Received 30 October 2021; revised 1 December 2021; accepted 16 December 2021. Date of publication 30 December 2021; date of current version 15 April 2022.

Digital Object Identifier 10.1109/OJCOMS.2021.3139462

Achieving Efficient and Secure Handover in LEO Constellation-Assisted Beyond 5G Networks

QINGLEI KONG[1] (Member, IEEE), RONGXING LU[2] (Fellow, IEEE), AND FENG YIN[3] (Senior Member, IEEE)

(Invited Paper)

[1]Institute of Space Science and Applied Technology, Harbin Institute of Technology (Shenzhen), Shenzhen 510080, China

[2]Faculty of Computer Science, University of New Brunswick, Fredericton, NB E3B 5A3, Canada

[3]School of Science and Engineering, The Chinese University of Hong Kong, Shenzhen 518172, China

CORRESPONDING AUTHOR: F. YIN (e-mail: yinfeng@cuhk.edu.cn)

This work was supported by the Natural Science Foundation of China under Grant 92067202.

ABSTRACT Ubiquitous connection to modern vehicles is mandatory to support diverse intelligent functions, including autonomous driving, telediagnosis, infotainment services, and others. Since the deployment of the cellular access points is still scarce in rural areas, the low earth orbit (LEO) constellation-based communication is believed to provide a realistic alternative. However, due to the long propagation delay and limited satellite on-board processing ability, the design of security protocols in LEO constellations remain challenging. Aiming at these challenges, we propose a secure user access and inter-satellite handover mechanism, which achieves the control- and user-plane key separation. Specifically, our proposed scheme exploits an identity-based encryption scheme with proxy re-encryption to achieve the key establishments with high efficiency, and it also achieves the highly efficient secure batch handover with the assistance of a stack. Detailed analysis is performed to demonstrate the security properties of our proposed scheme, in terms of confidentiality, authentication, and forward/backward key separation. Furthermore, simulation results illustrate that our proposed scheme achieves high computational complexity and communication overheads in comparison with a traditional scheme.

INDEX TERMS LEO constellation, user access, handover, security.

I. INTRODUCTION

NOWADAYS, universal automotive connectivity plays a critical role in supporting the smooth functioning of intelligent vehicles, which commonly depend on cellular networks [1], [2]. However, cellular connectivity relies on the pervasive deployment of terrestrial infrastructures, which suffers not only the non-existent terrestrial 5G cell towers in rural areas but also the service disruption in case of natural disasters or emergency events [3], [4]. To address these limitations, the integration of satellites into the cellular network provides an opportunity to the situation when a vehicle roams out of the cell tower coverage, which assures seamless vehicular connectivity [5], [6]. To date, *Starlink* has launched about $1,500$ low earth orbit (LEO) satellites, whose constellation orbits about 550 miles above the earth's surface. Even though the LEO satellites significantly reduce the receive-and-transmit latency compared with the geostationary earth orbit (GEO) satellites, each LEO satellite creates a smaller coverage area, where a user has to suffer from the continuous and frequent handover. Thus, to reach the full potential of the satellite-integrated vehicular network in the future 5G networks, several challenges have to be addressed, such as secure user access and handover.

The first challenge resides in the secure link generated between the involved entities, i.e., ground stations, satellites, and vehicles. In a satellite constellation, the satellite is no longer merely responsible for bouncing the signal between two ground devices. Instead, the signal is assumed to be able to reach any place on earth through a few satellite hops, regardless of the land obstacle and weather condition. On the other hand, since an LEO constellation needs to integrate with the 5G cellular system, the secure link establishment should also support the separation of the control- and user-plane signaling. Even though some secure authentication and key establishment mechanisms are proposed in [7], [8], they fail to take the separation of the control- and user-plane into consideration. Therefore, there is a high demand to design a secure user access and key establishment scheme for an LEO satellite constellation, which considers the control- and user-plane signaling separation.

The second challenge is the secure and frequent handover between different satellites. Specifically, an LEO satellite's orbital period ranges from 90 to 110 minutes, and each connection duration between an LEO satellite and a ground station is 5 to 15 minutes over 6 to 8 times per day [9], which leads to the consequence of frequent handover. Meanwhile, some secure handover authentication protocols are designed in [8], [10], [11], which realize both the mutual authentication and session key agreement during the handover processes. However, these schemes only consider one satellite hop case, i.e., the satellite directly connects to both the ground station and the vehicle. In an LEO satellite constellation, the vehicle may connect to the ground station through multiple satellites, and the secure handover mechanism should also include the inter-satellite links. Thus, there is also a requirement to design a novel secure and efficient handover mechanism, which considers the case of multi-hop satellite transmission.

Based on the above analysis, the main goal of our proposed scheme is to develop a secure user access and handover mechanism in an LEO constellation. Specifically, the main contributions of this paper are as follows.

Firstly, the proposed scheme achieves the highly efficient secure key establishments during the user access phase. Specifically, by generating one identity-based ciphertext tuple, the proposed scheme can achieve both the control-plane key establishment with the accessing satellite and the user-plane key construction with the ground station.

Secondly, the proposed scheme achieves the secure batch inter-satellite handover. With the assistance of a stack, the proposed scheme structures and delivers the involved vehicles' key generators with high efficiency, such that the control-plane keys shared between the users and the target satellite can be successfully established.

Thirdly, we demonstrate the security properties of the proposed mechanism, in terms of confidentiality, authentication, and backward/forward key separation. We also compare it with a traditional scheme, and the evaluation results show that our proposed scheme significantly reduces the computation and communication overheads.

The remainder of this paper organizes as follows. We introduce our system model, present our security requirements, and identify our design goals in Section II. In Section III, we show the bilinear pairing technique and describe the secure handover process defined in the 3GPP 5G standard. In Section IV, we present our proposed secure handover key establishment and handover mechanism in an LEO satellite constellation. Security analysis and performance evaluations are shown in Section V and Section VI, respectively. Related works are described in Section VII, and we conclude the paper in Section VIII.

II. SYSTEM MODEL, SECURITY REQUIREMENTS, AND DESIGN GOALS

In this section, we first describe the system model, then show the security requirements, and further identify our design goals.

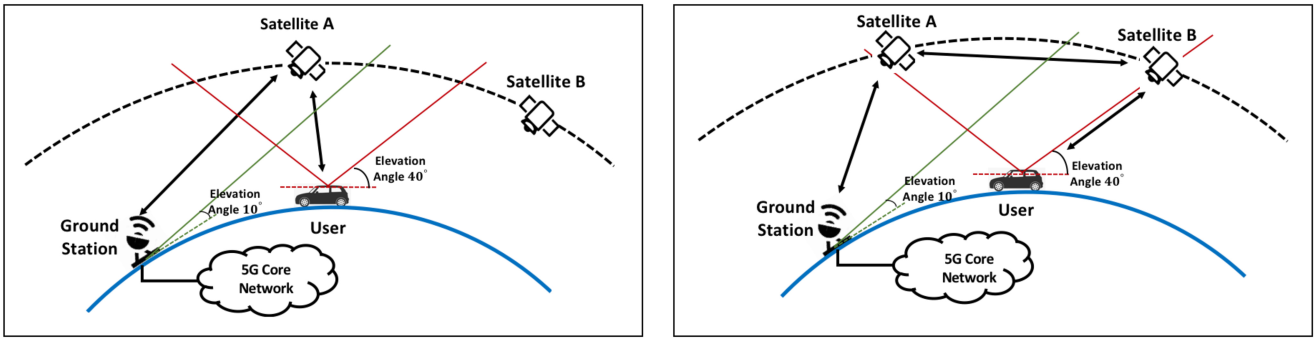
A. SYSTEM MODEL

LEO satellites can play a dominant role in extending 5G connections to remote areas outside the cellular networks, which function as an access network to the 5G core network through satellite connectivity. We consider the scenario when a vehicle roams out of the 5G core network coverage and migrates to the LEO satellite connectivity. The system includes three entity types: vehicles, LEO satellites, and ground stations.

- *Vehicle:* The vehicle under consideration moves through a rural environment without the terrestrial 5G cellular connectivity. Meanwhile, each vehicle owns the satellite communication capabilities (i.e., with a vehicle-mounted VSAT), enabling two-way satellite-ground communications. Besides, each automotive is communicating under the elevation angle of 40 degrees [9].
- *Satellite:* Each LEO satellite acts as a communication gateway between a vehicle and a ground station, and the LEO satellites communicate among themselves using the inter-satellite links. Meanwhile, a majority of modern satellites operate as relays, which frequency-convert, amplify and forward the received control-plane and user-plane signals. Furthermore, we assume the inter-satellite transmissions are realized through the narrow beam laser [12], [13]. Besides, we assume the LEO satellites are orbiting at an altitude of 550 km. In addition, we assume each LEO satellite is launched by a satellite company and rented by multiple mobile operators.
- *Ground station:* A ground station connects to the core terrestrial 5G cellular network. Meanwhile, we suppose the ground station communicates with satellites at 10 degree of elevation [9]. In addition, we assume the ground stations are also deployed by the satellite company and rented by multiple mobile operators.

The system model includes two phases, as shown in Fig. 1. (The figures are not with the real proportion.)

- *Connection Establishment Phase:* As shown in Fig. 1(a), when a vehicle roams out of the terrestrial 5G signal coverage, the vehicle connects to the core network



(a) User Access Phase

(b) Inter-satellite Handover Phase

FIGURE 1. Illustration of the Handover Process.

through the accessing satellite. Meanwhile, the accessing satellite may connect to the ground station via one or a few satellites. In addition, the ground station connects to the 5G core network.

- *Inter-Satellite Handover Phase:* Since the moving speed of a vehicle is negligible compared with the high-speed orbiting satellite, the frequent satellite handover happens due to the change of covering satellites. As illustrated in Fig. 1(b), the connection of the vehicle to Sat_a handovers towards a new satellite Sat_b. Since Sat_b cannot directly communicate with the ground station, the new connection path from the vehicle to the ground station passes through both Sat_a and Sat_b.

Note that in our proposed scheme, the user needs to establish a secure user-plane session key with the ground station, regardless of the intermediate satellites; meanwhile, the user only constructs a secure control-plane session key with the accessing satellite. The proposed scheme can also adapt to the scenario: when the ground station deployment is insufficient, Sat_b can connect to the ground station with the help of other satellites, like through Sat_a.

