A Lightweight and Secure Group Key Based Handover Authentication Protocol for the Software-Defined Space Information Network

Kaiping Xue, *Senior Member, IEEE*, Huancheng Zhou, Wei Meng, David S. L. Wei, *Senior Member, IEEE*, and Mohsen Guizani, *Fellow, IEEE*

***Abstract*— With rapid advances in satellite technology, space information network (SIN) has been proposed to meet the increasing demands of ubiquitous mobile communication due to its advantages in providing extensive access services. However, due to satellites' resource constraint and SIN's highly dynamic topology, it poses a challenge on management and resource utilization in the development of SIN. There have been some works integrating the software defined network (SDN) into SIN, defined as software defined space information network (SD-SIN), so as to simplify the management and improve resource utilization in SIN. However, these works ignore the security issue in SD-SIN. Meanwhile, the existing security mechanisms in SDN are still unable to cope with the uniqueness of satellite network, and some other critical security issues still haven't yet been well addressed. In this paper, based on (t, n) secret sharing, an SIN-specific lightweight group key agreement protocol is proposed for SD-SIN to ensure both the security and applicability. Moreover, considering the highly dynamic network topology, we also design a group key-based secure handover authentication scheme to reduce the overhead of handover authentication. Security analysis shows that the handover authentication protocol can resist to various known attacks. In addition, further performance evaluation shows its efficiency in terms of computation and communication overheads. Finally, the simulation results of computing overhead to the network entities demonstrate that our protocol is feasible in practical implementation.**

***Index Terms*— Space information network, software-defined networking, group key agreement, handover authentication.**

Manuscript received May 15, 2019; revised December 6, 2019; accepted February 6, 2020. Date of publication February 28, 2020; date of current version June 10, 2020. This work was supported in part by the National Key Research and Development Program of China under Grant 2016YFB0800301, in part by the Youth Innovation Promotion Association CAS under Grant 2016394, and in part by the National Natural Science Foundation of China under Grant 61671420. The associate editor coordinating the review of this article and approving it for publication was G. C. Alexandropoulos. *(Corresponding author: Kaiping Xue.)*

Kaiping Xue, Huancheng Zhou, and Wei Meng are with the Department of Electronic Engineering and Information Science, University of Science and Technology of China, Hefei 230027, China (e-mail: kpxue@ustc.edu.cn).

David S. L. Wei is with the Computer and Information Science Department, Fordham University, New York, NY 10458 USA.

Mohsen Guizani is with the Department of Computer Science and College of Engineering, Qatar University, Doha 2713, Qatar.

Color versions of one or more of the figures in this article are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TWC.2020.2975781

I. Introduction

With rapid advances in satellite technology, Space Information Network (SIN) is a promising network architecture for providing large-scale coverage as well as high data-rate transmission. Compared with the tradition terrestrial network, SIN can overcome the shortage of geographic limitation and provide more flexible and ubiquitous access services [1]–[3]. However, the security risks in SIN become more serious than those in traditional networks due to its distinctive structural features. Firstly, the highly exposed satellite-ground links and inter-satellite links in SIN make it vulnerable for adversaries to launch various attacks [4]. Secondly, the dynamic network topology makes mobile users hand over frequently during accessto SIN [5]. Finally, the limited computation capacity of entities in SIN makes it difficult to effectively execute highly complex algorithms. Therefore, it is essential to design some efficient security mechanisms to ensure secure communications in the SIN.

Meanwhile, the resource constraint of satellites and SIN's highly dynamic network topology have posed a challenge on the development of SIN. Software defined networking (SDN) technology has been integrated into SIN, e.g., [6]–[9], defined as software defined space information network (SD-SIN), to simplify the management and improve resource utilization in SIN. SDN technology, in which the data plane and control plane are decoupled, enables a network to be programmable and in turn simplifies the network management [10]. It has thus been attracting the attention of researchers and practitioners from academia and industry, respectively. The separation of control plane from data plane in SDN enables it to simplify network operations, which makes the implementation of new protocols and functions easier. Meanwhile, it enables the control of network flows to be elastic, and is thus able to monitor network status more easily. Therefore, there are increasing interests in deploying SDN switches in traditional or emerging networks [11]–[13]. By adopting the SDN technology in SIN, low orbit satellites in SIN act as SDN switches, and they just need to follow data forwarding instructions issued from a logically centralized controller. This way, it can greatly reduce hardware costs, and lower computation and signaling interaction overheads. According to the strategy of network

1536-1276 © 2020 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission.
See https://www.ieee.org/publications/rights/index.html for more information.

