shown in Figure 11, the registration delay of multicast services is greater than 1 s. This is because the timer in the satellite network is set to 1 s; after 1 s, all multicast service registration requests received within this period are sent to the BM-SC. The delay of group key distribution is basically the same as the network transmission delay in the communication process, as shown in Figure 12. After the group key distribution between the user and the BM-SC is completed, the multicast data transmission test is performed. The length of test data is 1400 bytes, and the throughput rate is sampled 50 times during the test. From

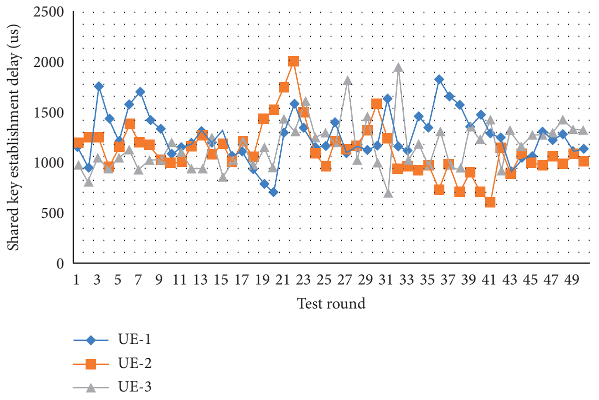


FIGURE 10: The shared key establishment delay.

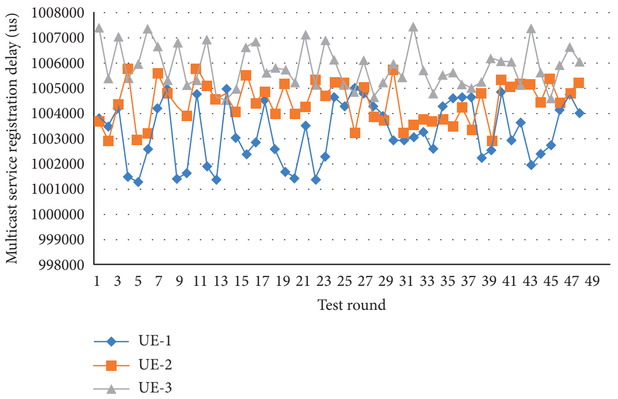


FIGURE 11: The multicast service registration delay.

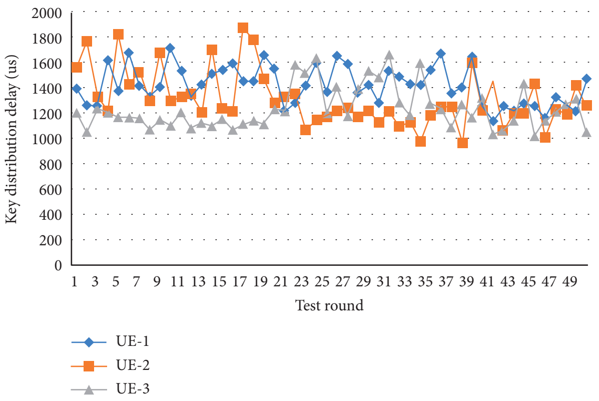


FIGURE 12: The key distribution delay.

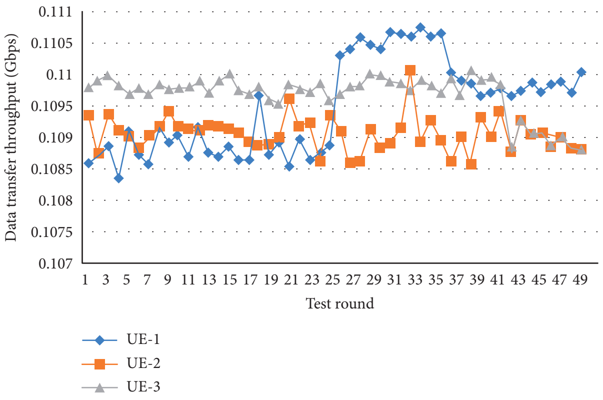


FIGURE 13: The data transfer throughput.

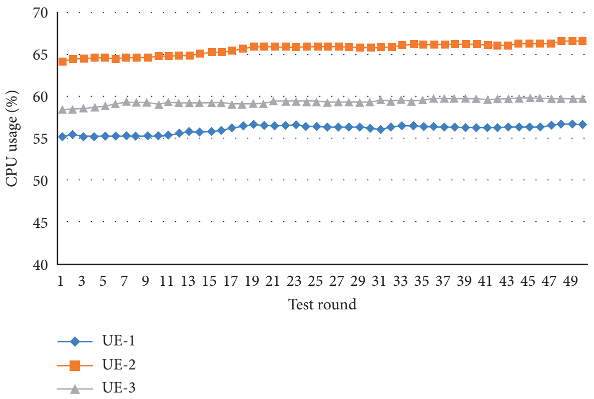


FIGURE 14: CPU usage.