B. SECURITY REQUIREMENT

In the threat model, we consider the satellites are honest-but-curious, that is, each satellite follows the defined protocol, but it tries to infer the content passes through it. Meanwhile, we assume a satellite can be rented by multiple (terrestrial) 5G core networks owned by different mobile operators. Furthermore, we assume there exists an attacker to eavesdrop and modify the data transmission, and we assume the control-plane signaling between the satellites is confidential by itself, by exploiting the narrow beam laser [12], which is assumed to be secure when the beam is narrow enough. On the other hand, some security-enhancing techniques like data fragmentation multi-path transmission can also be utilized for a free-space optical system [14], to protect the confidentiality of the inter-satellite links. In addition, we assume there is no collusion between the satellite and the ground station. Specifically, the proposed scheme should satisfy three security requirements: confidentiality, authentication, and backward/forward key separation.

- *Confidentiality:* The control-plane data transmission between the vehicle and accessing satellite should achieve confidentiality. The user-plane data should achieve confidentiality between the vehicle and the ground station, regardless of the intermediate system.
- *Authentication:* Before the key establishment process, all the involved entities should mutually authenticate each other. Meanwhile, the receiver should verify the correctness and origin of the message.
- *Backward/Forward Key Separation:* For the system under consideration, when a new satellite joins the transmission process, it should not recover the previously transmitted control-plane signaling. On the other hand, when a satellite leaves the transmission process, it should not learn the control-plane data transmission afterward.

C. DESIGN GOALS

Under the above system and security models, our primary design goal is to develop a secure and efficient key establishment mechanism during user access and inter-satellite handover in the satellite-assisted beyond 5G system. Specifically, the proposed scheme should achieve the following goals.

The proposed scheme should satisfy the above-defined security requirements: If the proposed secure handover scheme does not satisfy confidentiality, the user-plane data transmitted between the ground station and the vehicle may disclose to intermediate satellites. Meanwhile, the control-plane signaling containing the user-specific identifier and routing information between the vehicle and the accessing satellite may also leak. Besides, the security requirement of authentication verifies the origin of each message and guarantees its correctness. In addition, forward/backward key separation guarantees that when a satellite joins/leaves the transmission process, the satellite cannot decrypt the previous/subsequent control-plane data transmissions.

The proposed scheme should achieve high efficiency: Since the major obstacle for any satellite network is the propagation delay due to the long transmission distance, the communication overhead introduced needs to be deliberatively evaluated, especially the overheads of transmission links established between the satellites and the vehicles. Besides, the computation overhead introduced by the simultaneous handover of a group of vehicles also needs to be reduced as much as possible.

III. PRELIMINARIES

In this section, we first briefly review the security technique of bilinear pairing [15], which is the basic cryptographic building block of the proposed scheme. Then we show the secure handover key management scheme defined in the 3GPP 5G security architecture [16].

A. BILINEAR PAIRINGS

Let $\mathbb{G}$ and $\mathbb{G}_T$ be two cyclic groups with the same prime order p, and let (g, h) be two generators of $\mathbb{G}$. Meanwhile, more details of the bilinear pairing construction can refer to [15]. A bilinear map $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ has the following properties:

1) *Bilinearity:* $\forall g, h \in \mathbb{G}$, and $\forall a, b \in \mathbb{Z}_p$, we have $e(g^a, h^b) = e(g, h)^{ab}$;

2) *Non-degeneracy:* There exists $g \in \mathbb{G}$, which satisfies the condition that $e(g, g) \neq 1_{\mathbb{G}_T}$.

3) *Computability:* $\forall g, h \in \mathbb{G}$, there exists an efficient algorithm to compute $e(g, h)$.

Definition 1: A bilinear parameter generator $\mathcal{G}en$ denotes a probabilistic algorithm that takes a parameter κ as input, and outputs a 5-tuple $(p, g, \mathbb{G}, \mathbb{G}_T, e)$ as the output, where p is a prime number with $|p| = \kappa$, and $\mathbb{G}$ and $\mathbb{G}_T$ are two cyclic groups with order p. Meanwhile, $g \in \mathbb{G}$ is a generator, and $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ is a non-degenerated and computable bilinear map.

B. SECURE MOBILITY MANAGEMENT IN 5G

In 5G network, the UE and the gNB use the key K_{gNB} to secure the established transmission link [16]. During the handover process, the basis for the session key shared between the UE and the target gNB called K_{gNB^*}, is derived from either the current active session key K_{gNB} or from the NH parameter. In *Horizontal Key Derivation*, K_{gNB^*} is derived from the currently active session key K_{gNB}. While in *Vertical Key Derivation*, K_{gNB^*} is derived from the next hop parameter NH, which is only computable by the UE and access and mobility management function (AMF). Besides, only the *Vertical Key Derivation* method can achieve the security goal of forward key separation.

However, the secure handover key derivation process in 5G requires the constant control-plane signaling interaction between the UE and the gNBs, which is unrealistic in the context of satellite communications due to the high system overheads. From the perspective of users, when a vehicle roams out of the terrestrial 5G network, the vehicle will not request the satellite network service unless necessary, particularly due to the scarce satellite bandwidth, high transmission delay, and expensive communication costs.

IV. PROPOSED SCHEME

In this section, we propose a secure user access and inter-satellite handover mechanism in an LEO constellation-assisted beyond 5G system. Specifically, we first describe the *system initialization phase*, then show the *user access phase* between the user and the ground station, and finally illustrate the *inter-satellite handover phase*. Furthermore, a proxy re-encryption system with identity-based encryption [17] lays the foundation of our scheme.

A. SYSTEM INITIALIZATION

We assume the mobile 5G operator will act as a trusted authority (TA) to bootstrap the entire system. Given a security parameter κ, TA generates the bilinear parameters $(p, \mathbb{G}, \mathbb{G}_T, e, g, g_2, h)$, in which $|p| = \kappa$, $(g, g_2, h) \in \mathbb{G}$ and $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$. Meanwhile, the TA selects a random number $\alpha \in \mathbb{Z}_p^*$, computes the generator $g_1 = g^\alpha \in \mathbb{G}$, and generates the secret master key $mk = g_2^\alpha \in \mathbb{G}$. Furthermore, the TA chooses another random number $s \in \mathbb{Z}_p^*$, computes the system public key $pk = g^s \in \mathbb{G}$, and selects a secure cryptographic hash function H, where $H : \{0, 1\}^* \to \mathbb{Z}_p^*$. Finally, the TA announces the system parameters: $params = (p, \mathbb{G}, \mathbb{G}_T, e, g, g_1, g_2, h, pk, H)$.

During the registration of a vehicle v_i, the TA generates an identity-based secret key $sk_i = g^{1/(s+H(v_i))}$ for v_i, and securely transmits sk_i towards it. Meanwhile, during the registration of an entity e_j (i.e., a satellite or a ground station), the TA selects a random number $u_j \in \mathbb{Z}_p^*$ and generates an identity-based secret key, which denotes as $sk_j = (g_2^\alpha \cdot (g_1^{H(e_j)} \cdot h)^{u_j}, g^{u_j})$. In addition, the TA calculates the re-encryption key for v_i, which is $rk_j = g_1^{u_j}$. Finally, the TA securely delivers the secret key tuple (sk_j, rk_j) towards e_j.

B. USER ACCESS PHASE

During the *User Access Phase*, we consider the construction of the control-plane session key between vehicle v_i and satellite Sat_a, and that of the user-plane key shared between v_i and ground station GS.

Step-1: Assume v_i roams out of the 5G network, and it intends to connect to the 5G core network through the accessing satellite Sat_a. v_i selects one secret number $k_i \in \mathbb{Z}_p^*$ with two random numbers $(r_{i,1}, x_i) \in \mathbb{Z}_p^*$, and then generates the ciphertext tuple $c_i = (c_{i,1}, c_{i,2}, c_{i,3})$, which is

$$\begin{cases} c_{i,1} = g^{r_{i,1}}, c_{i,2} = \left(g_1^{H(Sat_a)} \cdot h\right)^{r_{i,1}}, \\ c_{i,3} = e(g, g)^{k_i} \cdot e(g_1, g_2)^{r_{i,1}}. \end{cases} \tag{1}$$

Furthermore, v_i selects another random number $r_{i,2} \in \mathbb{Z}_p^*$, and generates the identity-based signature pair $\sigma_i = (\sigma_{i,1}, \sigma_{i,2})$ with the current timestamp $TS_{i,1}$, which is

$$\begin{cases} \sigma_{i,1} = e(g, g)^{r_{i,2}}, \\ \sigma_{i,2} = g^{\frac{r_{i,2}+H\left(v_i \| Sat_a \| e(g,g)^{k_i} \| e(g,g)^{r_{i,2}} \| TS_{i,1}\right)}{s+H(v_i)}}. \end{cases} \tag{2}$$

Finally, v_i formulates a message $Msg_1 = v_i \| Sat_a \| c_i \| \sigma_i \| TS_{i,1}$, and delivers it to Sat_a.