Authorized licensed use limited to: University of Science & Technology of China. Downloaded on June 13,2020 at 04:55:55 UTC from IEEE Xplore. Restrictions apply.

management center, the controller can dynamically adjust network resources to improve the flexibility of resource utilization and service.

Although SDN technology with the centralized control mechanism and the open programming interface enhance the flexibility of management and operation in SIN, it also provides various opportunities for attackers, which make SD-SIN security protection much more challenging. In SDN, whether and when an information flow goes through a security device are determined by the flow rules issued by the controller. If an attacker can forge flow rules set by the controller, he/she will be able to control the path of network traffic and bypass various security devices deployed in SDN. Therefore, the *key agreement* technology is essential for SDN to establish secure channels between the controller and switches to protect information flows in software defined space information network (SD-SIN). It is not hard to see that key agreement is also a significant technology to guarantee the confidentiality in the broadcast communication of SIN. However, the existing security mechanisms in SDN, e.g., SSL, IPSec, are unable to cope with the uniqueness of satellite network, especially when the key management problem is involved. Meanwhile, some other critical security issues still haven't yet been well addressed. For example, due to the ever-changing network topology and intermittent physical link, satellite nodes have to reestablish secure channel with each other frequently, resulting in intolerably heavy handover overhead. Actually, entities in SD-SIN can be divided into different categories so as to complete the specific tasks according to their respective functions, missions, and so on [14], [15]. For ensuring the confidentiality in the group communication, group key agreement (GKA) protocols for SIN, used to establish a consistent group session key within a group, should also be well studied. The established group key can be used to protect the signaling messages and data transmission within the group, thus ensuring the confidentiality of information flows in SD-SIN. However, the features of a dynamic topology and the increasing number of satellite nodes in SIN pose a lot of challenges in designing GKA schemes. Most of the existing GKA protocols for traditional wireless networks, e.g., [16]–[20], are not suitable for SD-SIN, and some GKA protocols proposed for SIN, [21]–[24], have been designed to be implemented in the application layers without taking the topological features of satellite networks into consideration. Meanwhile, the existing handover authentication schemes proposed for traditional networks cannot be directly used in SIN, as there is a great difference in structure between SINs and other traditional wireless networks.

The handover mechanisms (e.g., spotbeam handover, inter-satellite links handover) in SIN have been surveyed extensively in literatures [8], [25]. Moreover, some literatures, e.g., [8], have introduced SDN into SIN to realize seamless handover to improve the overall quality of service (QoS). However, the security issues during the handover process have not received much attention so far. The handover authentication is still a fundamental security mechanism to provide seamless and secure access service for mobiles users in SIN. Although there have been quite a few handover authentication protocols for the traditional wireless networks, they are unable to work well in SIN networks due to the characteristics of long time delay for terrestrial transmission, highly dynamic of links, frequent handover, etc. Therefore, it is very essential to design an efficient and secure handover authentication scheme for SIN.

In this paper, to address the above mentioned challenges for the SD-SIN scenario, we present a lightweight group key agreement protocol based on the secret sharing technology, which is applicable to SD-SIN by taking the advantage of SDN. Meanwhile, the negotiated group key can also be used to protect signaling interactions in SD-SIN. The proposed group key agreement protocol is completed with the assistance of the controller in Geosynchronous Earth Orbit (GEO) satellites to implement the negotiation of the group key. Then, we design an SDN-enabled handover authentication based on the group key shared between the satellites to provide access services to reduce the redundant authentication process implemented across different satellites. Our contributions can be summarized as follows:

- We propose a secure SD-SIN architecture, in which a lightweight SIN-specific group key agreement protocol based on the secret sharing technology is proposed to ensure both of the security and applicability.
- Considering the highly dynamic network topology in SD-SIN, we design a group key-based secure handover authentication scheme to reduce the overhead of handover authentication.
- We formally analyze the security strength and conduct experiments by means of algorithm implementation and network analysis. The results show the superiority of our scheme in security and efficiency to the existing works.