Figure 13, the data transmission rate is basically stable at 0.109 Gbps. The reason for the low data transmission performance is that the software encryption and decryption algorithm is used to process the data, with a performance of 0.114 Gbps, slightly higher than the data transmission rate. The performance of data transmission has reached the upper limit of the communication rate in the experimental environment.

During the data transmission between the users and the BM-SC, the CPU usage of the three users is shown in Figure 14. For multicore CPU, the usage and the system load are lower. In addition, among the whole CPU usage, the part for key derivation and distribution between the users and the BM-SC is close to 0%.

According to the above experimental results, the proposed scheme has a low computational overhead in the process of shared key establishment, multicast service registration, and group key distribution. While achieving a higher communication rate, it takes fewer hardware resources. The security requirements of multicast services are well satisfied in the SGIN.

8. Conclusions

In this paper, we design an efficient authentication and key distribution protocol for multicast services in SGIN. Specifically, we have completed the secure derivation of the shared key for multicast services between the UE and the BM-SC with the help of the existing 5G-AKA mechanism. Then we design a group-based multicast service registration mechanism. Finally, based on the CRT, we design a secure and efficient group key distribution and update process. Security analysis and performance analysis results show that our scheme has robust security properties and has advantages in signaling overhead, computational overhead, and bandwidth overhead. By building a real experimental environment, we tested the actual application of our scheme.

From the perspective of the delay, transmission rate, and CPU usage, our scheme has good efficiency under the premise of ensuring security.

Data Availability

No datasets were used in this paper.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was supported in part by the National Natural Science Foundation of China under Grants nos. 62102298 and 61772404, in part by the Key Research and Development Program of Shaanxi under Grant no. 2020ZDLGY08-08, in part by the State Key Laboratory of Integrated Services Networks, Xidian University (ISN22-13), and in part by the Mobile Internet Security Innovation Team of Shaanxi Province (2018TD-007).

References

[1] M. H. Alsharif, A. H. Kelechi, and M. A. Albreem, "Sixth generation (6G) wireless networks: vision, research activities, challenges and potential solutions," *SYMMETRY-BASEL*, vol. 12, no. 4, 2020.

[2] Y. Shi, J. Liu, Z. M. Fadlullah, and N. Kato, "Cross-layer data delivery in satellite-aerial-terrestrial communication," *IEEE Wireless Communications*, vol. 25, no. 3, pp. 138–143, 2018.

[3] M. Sheng, D. Zhou, R. Liu, Y. Wang, and J. Li, "Resource mobility in space information networks: opportunities, challenges, and approaches," *IEEE Network*, vol. 33, no. 1, pp. 128–135, 2019.

[4] J. Liu, Y. Shi, Z. M. Fadlullah, and N. Kato, "Space-air-ground integrated network: a survey," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 4, pp. 2714–2741, 2018.

[5] T. Li, H. Zhou, H. Luo, and S. Yu, "Service: a software defined framework for integrated space-terrestrial satellite communication," *IEEE Transactions on Mobile Computing*, vol. 17, no. 3, pp. 703–716, 2018.

[6] M. Manulis, C. P. Bridges, R. Harrison, V. Sekar, and A. Davis, "Cyber security in new space," *International Journal of Information Security*, vol. 20, no. 3, pp. 287–311, 2021.

[7] C. Jiang, X. Wang, J. Wang, H.-H. Chen, and Y. Ren, "Security in space information networks," *IEEE Communications Magazine*, vol. 53, no. 8, pp. 82–88, 2015.

[8] S. K. Ahn, H. Jung, and S. Kwon, "Performance evaluation of rel-16 5G-MBMS," in *Proceedings of the 2021 IEEE International Symposium on Broadband Multimedia Systems and Broadcasting (BMSB)*, pp. 1–4, Chengdu, China, August, 2021.

[9] K. Elmufti, D. Weerasinghe, M. Rajarajan, V. Rakocevic, S. Khan, and J. A. MacDonald, "Mobile Web services authentication using SAML and 3GPP generic bootstrapping architecture," *International Journal of Information Security*, vol. 8, no. 2, pp. 77–87, 2009.

[10] A. Braeken, "Symmetric key based 5G AKA authentication protocol satisfying anonymity and unlinkability," *Computer Networks*, vol. 181, Article ID 107424, 2020.

[11] S. Zhang, D. Zhu, and Y. Wang, "A survey on space-aerial-terrestrial integrated 5G networks," *Computer Networks*, vol. 174, pp. 107212–107229, 2020.

[12] I. A. Sanchez, G. Moury, and H. Weiss, "The CCSDS space data link security protocol," in *Proceedings of the Military Communications Conference 2010 (MILCOM 2010)*, pp. 219–224, San Jose, CA, USA, October, 2010.