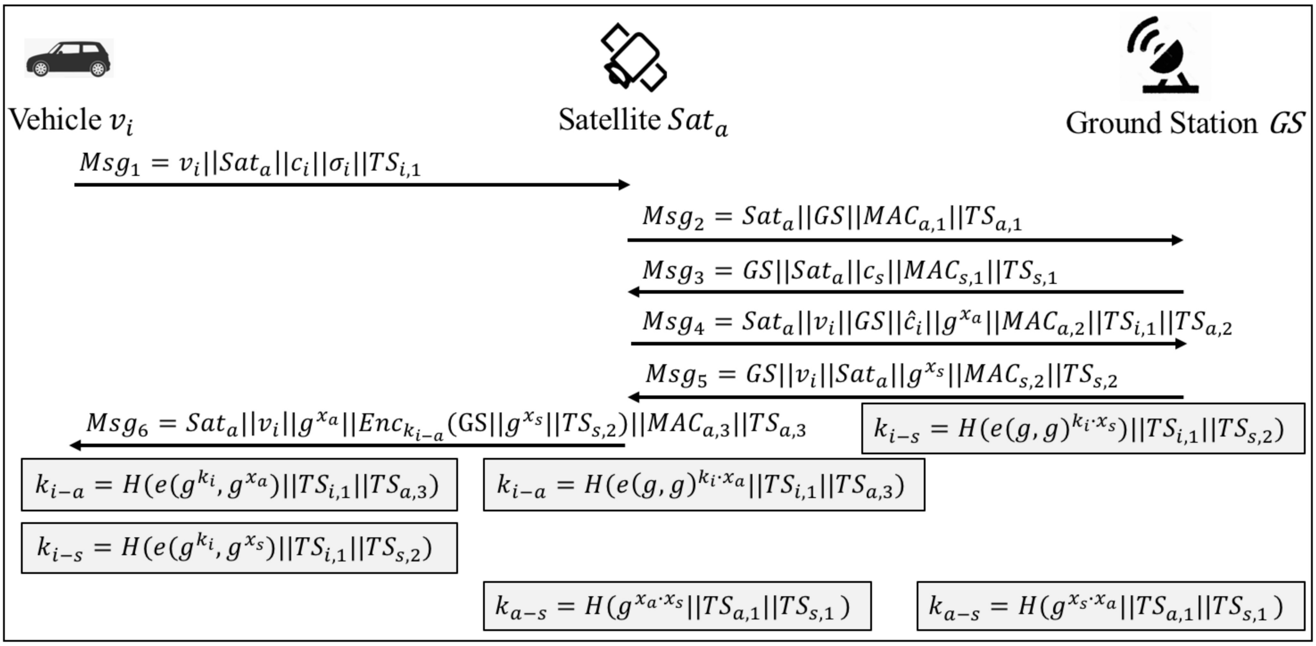


FIGURE 2. Message Flows during User Access.

Step-2: When Sat_a receives Msg_1, it first decrypts the ciphertext $c_i = (c_{i,1}, c_{i,2}, c_{i,3})$ with its secret key $(sk_{a,1} = g_2^{\alpha}\cdot(g_1^{H(Sat_a)}\cdot h)^{u_a}, sk_{a,2} = g^{u_a})$, which is

$$e(g,g)^{k_i} = \frac{c_{i,3}\cdot e\big(c_{i,2}, sk_{a,2}\big)}{e\big(c_{i,1}, sk_{a,1}\big)}. \tag{3}$$

Given the decryption result $e(g,g)^{k_i}$, Sat_a checks the correctness of $(\sigma_{i,1}, \sigma_{i,2})$, which is

$$e\Big(\sigma_{i,2}, pk\cdot g^{H(v_i)}\Big) \stackrel{?}{=} \sigma_{i,1}\cdot e(g,g)^{H\left(v_i\|Sat_a\|e(g,g)^{k_i}\|e(g,g)^{r_{i,2}}\|TS_{i,1}\right)}. \tag{4}$$

If Eq. (4) is verified to be correct, Sat_a formulates a message $Msg_2 = Sat_a\|GS\|MAC_{a,1}\|TS_{a,1}$, where $MAC_{a,1} = H(Sat_a\|GS\|TS_{a,1})$ is the message authentication code and $TS_{a,1}$ is the current timestamp, and it sends Msg_2 to GS.

Step-3: When GS receives Msg_2, it first checks the correctness of $MAC_{a,1}$ by computing

$$MAC_{a,1} \stackrel{?}{=} H\big(Sat_a\|GS\|TS_{a,1}\big). \tag{5}$$

If Eq. (5) is verified to be correct, GS generates the ciphertext tuple $c_s = (c_{s,1}, c_{s,2}, c_{s,3})$, which is

$$\begin{cases} c_{s,1} = g^{r_s}, c_{s,2} = \left(g_1^{H(Sat_a)}\cdot h\right)^{r_s}, \\ c_{s,3} = g_1^{u_s}\cdot H(e(g_1, g_2)^{r_s}), \end{cases} \tag{6}$$

where $r_s \in \mathbb{Z}_p^*$. Meanwhile, GS generates the message authentication code $MAC_{s,1} = H(GS\|Sat_a\|g_1^{u_s}\|TS_{s,1})$, where $TS_{s,1}$ is the current timestamp. In addition, GS formulates a message $Msg_3 = GS\|Sat_a\|c_s\|MAC_{s,1}\|TS_{s,1}$, and it delivers Msg_3 towards Sat_a.

Step-4: After receiving Msg_3, Sat_a first decrypts the ciphertext c_s with its secret key $(sk_{a,1}, sk_{a,2})$, which is

$$\begin{aligned} & c_{s,3}/H\left(\frac{e\big(c_{s,1}, sk_{a,1}\big)}{e\big(c_{s,2}, sk_{a,2}\big)}\right) \\ &= g_1^{u_s}\cdot H\big(e(g_1, g_2)^{r_s}\big)/H\left(\frac{e\left(g^{r_s}, g_2^{\alpha}\cdot\left(g_1^{H(Sat_a)}\cdot h\right)^{u_a}\right)}{e\left(\left(g_1^{H(Sat_a)}\cdot h\right)^{r_s}, g^{u_a}\right)}\right) \\ &= g_1^{u_s}\cdot H\big(e(g_1, g_2)^{r_s}\big)/H\big(e(g_1, g_2)^{r_s}\big) \\ &= g_1^{u_s}. \end{aligned} \tag{7}$$

Meanwhile, Sat_a verifies the correctness of $MAC_{s,1}$ by checking $MAC_{s,1} \stackrel{?}{=} H(GS\|Sat_a\|g_1^{u_s}\|TS_{s,1})$. If $MAC_{s,1}$ is verified to be correct, Sat_a re-encrypts the ciphertext c_i into a ciphertext $\hat{c}_i = (c_{i,1}, c_{i,2}, c_{i,4})$ of GS, which is

$$c_{i,4} = c_{i,3}\cdot e\Big(c_{i,1}^{H(gs)-H(Sat_a)}, g_1^{u_s}\Big). \tag{8}$$

In addition, Sat_a generates the message authentication code, which is $MAC_{a,2} = H(Sat_a\|v_i\|GS\|e(g,g)^{k_i}\|g_1^{u_s}\|g^{x_a}\|TS_{i,1}\|TS_{a,2})$, where $x_a \in \mathbb{Z}_p^*$. Finally, Sat_a formulates a message $Msg_4 = Sat_a\|v_i\|GS\|\hat{c}_i\|g^{x_a}\|MAC_{a,2}\|TS_{i,1}\|TS_{a,2}$, and delivers it to GS.

Step-5: When GS receives Msg_4, GS decrypts $\hat{c}_i$ with the secret key $(sk_{s,1} = g_2^{\alpha}\cdot(g_1^{H(s)}\cdot h)^{u_s}, sk_{s,2} = g^{u_s})$, which is

$$e(g,g)^{k_i} = \frac{c_{i,4}\cdot e\big(c_{i,2}, sk_{s,2}\big)}{e\big(c_{i,1}, sk_{s,1}\big)}. \tag{9}$$

Furthermore, GS verifies the correctness of $MAC_{a,2}$, which is

$$MAC_{a,2} \stackrel{?}{=} H\Big(Sat_a\|v_i\|GS\Big\|e(g,g)^{k_i}\Big\|g_1^{u_s}\Big\|g^{x_a}\Big\|TS_{i,1}\|TS_{a,2}\Big). \tag{10}$$

If Eq. (10) is verified to be correct, GS authenticates Sat_a, and formulates a message $Msg_5 = GS\|Sat_a\|g^{x_s}\|v_i\|MAC_{s,2}\|TS_{s,2}$, where $TS_{s,2}$ is the current timestamp and $MAC_{s,2} = H(GS\|v_i\|Sat_a\|g^{x_s}\|e(g,g)^{k_i}\|TS_{s,2})$ is the message authentication code. Besides, GS generates user-plane the session key $k_{i-s} = H(e(g,g)^{k_i \cdot x_s}\|TS_{i,1}\|TS_{s,2})$ shared with v_i, and the session key $k_{a-s} = H(g^{x_a \cdot x_s}\|TS_{a,1}\|TS_{s,1})$ shared with Sat_a. Finally, GS sends Msg_5 towards Sat_a.

Step-6: After receiving Msg_5, Sat_a first verifies the correctness of $MAC_{s,2}$. If $MAC_{s,2}$ is verified to be correct, Sat_a authenticates GS by guaranteeing that GS can correctly recover the key generator $e(g,g)^{k_i}$. Meanwhile, Sat_a generates the session key $k_{a-s} = H(g^{x_s \cdot x_a}\|TS_{a,1}\|TS_{s,1})$ shared with GS. Besides, Sat_a generates the control-plane session key shared with v_i, which is $k_{i-a} = H(e(g,g)^{k_i \cdot x_a}\|TS_{i,1}\|TS_{a,3})$ and $TS_{a,3}$ is the current timestamp. Furthermore, Sat_a encrypts the key generator g^{x_s} with k_{i-a} to protect the routing information. In addition, Sat_a generates the message authentication code $MAC_{a,3} = H(Sat_a\|v_i\|g^{x_a}\|GS\|g^{x_s}\|TS_{s,2}\|TS_{a,3})$. Finally, Sat_a formulates a message $Msg_6 = Sat_a\|v_i\|g^{x_a}\|Enc_{k_{i-a}}(GS\|g^{x_s}\|TS_{s,2})\|MAC_{a,3}\|TS_{a,3}$, and delivers it towards v_i, where $Enc(\cdot)$ is symmetric encryption algorithm like AES.

Step-7: After receiving Msg_6, v_i first calculates the control-plane session key $k_{i-a} = H(e(g^{k_i}, g^{x_a})\|TS_{i,1}\|TS_{a,3})$, and exploits k_{i-a} to decrypt $Enc_{k_{i-a}}(GS\|g^{x_s}\|TS_{s,2})$. Meanwhile, v_i verifies the correctness of $MAC_{a,3} \stackrel{?}{=} H(Sat_a\|v_i\|g^{x_a}\|GS\|g^{x_s}\|TS_{s,2}\|TS_{a,3})$. If $MAC_{a,3}$ is verified to be correct, v_i generates the user-plane session key $k_{i-s} = H(e(g^{k_i}, g^{x_s})\|TS_{i,1}\|TS_{s,2})$ shared with GS.