The rest of this paper is organized as follows. In Section II, the related work is discussed. We introduce the system model, security assumption, design goals, and the overview of our scheme in Section III. In Section IV and Section V, we respectively describe the proposed group key agreement protocol and handover authentication protocol in details. Then, security evaluation and performance analysis are presented in Section VI and Section VII, respectively. Finally, the paper is concluded in Section VIII.

II. Related Work

A. The Group Key Agreement Protocol

In group broadcast communication, group key agreement protocol (GKA) has a wide range of applications. GKA guarantees secure communication between group members. The traditional GKA let all group members negotiate a symmetric group key together and then use the key to encrypt and decrypt messages sent among the group members. In recent years, some protocols have been proposed to establish a group key for the group communication in different network scenarios. These protocols can be classified into two categories: 1) ***Centralized GKA***: A group key generation center is introduced to manage the entire group, distribute group keys and implement key updating; 2) ***Distributed GKA***: Each group member can contribute to key generation and distribution without the involvement of a group key generation center.

Authorized licensed use limited to: University of Science & Technology of China. Downloaded on June 13,2020 at 04:55:55 UTC from IEEE Xplore. Restrictions apply.

Many distributed GKA schemes, e.g., [26], are introduced to different network environments and they are able to remove the single point bottleneck, but they are not suitable for the network scenarios where the communication capacity is limited. Meanwhile, in distributed GKA schemes, the overall overhead of the system is much heavier, and moreover the design and operation of the scheme depend on the topology of the specific network. In comparison, centralized GKA protocols are more widely used in various wireless network scenarios [16], [19], [20], where the computational complexity and communication overhead introduced by key management is lower from the perspective of the group participants. However, the centralized key management center usually has much heavier computational complexity and communication overhead. To be noted, most of the existing GKA protocols, e.g., [16]–[20], that are suitable for various traditional wireless network scenarios, are unable to work well in SD-SIN due to its specific characteristics, including limited resources, existence of long delay links, and dynamic network topologies.

In recent years, a few GKA schemes for satellite networks have been proposed [21]–[24]. For satellite multicast, Howarth *et al.* [21] straightly introduced the existing logical-key-hierarchy (LKH) based GKA, where end users are placed in one branch of the LKH tree, and the satellite terminals or gateways are located in another branch. In this scheme, satellites are transparent relays at the physical communications level and do not participate in the group key agreement process. Wang *et al.* [22] proposed an identity-based GKA protocol for SIN, which supports members' dynamic joining and leaving, but it introduces some expensive operations, e.g., bilinear pairing operations, to the cluster head. The schemes in literatures [23], [24] belong to distributed GKA schemes with the hierarchical characteristic, both of which haven't considered the topological details of SIN. In addition, in [23], group members are primarily ground gateways and users. In summary, the issues considered in these schemes are quite different from those considered in our work.

In SD-SIN, high-orbit satellites act as SDN controller nodes, while low-orbit satellites act as SDN switch nodes. Therefore, one high-orbit satellite together with some low-orbit satellites can form a communication group. Aiming at this group communication and jointly considering the characteristics of network topology in SD-SIN, it is necessary to propose a more suitable and efficient group key scheme. In a group, both the control messages on the control plane and transmitted data on the data plane can be protected by the group key and its subsequent derivations. As far as we know, there is still no effective and efficient GKA scheme proposed for SD-SIN.

B. Handover Authentication in Mobile Networks and SIN

Handover authentication is always an important issue of mobile communication networks, which ensures mobile users to seamlessly and securely hand over across multiple access points. In 5G standardization, the mechanism design of handover authentication is still in the process of protocol standardization [27], [28]. Recently, in academia, many handover authentication protocols by adopting different techniques have been proposed for different mobile/wireless network environments.

Choi *et al.* [29] proposed an hash chain based handover authentication scheme. However, the scheme requires a certain amount of storage overhead, and it's hard to synchronize hash values between the two ends of conducting mutual authentication. For the machine-type communication scenario mentioned in the 3GPP standard, Lai *et al.* [30] proposed a 3GPP to Wimax network roaming scheme, including handover authentication and security channel establishment. Considering handover between different types of access points on LTE network, Cao *et al.* [31] proposed a lightweight handover authentication scheme based on context transfer between MMEs (Mobility Management Entity). He *et al.* [32] proposed a lightweight handover authentication scheme, which mainly utilized hash operations, and meanwhile minimize modular exponentiation and pairing operations, so as to improve its security and efficiency simultaneously. In the 3GPP standard [28], [33], relevant handover authentication protocol has been given to ensure the quality of network communication, but it implements the similar procedure as the initial access authentication.