[13] Z. Sun, M. P. Howarth, and H. Cruickshank, "Networking issues in IP multicast over satellite," *International Journal of Satellite Communications and Networking*, vol. 21, no. 4-5, pp. 489–507, 2003.

[14] X. Lv, Y. Mu, and H. Li, "Non-interactive key establishment for Bundle security protocol of space DTNs," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 1, pp. 5–13, 2014.

[15] D. W. Matolak, A. Noerpel, and R. Goodings, "Recent progress in deployment and standardization of geostationary mobile satellite systems," in *Proceedings of the 2002 MILCOM Proceedings, Vols 1 and 2: Global Information Grid-Enabling Transformation through 21st Century Communications*, pp. 173–177, Anaheim, CA, USA, October, 2002.

[16] M. Bowyer, L. Erup, and H. P. Lexow, "Security in DVB-RCS2," *International Journal of Satellite Communications and Networking*, vol. 31, no. 5, pp. 263–276, 2013.

[17] A. Ostad-Sharif, D. Abbasinezhad-Mood, and M. Nikooghadam, "Efficient utilization of elliptic curve cryptography in design of a three-factor authentication protocol for satellite communications," *Computer Communications*, vol. 147, pp. 85–97, 2019.

[18] I. Altaf, M. A. Saleem, K. Mahmood, S. Kumari, P. Chaudhary, and C.-M. Chen, "A lightweight key agreement and authentication scheme for satellite-communication systems," *IEEE Access*, vol. 8, Article ID 46278, 2020.

[19] Y. Zhang, J. Chen, and B. Huang, "An improved authentication scheme for mobile satellite communication systems," *International Journal of Satellite Communications and Networking*, vol. 33, no. 2, pp. 135–146, 2015.

[20] M. Qi and J. Chen, "An enhanced authentication with key agreement scheme for satellite communication systems," *International Journal of Satellite Communications and Networking*, vol. 36, no. 3, pp. 296–304, 2018.

[21] M. Qi, J. Chen, and Y. Chen, "A secure authentication with key agreement scheme using ECC for satellite communication systems," *International Journal of Satellite Communications and Networking*, vol. 37, no. 3, pp. 234–244, 2019.

[22] 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*, vol. 14, no. 2, pp. 486–497, 2019.

[23] A. Vazquez-Castro and M. Hayashi, "Physical layer security for RF satellite channels in the finite-length regime," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 4, pp. 981–993, 2019.

[24] J. Xiong, D. Ma, H. Zhao, and F. Gu, "Secure multicast communications in cognitive satellite-terrestrial networks," *IEEE Communications Letters*, vol. 23, no. 4, pp. 632–635, 2019.

[25] S. R. Pokhrel, "Blockchain brings trust to collaborative drones and LEO satellites: an intelligent decentralized learning in the space," *IEEE Sensors Journal*, vol. 21, no. 22, Article ID 25331, 2021.

[26] Z. Bao, M. Luo, H. Wang, K.-K. R. Choo, and D. He, "Blockchain-based secure communication for space

information networks," *IEEE Network*, vol. 35, no. 4, pp. 50–57, 2021.

[27] D. R. Gozzard, S. Walsh, and T. Weinhold, "Vulnerability of satellite quantum key distribution to disruption from ground-based lasers," *Sensors*, vol. 21, no. 23, 2021.

[28] A. Vázquez-Castro, D. Rusca, and H. Zbinden, "Quantum keyless private communication versus quantum key distribution for space links," *Physical Review Applied*, vol. 16, no. 1, Article ID 014006, 2021.

[29] J. Zhang, J. Cui, H. Zhong, Z. Chen, and L. Liu, "PA-CRT: Chinese remainder theorem based conditional privacy-preserving authentication scheme in vehicular ad-hoc networks," *IEEE Transactions on Dependable and Secure Computing*, vol. 18, no. 2, pp. 722–735, 2021.

[30] "Security architecture and procedures for 5G system (Release 17)," 3GPP TS 33.501 v17.0.0, 2020, https://www.3gpp.org/ftp/Specs/archive/33_series/33.501/33501-h00.zip.

[31] X. Han, S. Q. Lu, and Q. F. Chen, "The improvement and instance analysis of the formal verification tool scyther," *Journal of Information Security Research*, vol. 2, no. 3, pp. 272–279, 2016.

[32] Scyther, "Scyther," 2019, https://www.cs.ox.ac.uk/people/cas.cremers/scyther/.

[33] R. Ma, J. Cao, D. Feng, and H. Li, "LAA: lattice-based access authentication scheme for IoT in space information networks," *IEEE Internet of Things Journal*, vol. 7, no. 4, pp. 2791–2805, 2020.