C. INTER-SATELLITE HANDOVER PHASE

In this subsection, we show the key establishment process during inter-satellite handover, and Fig. 3 shows the message flows between the involved entities, i.e., v_i, Sat_a and Sat_b. When Sat_a orbits out of the coverage of v_i, the accessing satellite switches from Sat_a towards Sat_b.

Step-1: Sat_a formulates a message $Msg_1 = Sat_a\|Sat_b\|MAC_{a,1}\|TS_{a,1}$, and delivers it towards Sat_b, where $MAC_{a,1} = H(Sat_a\|Sat_b\|TS_{a,1})$ is the message authentication code and $TS_{a,1}$ is the current timestamp. Meanwhile, Sat_a sends the message Msg_1 towards Sat_b.

Step-2: When Sat_b receives the message Msg_1, it first verifies the correctness of $MAC_{a,1}$. If $MAC_{a,1}$ is verified to be correct, Sat_b generates the ciphertext of $g_1^{u_b}$, which is

$$\begin{cases} c_{b,1} = g^{r_b}, c_{b,2} = \left(g_1^{H(Sat_b)} \cdot h\right)^{r_b}, \\ c_{b,3} = g_1^{u_b} \cdot H(e(g_1, g_2)^{r_b}). \end{cases} \tag{11}$$

Meanwhile, Sat_b generates the message authentication code $MAC_{b,1} = H(Sat_b\|Sat_a\|g^{x_b}\|g_1^{u_b}\|TS_{b,1})$, formulates a message $Msg_2 = Sat_b\|Sat_a\|g^{x_b}\|c_b\|MAC_{b,1}\|TS_{b,1}$, and it sends Msg_2 towards Sat_a.

Algorithm 1 Stack_Generation($\{e(g,g)^{k_i}, i \in \mathcal{K}\}$)

for $i = 1$ to $(n-2)$ **do**
  $w_i = e(g,g)^{k_{i+1} - k_{i+2}}$;
  $Push(w_i)$;
end for
$w_{n-1} = \prod_{i \in \mathcal{K}, i \neq n} e(g,g)^{-k_i}$;
$Push(w_{n-1})$;
Output: Stack $\mathcal{S}$

Step-3: After receiving Msg_2, Sat_a decrypts $g_1^{u_b}$ with its secret key $(sk_{b,1} = g_2^{\alpha} \cdot (g_1^{H(Sat_b)} \cdot h)^{u_b}, sk_{b,2} = g^{u_b})$, which is

$$g_1^{u_b} = c_{b,3}/H\left(\frac{e(c_{b,1}, sk_{b,1})}{e(c_{b,2}, sk_{b,2})}\right). \tag{12}$$

Meanwhile, Sat_a verifies the correctness of $MAC_{b,1}$. If $MAC_{b,1}$ is verified to be correct, Sat_a encrypts $Sat_b\|g^{x_b}$ with the session key k_{i-a}, which is $Enc_{k_{i-a}}(Sat_b\|g^{x_b}\|TS_{b,1})$. In addition, Sat_a generates the message authentication code $MAC_{a,i} = H(Sat_a\|v_i\|Sat_b\|g^{x_b}\|TS_{b,1}\|TS_{a,i})$, formulates a message $Msg_{a-i} = Sat_a\|v_i\|Enc_{k_{i-a}}(Sat_b\|g^{x_b}\|TS_{b,1})\|MAC_{a,i}\|TS_{a,i}$, and delivers it towards v_i, where $TS_{a,i}$ is the current timestamp.

Step-4: When v_i receives Msg_{a-i}, it first decrypts $Enc_{k_{i-a}}(Sat_b\|g^{x_b}\|TS_{b,1})$ with the session key k_{i-a}, and verifies the correctness of $MAC_{a,i}$. If $MAC_{a,i}$ is verified to be correct, v_i generates the message authentication code $MAC_{i,a} = H(v_i\|Sat_a\|Sat_b\|g^{x_b}\|TS_{b,1}\|TS_{i,a})$, formulates a message $Msg_{i-a} = v_i\|Sat_a\|MAC_{i,a}\|TS_{i,a}$, and delivers it to Sat_a. Besides, v_i generates the session key $k_{i-b} = H(e(g^{x_b}, g^{k_i}))$ shared with Sat_b.

Step-5: After receiving the handover responses from a group $\mathcal{K}$ of n users, Sat_a first verifies the correctness of $\{MAC_{i,a}, i \in \mathcal{K}\}$. If they are verified to be correct, Sat_a aggregates the received ciphertext contained in the set $\{c_i, i \in \mathcal{K}\}$, and derives the aggregated ciphertext $(\hat{C}_1, \hat{C}_2, \hat{C}_3)$, which is

$$\begin{cases} \hat{C}_1 = \prod_{i \in \mathcal{K}} c_{i,1} = g^{\sum_{i \in \mathcal{K}} r_{i,1}}, \\ \hat{C}_2 = \prod_{i \in \mathcal{K}} c_{i,2} = \left(g_1^{H(Sat_a)} \cdot h\right)^{\sum_{i \in \mathcal{K}} r_{i,1}}, \\ \hat{C}_3 = \prod_{i \in \mathcal{K}} c_{i,3} = e(g,g)^{\sum_{i \in \mathcal{K}} k_i} \cdot e(g_1, g_2)^{\sum_{i \in \mathcal{K}} r_{i,1}}. \end{cases} \tag{13}$$

Meanwhile, Sat_a re-encrypts $\hat{C}_3$ with Sat_b's re-encryption key $g_1^{u_b}$, and derives a new ciphertext $\hat{C}_4$, which is $\hat{C}_4 = \hat{C}_3 \cdot e(\hat{C}_1^{H(Sat_b) - H(Sat_a)}, g_1^{u_b})$. Furthermore, Sat_a generates a stack $\mathcal{S}$ based on the key generators $\{e(g,g)^{k_i}, i \in \mathcal{K}\}$, following the steps defined in Algorithm 1. Here we exploit a stack to characterize the sequential storage of the elements in the stack, which contains the sequential vector $[w_1, w_2, \ldots, w_{n-1}]^T$, and the storage of the vector is based on the *last in first out (LIFO)* principal. Besides, Sat_a generates the message authentication code $MAC_{a,2} = H(Sat_a\|Sat_b\|e(g,g)^{k_1}\|\cdots\|e(g,g)^{k_n}\|TS_{a,2})$ of set $\mathcal{K}$, where $TS_{a,2}$ is the current timestamp. Finally, Sat_a formulates a handover message $Msg_3 =$

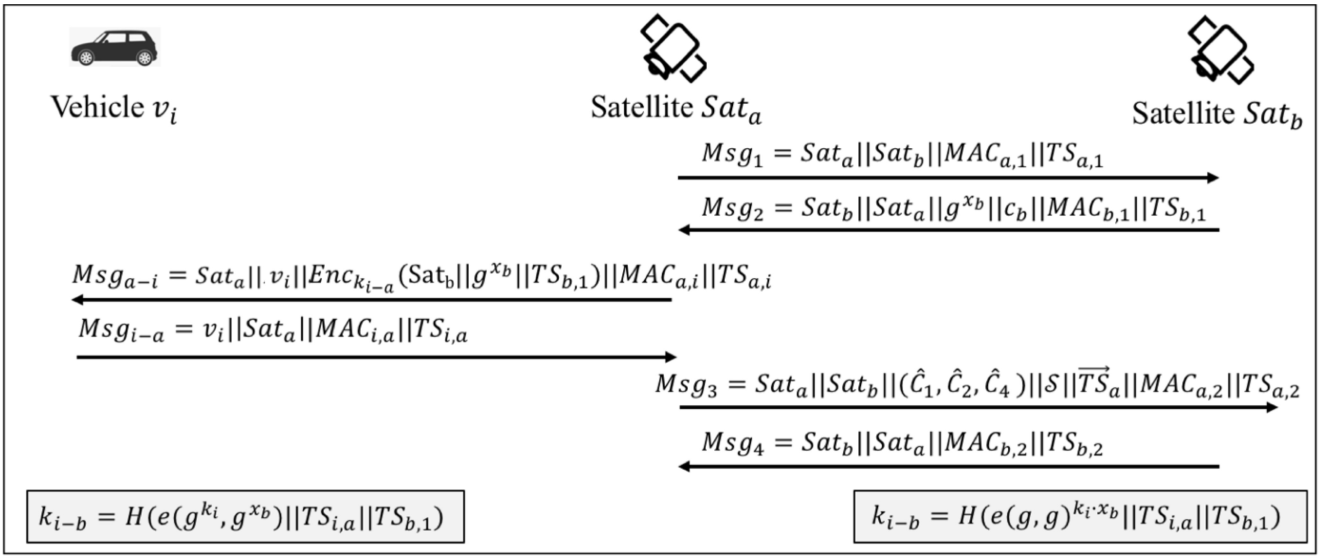


FIGURE 3. Message Flows during Inter-satellite Handover.

Algorithm 2 Generator_Recovery(Stack $\mathcal{S}$, w_n)

$y_n = Pop(\mathcal{S}) \cdot w_n$
$z_n = w_n / y_n$
for $i = (n-1)$ to 2 **do**
  $y_i = y_{i+1} \cdot Pop(\mathcal{S})$;
  $z_i = z_{i+1} / y_i$;
end for
$y_1 = z_2$;
Output: $\mathcal{Y} = \{y_n, y_{n-1}, \ldots, y_2, y_1\}$

$Sat_a \| Sat_b \| (\hat{C}_1, \hat{C}_2, \hat{C}_4) \| \mathcal{S} \| \overrightarrow{TS}_a \| MAC_{a,2} \| TS_{a,2}$, and sends it to Sat_b.