However, these schemes, suitable in traditional wireless networks, cannot be directly used in SIN, as there is a great difference between SINs and other traditional wireless networks [4]. Therefore, it is a focused research topic to design security protection mechanisms suitable for the unique characteristics of SIN. In order to guarantee communication continuity in SIN, many handover algorithms are proposed. However, the security issues during the handover procedure still have not yet received sufficient attentions. These schemes mainly focus on handover efficiency, aiming at realizing fast handover in the high-rate SIN environment with lossy links. In terms of security, they often adopt the same scheme as the initial access authentication scheme, or use some lightweight but weakened security mechanisms. These operations give attackers more opportunities to further exploit security threats existing in these schemes to illegally access the network and even destroy the availability of the entire network.

In order to improve the efficiency of handover authentication and ensure that the re-established link after handover is also secure, some new handover protocols, e.g., [34], [35], have been proposed based on some cryptographic algorithms. But there are too many interactions between the involved nodes in these protocols and the participation of the authentication server is often required. If these schemes are applied to SIN, users' communication continuity will be greatly affected. Although our previous works [34], [35] provide solutions to implement handover authentication with different security features, respectively, they are still not efficient enough and not very general. The handover authentication in [34] requires the current attached satellite to send the access control list, which contains the identification of all legal accessed users currently attached within it, to the subsequent attached satellite. When the number of users in the domain is drastically increased, the transmission of the list will consume too much inter-satellite link bandwidth, and the lookup operation in the list will also reduce the efficiency of handover. In another

Authorized licensed use limited to: University of Science & Technology of China. Downloaded on June 13,2020 at 04:55:55 UTC from IEEE Xplore. Restrictions apply.

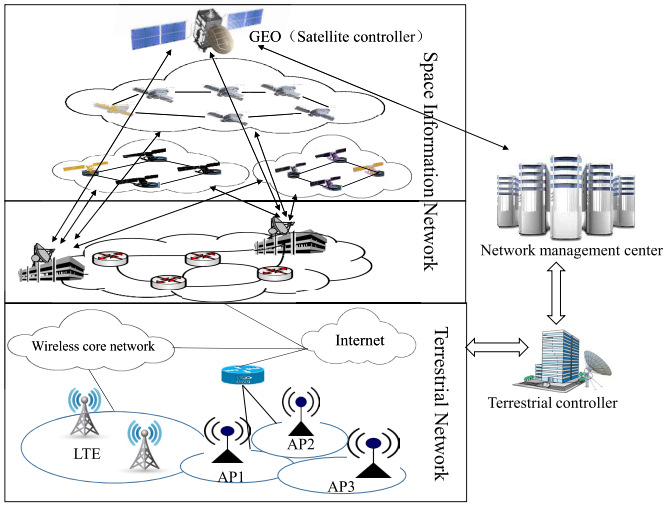


Fig. 1. System model.

work [35], each time when users hand over to a new satellite, the access authentication process needs to be re-executed, which brings large computational overhead to the hardware-constrained satellites. Meanwhile, Yang *et al.* [36] further proposed a group signature based scheme for SIN, but group signature introduces considerable computational complexity. Moreover, the group signature technology requires the update of signing key or public key once revocation occurs, which will also bring in unnecessary implementation delay. To be noted, there is no secure seamless handover scheme introduced in [36], which is mainly for access authentication in cross-domain roaming scenarios. Therefore, for the secure communication in satellite network environment, it is in a desperate need to design a secure and lightweight handover authentication scheme. In this paper, the proposed GKA mechanism actually provides a secure and trusted environment among low orbit satellite nodes. The existence of shared group keys provides a good opportunity for designing an efficient handover authentication scheme.

III. System Model, Security Assumption, Design Goals and Overview of Our Scheme

A. System Model

As shown in Fig. 1, a general SD-SIN architecture consists of space information network, terrestrial network, and some extra specific servers. The space information network (SIN) is a heterogeneous one with satellite network as the backbone, and consists of a variety of satellites and spacecrafts in general. SIN is deployed with spacecrafts at different orbits, ground stations, and mobile terminals provided with the satellite communication capability [37]. The terrestrial network is mainly composed of the traditional wireless networks deployed on the ground, such as LTE-A networks, WiFi, and so on [38]. As shown in Fig. 1, the differences between SIN and SD-SIN include the replacement of the service router with the SDN switch and the requirement for a logical control channel [6].