After receiving Msg_3, Sat_b first decrypts $w_n = e(g, g)^{\sum_{i \in \mathcal{K}} k_i}$, which is

$$w_n = e(g, g)^{\sum_{i \in \mathcal{K}} k_i} = \frac{\hat{C}_4 \cdot e\left(\hat{C}_2, sk_{b,2}\right)}{e\left(\hat{C}_1, sk_{b,1}\right)}. \tag{14}$$

Meanwhile, Sat_b first derives the sequential vector $W = [w_{n-1}, \ldots, w_2, w_1]^T$, by recovering the value set $\mathcal{Y}$ with Algorithm 2, and finally obtains the key generator set $\mathcal{Y} = \{y_n, y_{n-1}, \ldots, y_2, y_1\} = \{e(g, g)^{k_n}, e(g, g)^{k_{n-1}}, \ldots, e(g, g)^{k_2}, e(g, g)^{k_1}\}$. Furthermore, Sat_b verifies the correctness of $MAC_{a,2}$ with the recovered key generator set $\mathcal{Y}$. In addition, Sat_b generates a message authentication code $MAC_{b,2} = H(Sat_b \| Sat_a \| e(g, g)^{k_1} \| \cdots \| e(g, g)^{k_n} \| TS_{b,2})$, formulates a message $Msg_4 = Sat_b \| Sat_a \| MAC_{b,2} \| TS_{b,2}$, and delivers Msg_4 towards Sat_a, where $TS_{b,2}$ is the current timestamp. Finally, Sat_b computes the session key $k_{i-b} = H((e(g, g)^{k_i})^{x_b})$ shared with each vehicle v_i.

Step-6: After receiving Msg_4, Sat_a first verifies the correctness of $MAC_{b,2}$, and if $MAC_{b,2}$ is verified to be correct, Sat_a can authenticate Sat_b.

V. SECURITY ANALYSIS

In this section, we analyze the security properties of the proposed secure user access and inter-satellite handover scheme in an LEO constellation, in terms of confidentiality, authentication, and backward/forward key separation.

Confidentiality: We first analyze the goal of confidentiality during the *User Access Phase*. For the control-plane confidentiality, the key generator $e(g, g)^{k_i}$ of vehicle v_i is protected with the ciphertext tuple $(c_{i,1}, c_{i,2}, c_{i,3})$. Since the identity-based proxy re-encryption system [17] we exploit is proven to be semantically secure under the $(k, t, \epsilon) - dBDH$ assumption, the key generator $e(g, g)^{k_i}$ can be successfully protected. Even though the key generator $e(g, g)^{k_i}$ is shared with GS, the construction of the session key k_{i-a} also requires the secret value x_a at the Sat_a side. Meanwhile, the key establishment at the v_i side requires both the value of g^{x_a} and g^{k_i}, and only v_i can recover the value of g^{k_i}. Therefore, only v_i and Sat_a can generate the control-plane session key k_{i-a}. For the user-plane confidentiality, our scheme first generates the re-encrypted ciphertext $(c_{i,1}, c_{i,2}, c_{i,4})$, which is proven to be secure. Given the re-encrypted ciphertext-tuple $(c_{i,1}, c_{i,2}, c_{i,4})$ generated by Sat_a, only GS can decrypt the value $e(g, g)^{k_i}$ for the establishment of the user-plane session key k_{i-s}. Even though Sat_a can obtain the value $e(g, g)^{k_i}$, Sat_a still cannot recover the session key k_{i-s} without the secret value x_s. Thus, the security goal of confidentiality can be achieved during the *User Access Phase*.

During the *Inter-satellite Handover Phase*, Sat_a aggregates the received ciphertexts $(c_{i,1}, c_{i,2}, c_{i,3}), i \in \mathcal{K}$ for $(\hat{C}_1, \hat{C}_2, \hat{C}_3)$, re-encrypts it to derive a new ciphertext $(\hat{C}_1, \hat{C}_2, \hat{C}_4)$, and delivers it towards Sat_b with the stack $\mathcal{S}$. For Sat_b, it decrypts $(\hat{C}_1, \hat{C}_2, \hat{C}_4)$ for the aggregated key generator $w_n = e(g, g)^{\sum_{i \in \mathcal{K}} k_i}$, and then recovers the key generators $\{e(g, g)^{k_1}, e(g, g)^{k_2}, \ldots, e(g, g)^{k_n}\}$. Without Sat_b's secret key sk_b, the key generators cannot be recovered merely based on content stored in the stack $\mathcal{S}$. Therefore, the security goal of confidentiality can be achieved during the *Inter-satellite Handover Phase*.

Authentication: During the *User Access Phase*, v_i authenticates itself towards Sat_a through an identity-based signature proposed in [18], which is proven to be semantically secure on k-CCA. Given the signature pair $(\sigma_{i,1}, \sigma_{i,2})$, Sat_a can authenticate the correctness of the key generator $e(g, g)^{k_i}$. After receiving Msg_6, v_i can authenticate Sat_a by checking the $MAC_{a,3}$, which contains the key generator $e(g, g)^{k_i}$, this is because only Sat_a can decrypt $(c_{i,1}, c_{i,2}, c_{i,3})$. Based on the ciphertext c_s contained in Msg_3 and $MAC_{a,2}$ contained in Msg_4, the authentication of Sat_a towards GS can be achieved through the successful recovery of the re-encryption key $g_1^{u_s}$. Furthermore, based on $\hat{c}_i$ contained in Msg_4 and $MAC_{s,2}$ contained in Msg_5, the authentication of GS towards Sat_a can be achieved through the successful decryption of the key generator $e(g, g)^{k_i}$.

During the *Inter-satellite Handover Phase*, Sat_a can authenticate itself towards Sat_b, based on the ciphertext c_b contained in Msg_2 and $MAC_{a,2}$ contained in Msg_3, by the recovery of the re-encryption key $g_1^{u_b}$. On the other hand, Sat_b can authenticate itself towards Sat_a through the derivation of the key generators contained in Msg_4. Therefore, the security goal of authentication can be achieved in the proposed scheme.

Backward/Forward Key Separation: The proposed scheme also achieves the security goal of forward/backward key separation. Since the user-plane session key k_{i-s} is only shared between GS and v_i, it keeps unchanged during each inter-satellite handover, and we only consider the key separation in the control-plane. For the backward key separation, the construction of the session key k_{i-a} shared between Sat_a and v_i requires the recovery of $e(g, g)^{k_i}$ contained in $(c_{i,1}, c_{i,2}, c_{i,3})$, which can only be decrypted by Sat_a and it cannot be decrypted by Sat_b before handover.

For the forward key separation, the construction of the session key k_{i-b} requires the recovery of the generator $e(g, g)^{k_i}$, which is contained in the ciphertext tuple $(\hat{C}_1, \hat{C}_2, \hat{C}_4)$ and the stack $\mathcal{S}$. Simply based on the value vector $\{w_1, w_2, \ldots, w_{n-1}\}$ contained in the stack $\mathcal{S}$, it is impossible to infer the value of the set $\mathcal{Y} = \{y_1, y_2, \ldots, y_n\}$. This is because there is infinite possible solutions of a equation set with $n-1$ equations and n unknown variables. Thus, if an adversary obtains the stack $\mathcal{S}$, the set $\mathcal{Y}$ still cannot be recovered without w_n. Even though Sat_a can also obtain the value $e(g, g)^{k_i}$, the construction of the session key k_{i-b} includes the secret value x_b at Sat_b side, which is unknown by Sat_a. Thus, the security goal of forward/backward key separation can be achieved.

VI. PERFORMANCE EVALUATIONS

In this section, we evaluate the performance of the proposed secure user access and inter-satellite handover mechanism in an LEO constellation. We first show a traditional scheme for comparison, and then we compare and illustrate the efficiency of the proposed scheme in terms of computational and communication efficiency. We compare the proposed scheme with a traditional scheme without the identity-based proxy re-encryption scheme. For a vehicle v_i, it performs the following steps to generate the service request.

- Since the proposed scheme does not consider the proxy re-encryption process, to achieve both the control-plane and user-plane key establishments, v_i selects two random numbers $(\hat{r}_{i,1}, \hat{k}_{i,1}) \in \mathbb{Z}_p^*$ to generate the identity-based ciphertext pairs,

$$\begin{cases} \hat{c}_{i,1}^a = g^{\hat{r}_{i,1}}, \hat{c}_{i,2}^a = \left(g_1^{H(Sat_a)} \cdot h\right)^{\hat{r}_{i,1}}, \\ \hat{c}_{i,3}^a = e(g, g)^{\hat{k}_{i,1}} \cdot e(g_1, g_2)^{\hat{r}_{i,1}}, \end{cases} \tag{15}$$

  in which $e(g, g)^{\hat{k}_{i,1}}$ is a generator for the control-plane session key $\hat{k}_{i-a}$ shared between Sat_a and V_i. Meanwhile, it generates the corresponding identity-based signature pair $(\hat{\sigma}_{i,1}^a, \hat{\sigma}_{i,2}^a)$. To achieve the user-plane key establishment, v_i selects another two random numbers $(\hat{r}_{i,2}, \hat{k}_{i,2}) \in \mathbb{Z}_p^*$ to compute the ciphertext pairs,

$$\begin{cases} \hat{c}_{i,1}^s = g^{\hat{r}_{i,2}}, \hat{c}_{i,2}^s = \left(g_1^{H(gs)} \cdot h\right)^{\hat{r}_{i,2}}, \\ \hat{c}_{i,3}^s = e(g, g)^{\hat{k}_{i,2}} \cdot e(g_1, g_2)^{\hat{r}_{i,2}}, \end{cases} \tag{16}$$

  where $e(g, g)^{\hat{k}_{i,2}}$ is a generator for the user-plane session key $\hat{k}_{i-s}$ shared between GS and v_i. Besides, it generates the corresponding identity-based signature pair $(\hat{\sigma}_{i,1}^s, \hat{\sigma}_{i,2}^s)$ with the key generator $e(g, g)^{\hat{k}_{i,2}}$. Finally, v_i formulates an access request $\hat{Req}_{v-a} = \hat{c}_i^a \| \hat{\sigma}_i^a \| \hat{c}_i^s \| \hat{\sigma}_i^s \| \hat{TS}_i$, and sends it towards Sat_a.
- For Sat_a, it first decrypts the key generator $e(g, g)^{\hat{k}_{i,1}}$ with its private key $(sk_{a,1}, sk_{a,2})$, and verifies the correctness of the key generator with the signature pair $(\hat{\sigma}_{i,1}^a, \hat{\sigma}_{i,2}^a)$. Furthermore, Sat_a delivers the request $\hat{Req}_{v-s} = \hat{c}_i^s \| \hat{\sigma}_i^s \| \hat{TS}_i$ towards GS. After receiving $\hat{Req}_{v-s}$, GS decrypts the key generator $e(g, g)^{\hat{k}_{i,2}}$ with the private key $(sk_{s,1}, sk_{s,2})$, and verifies its correctness of the signature pair $(\hat{\sigma}_{i,1}^s, \hat{\sigma}_{i,2}^s)$.
- During the handover process, v_i selects two random numbers $(\hat{r}_{i,3}, \hat{k}_{i,3}) \in \mathbb{Z}_p^*$, and generates the ciphertext pairs, which is

$$\begin{cases} \hat{c}_{i,1}^b = g^{\hat{r}_{i,3}}, \hat{c}_{i,2}^b = \left(g_1^{H(Sat_b)} \cdot h\right)^{\hat{r}_{i,3}}, \\ \hat{c}_{i,3}^b = e(g, g)^{\hat{k}_{i,3}} \cdot e(g_1, g_2)^{\hat{r}_{i,3}}. \end{cases} \tag{17}$$

  Meanwhile, v_i also generates the identity-based signature pair $(\hat{\sigma}_{i,1}^b, \hat{\sigma}_{i,2}^b)$ with the key generator $e(g, g)^{\hat{k}_{i,3}}$. Besides, v_i formulates a handover request $HO\_msg_{v-b} = \hat{c}_i^b \| \hat{\sigma}_i^b \| \hat{TS}_i$, and sends it to Sat_b through the forwarding of Sat_a. For Sat_b, it also decrypts the key generator $e(g, g)^{\hat{k}_{i,3}}$ with its private key $(sk_{b,1}, sk_{b,2})$, and verifies its correctness of the signature $(\hat{\sigma}_{i,1}^b, \hat{\sigma}_{i,2}^b)$.

A. COMPUTATIONAL EFFICIENCY

In this subsection, we demonstrate the computational efficiency of the proposed scheme. Specifically, we test the performance by using a desktop with Windows 10 Enterprise platform, Intel Core i7-8700 CPU @ 3.20GHz 3.19GHz processor, and 8.00 GB RAM. Furthermore, we exploit the Java Pairing-Based Cryptography Library (JPBC) Type-A1 generator for the bilinear parameters. In addition, we test the computational costs of one exponentiation operation in $\mathbb{G}$, one exponentiation operation in $\mathbb{G}_T$, and that of one bilinear pairing operation, and we derive the test results of $T^1_{exp} = 7.92$ ms, $T^2_{exp} = 0.55$ ms, and $T_{bp} = 4.39$ ms.

1) USER ACCESS PHASE

In *Step-1*, v_i takes 4 exponentiation operations in $\mathbb{G}$ and 3 exponentiation operation in $\mathbb{G}_T$ to generate Msg_1. In *Step-2*, Sat_a it takes 2 bilinear pairing operations to decrypt the ciphertext $(c_{i,1}, c_{i,2}, c_{i,3})$, as well as 1 exponentiation operation in $\mathbb{G}$, 1 exponentiation operation in $\mathbb{G}_T$, and 1 bilinear pairing operation to verify the correctness of σ_i. In *Step-3*, *GS* performs 3 exponentiation operations in $\mathbb{G}$ and 1 exponentiation operation in $\mathbb{G}_T$ to generate c_s. In *Step-4*, Sat_a takes 2 bilinear pairing operations to decrypt c_s, as well as 1 exponentiation operation in $\mathbb{G}$ and 1 bilinear pairing operation for proxy re-encryption. In *Step-5*, *GS* takes 2 bilinear pairing operations for decryption, 1 exponentiation operation in $\mathbb{G}$ to generate g^{x_s}, and 1 exponentiation operation in $\mathbb{G}_T$ to generate the user-plane session key k_{i-s}. In *Step-6*, Sat_a takes 1 exponentiation operation in $\mathbb{G}$ to generate g^{x_a}, and 1 exponentiation operation in $\mathbb{G}_T$ to generate the control-plane session key k_{i-a}. Meanwhile, v_i takes 2 bilinear pairing operations for the generation of k_{i-a} and k_{i-s}. Therefore, when there exists n users, the computational complexity introduced to each vehicle is $4 \times T^1_{exp} + 3 \times T^2_{exp} + 2 \times T_{bp}$, the computational complexity introduced to Sat_a is $(2 \times T^1_{exp} + 2 \times T^2_{exp} + 3 \times T_{bp}) \times n + T^2_{exp} + 3 \times T_{bp}$, and the computational overhead introduced to *GS* is $(T^1_{exp} + T^2_{exp} + 2 \times T_{bp}) \times n + 3 \times T^1_{exp} + T^2_{exp}$.

For the compared traditional scheme, to generate n ciphertext pairs and signature pairs, the computational overhead of the vehicles is $6 \times n \times T^1_{exp} + 6 \times n \times T^2_{exp}$. Besides, the corresponding overhead for key establishment is $2 \times n \times T^1_{exp} + 2 \times n \times T_{bp}$. For Sat_a, the computational complexity introduced for decryption, signature verification and key establishment of n users is $2 \times n \times T^2_{exp} + 4 \times n \times T_{bp}$. Meanwhile, the corresponding overhead of *GS* introduced by n users is $2 \times n \times T^2_{exp} + 4 \times n \times T_{bp}$.

As shown in Fig. 4, during the *User Access Phase*, when the scale of vehicles ranges between 1 to 20, the computational overhead introduced by the proposed scheme greatly reduces in comparison with the traditional scheme. When the number of vehicle is set to be 20, the computational overhead of the proposed scheme during the user access phase, is 1805.3 ms and that of the compared scheme is 2552.2 ms.

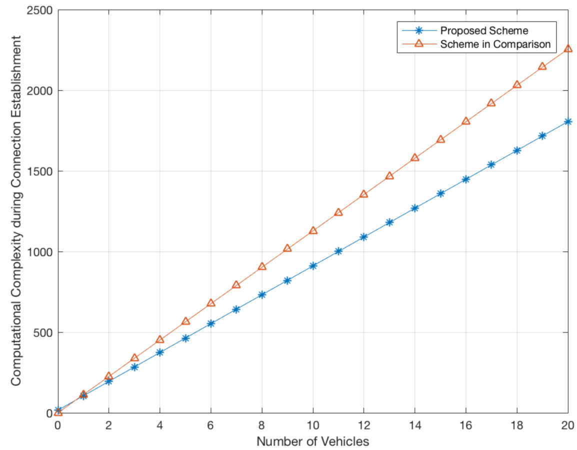


FIGURE 4. Computational Complexity for Key Establishment during User Access.

2) INTER-SATELLITE HANDOVER PHASE

In *Step-2*, Sat_b takes 3 exponentiation operations in $\mathbb{G}$ and 1 exponentiation operation in $\mathbb{G}_T$ to generate the ciphertext c_b; meanwhile, it takes 1 exponentiation operation in $\mathbb{G}$ to generate the generator g^{x_b}. In *Step-3*, Sat_a exploits 2 bilinear pairing operations for decryption. In *Step-4*, v_i performs 1 bilinear pairing operation for the key generation of k_{i-b}. In *Step-5*, Sat_a performs 1 exponentiation operation in $\mathbb{G}$ and 1 bilinear pairing operation for proxy re-encryption. On the other hand, Sat_b takes 2 bilinear pairing operations for decryption and n exponentiation operations in $\mathbb{G}_T$ for key generation. Thus, when there exists n users, the computational complexity of Sat_a is $T^1_{exp} + 3 \times T_{bp}$, the computational complexity of Sat_b is $n \times T^2_{exp} + 4 \times T^1_{exp} + T^2_{exp} + 2 \times T_{bp}$, and the computational complexity of each vehicle is T_{bp}.

In the traditional scheme, the computational overhead for the ciphertext and signature generation of n users is $3 \times n \times T^1_{exp} + 3 \times n \times T^2_{exp}$, and that of key establishment is $n \times T^1_{exp} + n \times T_{bp}$. The computational overhead introduced by n users towards Sat_b is $n \times T^2_{exp} + 5 \times n \times T_{bp}$.

As shown in Fig. 5, during the *Inter-satellite Handover Phase*, when the scale of vehicle ranges between 1 to 20, our proposed scheme requires less computational complexity than the traditional scheme. Specifically, when the number of vehicle is set to be 20, the corresponding overhead of the proposed scheme is 160.9 ms, and that of the traditional scheme is 1204.4 ms. The reduction of the computational overhead in our proposed scheme is because of the introduction of the proxy re-encryption technique and the stack.

B. COMMUNICATION OVERHEADS

We exploit the Type-A1 bilinear pairing for the generation of security parameters, in which each generator has the length of 1024 bits. Meanwhile, the length of each timestamp is set to be 32 bits, and that of each identity is 32 bits.

For the proposed scheme, during the *User Access Phase*, the v_i-to-Sat_a communication overhead of Msg_1 is $5 \times 1024+$

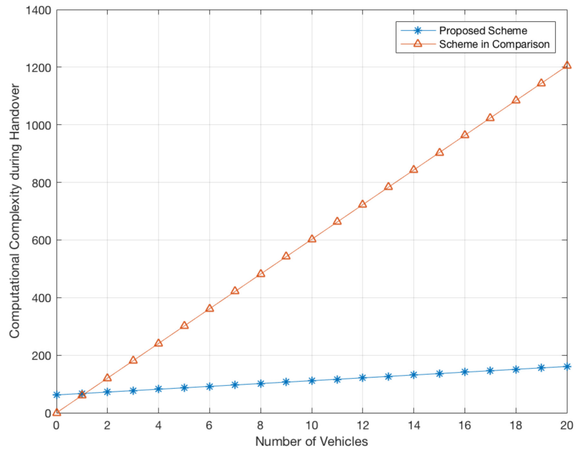


FIGURE 5. **Computational Complexity for Key Establishment during Inter-satellite Handover.**

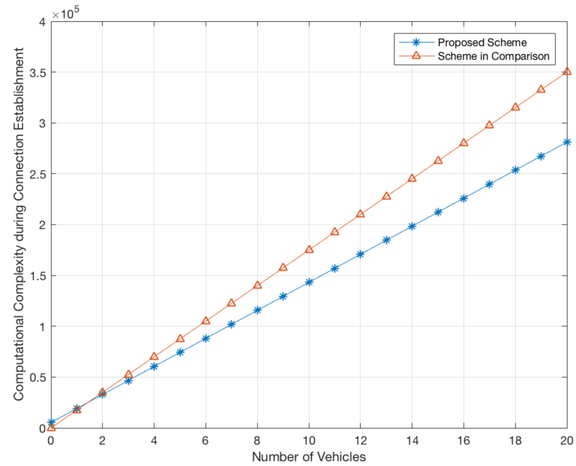


FIGURE 6. **Communication Overhead during User Access.**

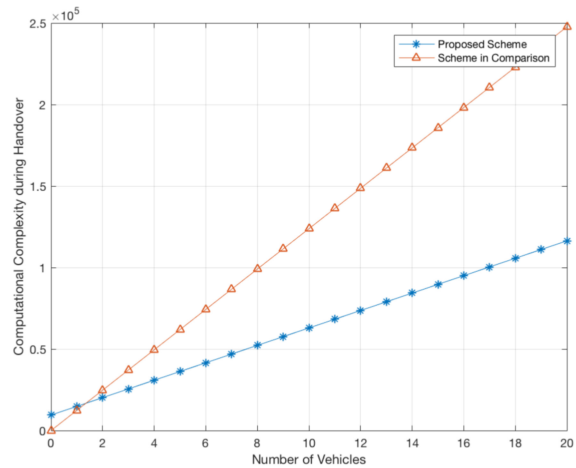


FIGURE 7. **Communication Overhead during Secure Handover.**

3×32 bits. Meanwhile, the Sat_a-to-GS communication overhead of Msg_2 is $1024 + 3 \times 32$ bits, and the GS-to-Sat_a communication overhead of Msg_3 is $4 \times 1024 + 3 \times 32$ bits. Furthermore, the Sat_a-to-GS communication overhead of Msg_4 is $4 \times 1024 + 5 \times 32$ bits, and the GS-to-Sat_a communication overhead of Msg_5 is $2 \times 1024 + 4 \times 32$ bits. In addition, the Sat_a-to-v_i overhead is $4 \times 1024 + 3 \times 32$ bits. Thus, when there exists n users, the involved communication overhead of the *User Access Phase* is $(13 \times n + 5) \times 1024 + (15 \times n + 6) \times 32$ bits.

During the *Inter-satellite Handover Phase*, the Sat_a-to-Sat_b communication overhead of Msg_1 is $1024 + 3 \times 32$ bits, and the Sat_b-to-Sat_a communication overhead of Msg_2 is $5 \times 1024 + 3 \times 32$ bits. Meanwhile, the Sat_a-to-v_i communication overhead of Msg_{a-i} is $3 \times 1024 + 3 \times 32$ bits, and v_i-to-Sat_a communication overhead of Msg_{i-a} is $1024 + 3 \times 32$ bits. In addition, the Sat_a-to-Sat_b communication overhead Msg_3 is $(n + 3) \times 1024 + (n + 3) \times 32$ bits, and the Sat_b-to-Sat_a communication overhead of Msg_4 is $1024 + 3 \times 32$ bits. Therefore, the communication overhead of the *Inter-satellite Handover Phase* is $(5 \times n + 9) \times 1024 + (7 \times n + 9) \times 32$ bits.

For the traditional scheme, during the *User Access Phase*, the overhead of the v_i-to-Sat_a connection $\hat{c}_i^a \| \hat{\sigma}_i^a \| \hat{c}_i^s \| \hat{\sigma}_i^s \| \hat{TS}_i$ is $(10 \times 1024 + 32)$ bits, the communication overhead introduced by the Sat_a-to-v_i connection $Enc_{k_{i-a}}(GS \| g^{x_s}) \| MAC_{a,1} \| \hat{TS}_{a,1}$ is also $(2 \times 1024 + 32)$ bits. Meanwhile, the overhead of the Sat_a-to-GS connection is $\hat{c}_i^s \| \hat{\sigma}_i^s \| \hat{TS}_i$ is $(5 \times 1024 + 32)$ bits. Besides, during the *Inter-satellite Handover Phase*, the Sat_a-to-v_i communication overhead is $(2 \times 1024 + 32)$ bits, the v_i-to-Sat_a overhead of $\hat{c}_i^b \| \hat{\sigma}_i^b \| \hat{TS}_i'$ is $(5 \times 1024 + 32)$ bits, and the Sat_a-to-Sat_b overhead of $\hat{c}_i^b \| \hat{\sigma}_i^b \| \hat{TS}_i'$ is $(5 \times 1024 + 32)$ bits.

Fig. 6 and Fig. 7 show the communication overheads of the proposed scheme and the traditional scheme with respect to the increase of vehicles, during both the *User Access* and *Secure Handover* phases. As shown in Fig. 6, when the number of vehicle is 20, the communication overhead of the proposed scheme is 281152 bits, and that of the traditional scheme is 350080 bits. While during the handover phase, the communication overhead of the proposed scheme is 116384 bits when the number of vehicles is 20, and the corresponding communication overhead of the traditional scheme is 247680 bits. As shown in the above figures, the communication overhead of the proposed scheme is greatly reduced in comparison with the traditional scheme.

To show the feasibility of the proposed scheme, we further examine the relationship of the communication complexity with the number of handover, as well as the average number of users. During each inter-satellite handover, the communication overhead introduced is $(5 \times n + 9) \times 1024 + (7 \times n + 9) \times 32$ bits when there exists n vehicles. When it experiences m handovers, the total communication overhead introduced is $((5 \times n + 9) \times 1024 + (7 \times n + 9) \times 32) \times m$ bits. As shown in Fig. 8, when the number of vehicle is 20 and the handover scale is 10, the communication overhead incurred is 1.16×10^6 bits.

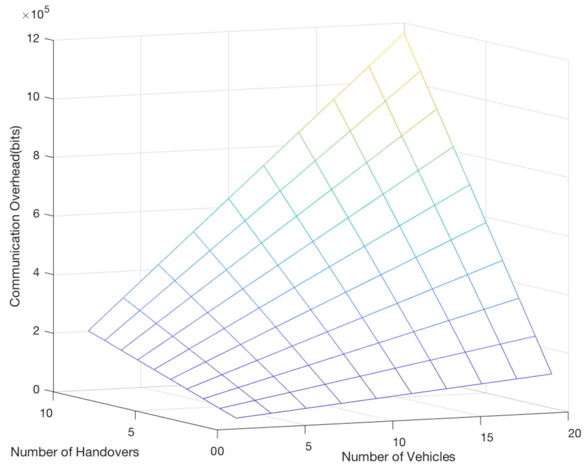


FIGURE 8. Communication Overhead with Scale of Vehicles and Number of Handovers.

VII. RELATED WORKS

In this section, we briefly review some works highly relevant to our proposed scheme, i.e., key management schemes [19] and secure handover mechanisms related to LEO satellite constellations.

A. KEY MANAGEMENT SCHEMES IN LEO SATELLITE NETWORKS

Chowdhury *et al.* in [20], [21] propose a key management framework for a hybrid satellite network, which securely and scalably distributes the cryptographic keys for group communications. Howarth *et al.* in [22] address the issue of efficient key management, for the protection of the satellite-based multi-cast traffic transmission. Since the group scale and dynamics highly influence the network overhead, the proposed scheme exploits a logical key hierarchy (LKH) to reduce the life-cycle key management costs. For the marine-based STIN scenario, Shen *et al.* in [23] design a secure emergency data protection scheme. Specifically, the proposed scheme exploits a block-design-based key agreement to achieve efficient communication among the satellites. Besides, Li *et al.* in [24] propose a network intrusion detection system in STIN, which analyzes and resists malicious traffic, especially the distributed denial-of-service (DDoS) attacks. By exploiting an ID-based framework, Gowri *et al.* in [25] propose an efficient identity-based authentication scheme for the Automatic dependent surveillance-broadcast (ADS-B) system, which is pairing-free and supports batch verification.

However, the above key management schemes focus the multicast or broadcast cases, which is different from the LEO satellite scenario, which requires the control-plane and user-plane key establishments. Besides, the main resource bottleneck of the above schemes is the computational complexity; however, for the LEO constellation, the resource bottleneck also exists in the long propagation delay and the communication overhead.

B. SECURE HANDOVER SCHEMES IN LEO SATELLITE NETWORKS

To achieve the efficient handover between different satellites, various handover mechanisms for satellite networks have been proposed [26]–[28], and these mechanisms can be characterized into three types: reinforcement learning, game theory, and optimization criteria. Zhu *et al.* in [29] propose a novel proactive group handover scheme for an LEO satellite network, which partitions the users with similar patterns in terms of the handover trajectory and mobility pattern into groups. However, the above-mentioned schemes focus on handover planning and do not consider any security issue. Chang *et al.* in [30] propose an authentication scheme for satellite communication systems; however, each authentication process involves the participation of the network control center (NCC), which is unrealistic for our scenario with ground stations deployed by third-parties. Meng *et al.* in [7] propose a proxy signature-based authentication scheme for SIN, in which the ground station produces a temporal delegation for the satellite after authentication. However, when a user migrates to a new satellite, the same authentication process between the user and the satellite needs to be performed again, which involves heavy overheads.

Yang *et al.* in [8] propose an anonymous and fast roaming authentication scheme, which exploits the group signature to provide anonymity for the roaming users. For example, when a user roams to a foreign network, the foreign LEO can act as a verifier to check the validity of the access request. However, when a user attaches to a new satellite, a new session key needs to be re-constructed following the identical access authentication process, which involves heavy communication and computation overheads. Xue *et al.* in [11] present a lightweight key agreement protocol based on the secret-sharing technology, in which the LEO satellites negotiate a shared group key with the assistance of the GEO satellites. When a user roams across different LEO satellites, the overhead of the secure link re-establishment in terms of the handover authentication phase can be greatly reduced due to the construction of group keys. However, the group key construction process requires the involvement of the group manager and the GEO satellite. Meanwhile, due to the dynamic changing topology of LEO satellites, the availability of GEO satellites and the update frequency of the LEO satellite group also need to be carefully evaluated. In addition, Xue *et al.* in [10] propose a secure access and handover scheme for space information networks (SINs), which does not require the online involvement of the network control center (NCC). However, the above scheme still fails to consider the inter-satellite links in an LEO constellation.

In the above schemes, the secure handover mechanisms only focus on the scenario in which the ground station changes with the satellite. In the case of scarce ground station deployment, we should also take the case when a satellite cannot be directly linked to a ground station, and the links established between the satellites also need to be evaluated. Furthermore, the above schemes do not consider the separation of the control- and user-plane signaling during the user access and inter-satellite handover phases.

VIII. CONCLUSION

In this paper, we have proposed an efficient and secure user access and inter-satellite handover mechanism in an LEO constellation-assisted beyond 5G system. With the proposed scheme, the control- and the user-plane session keys can be successfully established with high efficiency, during both the user access and inter-satellite handover phases. Detailed security analysis has been performed to demonstrate that our scheme satisfies the security goals of confidentiality, authentication, and backward/forward key separation. Performance evaluations have shown that our proposed scheme greatly outperforms the scheme without proxy re-encryption and stack, in terms of computational complexity and communication overhead. In future work, we will consider the design of security mechanisms for other LEO constellation use cases, like secure self-organizing satellite networks with high dynamics.

REFERENCES

[1] F. Yin *et al.*, "FedLoc: Federated learning framework for data-driven cooperative localization and location data processing," *IEEE Open J. Signal Process.*, vol. 1, pp. 187–215, 2020.

[2] W. Guo, H. Li, F. Yin, and B. Ai, "Vehicle location algorithm based on federated learning and smart phone in GNSS low sampling rate scene," *J. Phys. Conf. Ser.*, vol. 2066, no. 1, 2021, Art. no. 012052.

[3] B. Kloiber, T. Strang, H. Spijker, and G. J. Heijenk, "Improving information dissemination in sparse vehicular networks by adding satellite communication," in *Proc. IV*, 2012, pp. 611–617.

[4] G. Guo and S. Wen, "Communication scheduling and control of a platoon of vehicles in VANETs," *IEEE Trans. Intell. Transp. Syst.*, vol. 17, no. 6, pp. 1551–1563, Jun. 2016.

[5] Q. Kong, R. Lu, S. Chen, and H. Zhu, "Achieve secure handover session key management via mobile relay in LTE-advanced networks," *IEEE Internet Things J.*, vol. 4, no. 1, pp. 29–39, Feb. 2017.

[6] Q. Kong, M. Ma, and R. Lu, "Achieving secure CoMP joint transmission handover in LTE-A vehicular networks," in *Proc. VTC-Fall*, Toronto, ON, Canada, 2017, pp. 1–5.

[7] W. Meng, K. Xue, J. Xu, J. Hong, and N. Yu, "Low-latency authentication against satellite compromising for space information network," in *Proc. MASS*, Chengdu, China, 2018, pp. 237–244.

[8] Q. Yang, K. Xue, J. Xu, J. Wang, F. Li, and N. Yu, "AnFRA: Anonymous and fast roaming authentication for space information network," *IEEE Trans. Inf. Forensics Security*, vol. 14, pp. 486–497, 2019.

[9] S. Cakaj, "The parameters comparison of the 'starlink' LEO satellites constellation for different orbital shells," *Front. Commun. Netw.*, vol. 2, p. 7, May 2021.

[10] K. Xue, W. Meng, S. Li, D. S. L. Wei, H. Zhou, and N. Yu, "A secure and efficient access and handover authentication protocol for Internet of Things in space information networks," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 5485–5499, Jun. 2019.

[11] K. Xue, W. Meng, H. Zhou, D. S. L. Wei, and M. Guizani, "A lightweight and secure group key based handover authentication protocol for the software-defined space information network," *IEEE Trans. Wireless Commun.*, vol. 19, no. 6, pp. 3673–3684, Jun. 2020.

[12] A. K. Majumdar, "Free-space laser communication performance in the atmospheric channel," *J. Opt. Fiber Commun. Rep.*, vol. 2, no. 4, pp. 345–396, 2005.

[13] A. U. Chaudhry and H. Yanikomeroglu, "Laser intersatellite links in a starlink constellation: A classification and analysis," *IEEE Veh. Technol. Mag.*, vol. 16, no. 2, pp. 48–56, Jun. 2021.

[14] Q. Huang *et al.*, "Secure free-space optical communication system based on data fragmentation multipath transmission technology," *Opt. Exp.*, vol. 26, no. 10, pp. 13536–13542, 2018.

[15] D. Boneh, E.-J. Goh, and K. Nissim, "Evaluating 2-DNF formulas on ciphertexts," in *Proc. TCC*, 2005, pp. 325–341.

[16] *5G; Security Architecture and Procedures for 5G System*, 3GPP Standard TS 33.501 (version 15.1.0) Release 15, Jul. 2018.

[17] T. Matsuo, "Proxy re-encryption systems for identity-based encryption," in *Proc. Int. Conf. Pairing Based Cryptogr.*, 2007, pp. 247–267.

[18] S. Cui, P. Duan, C. W. Chan, and X. Cheng, "An efficient identity-based signature scheme and its applications," *Int. J. Netw. Security*, vol. 5, no. 1, pp. 89–98, 2007.

[19] L. Jianwei, L. Weiran, W. Qianhong, L. Dawei, and C. Shigang, "Survey on key security technologies for space information networks," *J. Commun. Inf. Netw.*, vol. 1, no. 1, pp. 72–85, Jun. 2016.

[20] A. R. Chowdhury and J. S. Baras, "Key management for secure multicast in hybrid satellite networks," in *Proc. SEC*, 2004, pp. 533–548.

[21] A. R. Chowdhury, J. S. Baras, M. H. Hadjitheodosiou, and S. Papademetriou, "Security issues in hybrid networks with a satellite component," *IEEE Wireless Commun.*, vol. 12, no. 6, pp. 50–61, Dec. 2005.

[22] M. P. Howarth, S. Iyengar, Z. Sun, and H. S. Cruickshank, "Dynamics of key management in secure satellite multicast," *IEEE J. Sel. Areas Commun.*, vol. 22, no. 2, pp. 308–319, Feb. 2004.

[23] J. Shen, C. Wang, S. Ji, T. Zhou, and H. Yang, "Secure emergent data protection scheme for a space-terrestrial integrated network," *IEEE Netw.*, vol. 33, no. 1, pp. 44–50, Jan. 2019.

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

[25] T. Gowri, N. B. Gayathri, P. V. Reddy, M. Z. U. Rahman, and A. Lay-Ekuakille, "Efficient pairing-free identity-based ADS-B authentication scheme with batch verification," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 55, no. 5, pp. 2473–2486, Oct. 2019.

[26] B. Yang, Y. Wu, X. Chu, and G. Song, "Seamless handover in software-defined satellite networking," *IEEE Commun. Lett.*, vol. 20, no. 9, pp. 1768–1771, Sep. 2016.

[27] Z. Wu, F. Jin, J. Luo, Y. Fu, J. Shan, and G. Hu, "A graph-based satellite handover framework for LEO satellite communication networks," *IEEE Commun. Lett.*, vol. 20, no. 8, pp. 1547–1550, Aug. 2016.

[28] S. Park and J. Kim, "Trends in LEO satellite handover algorithms," 2021, *arXiv:2107.08619*.

[29] K. Zhu, C. Hua, P. Gu, and W. Xu, "User clustering and proactive group handover scheduling in LEO satellite networks," in *Proc. ComComAp*, Beijing, China, 2020, pp. 1–6.

[30] C. Chang, T. Cheng, and H. Wu, "An authentication and key agreement protocol for satellite communications," *Int. J. Commun. Syst.*, vol. 27, no. 10, pp. 1994–2006, 2014.

QINGLEI KONG (Member, IEEE) received the B.Eng. degree in communication engineering from the Harbin Institute of Technology, Harbin, China, in 2012, the M.Eng. degree in electronic and information engineering from the Shenzhen Graduate School, Harbin Institute of Technology, Shenzhen, China, in 2015, and the Ph.D. degree from the School of Electrical and Electronics Engineering, Nanyang Technological University, Singapore, in 2018. She is currently working as an Assistant Professor with the Institute of Space Science and Applied Technology, Harbin Institute of Technology (Shenzhen). She used to work with Cyber Security Cluster, Institute for Infocomm Research, Singapore, and Tencent Security, Shenzhen, as a Research Scientist. She was a Postdoctoral Researcher with the Chinese University of Hong Kong, Shenzhen. Her research interests include applied cryptography, blockchain, VANET, and game theory.

RONGXING LU (Fellow, IEEE) received the Ph.D. degree from the Department of Electrical and Computer Engineering, University of Waterloo, Canada, in 2012. He is an Associate Professor with University Research Scholar, Faculty of Computer Science, University of New Brunswick, Canada. Before that, he worked as an Assistant Professor with the School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore, from April 2013 to August 2016. He worked as a Postdoctoral Fellow of the University of Waterloo from May 2012 to April 2013. He was awarded the most prestigious "Governor General's Gold Medal," from the Department of Electrical and Computer Engineering, University of Waterloo, Canada, in 2012, and won the 8th IEEE Communications Society Asia–Pacific Outstanding Young Researcher Award, in 2013.

FENG YIN (Senior Member, IEEE) received the B.Sc. degree from Shanghai Jiao Tong University, Shanghai, China, in 2008, and the M.Sc. and Dr.-Ing. degrees from Technische Universitat Darmstadt, Darmstadt, Germany, in 2011 and 2014, respectively. From 2014 to 2016, he worked with Ericsson Research, Linkoping, Sweden, mainly working on the European Union FP7 Marie Curie Training Programme on Tracking in Complex Sensor Systems. He is currently working with The Chinese University of Hong Kong, Shenzhen, and Shenzhen Research Institute of Big Data in June 2016. His research interests include statistical signal processing, machine learning, and sensory data fusion with applications to wireless positioning and tracking. In 2013, he received the Chinese Government Award for outstanding self-financed students abroad. In 2014, he received the MarieCurie Scholarship from European Union.