From the aspect of SDN technology, in SD-SIN, there are mainly three types of entities, including SD-SIN switch, SD-SIN controller, and network management center (NMC). NMC serves as the orchestrator of the whole SD-SIN, including both space information networks and terrestrial networks. The functions of NMC mainly include resource registration and inquiry and devising some strategies (e.g., routing, security, and accounting) [39]. The Geosynchronous Earth Orbit (GEO) satellites acts as controllers of space information network, which is responsible for collecting link status among satellites and forwarding instructions from NMC to satellites. Meanwhile, GEO can also predict satellite trajectories. With no less than three GEOs, the service of SD-SIN could cover the entire globe. Terrestrial controller is deployed on the ground, and the function of which includes maintaining the local service information (e.g., service type and location) in the database and distributing the instructions from NMC to switches via the secure link between controllers and NMC. Low orbit satellites with limited computational ability play a role of SDN switches. It is worth noting that in addition to data forwarding, they are only allowed to support simple verification operations, such as implementation of symmetric cipher algorithm and one-way hash, as performing complex cryptographic operations introduce significant delays. In addition, we assume that these LEO satellites have a moderate storage capacity just like traditional network routers and a small trust zone, e.g., a secure digital memory card, to store some secure values. With this architecture, user's track can be easily predicted, which will facilitate the implementation of handover authentication scheme.

B. Security Assumption

We assume that the network management center (NMC) cannot be compromised by any adversary, and thus can be completely trusted for all entities in our system. LEO satellites in the system can be impersonated by other malicious adversaries, and then they will deceive other LEO satellites to provide access services for illegal users. As the satellite controller in SIN, GEO satellites can be considered to be fully trusted, and it will honestly forward signaling messages between other satellite nodes and NMC. As each GEO satellite is static related to the NMC, it is easy to pre-establish the secure channel by traditional secure protocols based on pre-shared key, e.g., using the Third Generation Partnership Project Authentication and Key Agreement (3GPP-AKA). Thereafter, each GEO can establish a secure channel by key agreement algorithm with other GEOs with the help of NMC. In addition, we assume that the adversary has the ability to modify, inject or interrupt the interaction messages over the air, and tries to corrupt the proposed scheme. Moreover, all satellite nodes may suffer from virus attacks, even being hijacked.

C. Design Goals

In this paper, we propose a secure SD-SIN architecture, in which a SIN-specific lightweight group key agreement protocol based on (t, n) secret sharing is proposed to ensure both of the security and applicability. Moreover, considering the highly dynamic network topology in SD-SIN, we design

Authorized licensed use limited to: University of Science & Technology of China. Downloaded on June 13,2020 at 04:55:55 UTC from IEEE Xplore. Restrictions apply.

a group key-based secure handover authentication scheme to reduce the overhead of handover authentication. In view of the inherent characteristics of SIN, it's necessary to find a compromise state between security and availability. In general, in addition to providing the basic functions of SDN, a well-designed security protection scheme for SD-SIN should satisfy the following properties:

- ***Applicability and Efficiency:*** The proposed scheme must be suitable to SD-SIN and achieve a high efficiency in terms of computation and communication complexity, especially for the access to satellites. The access to satellites is usually resource-constraints, which cannot support the implemention of complex operations.
- ***Integrity and Confidentiality:*** Since the controller in SD-SIN can control the whole network, the proposed scheme should prevent control signaling from being forged. Besides, sensitive data in SD-SIN should also be protected from disclosure to any other parties. Therefore, low orbit satellites must establish secure channels with each other when having communication needs between them. So do between low orbit satellites and high orbit satellites.
- ***Low Overhead of Secure Channel Reconstruction:*** The low orbit satellite network is highly dynamic, and the movement of satellites in low earth orbit is so fast that most satellites have to reestablish secure channels with each other frequently, which brings in heavy handover overhead in SD-SIN. In addition to reducing the overhead of link reconstruction by means of the specific communication and network technologies, the proposed security scheme should consider the special features of SD-SIN and reduce the handover overhead to reduce the secure channel reconstruction overhead.

D. Overview of Our Scheme

The overview of the group key agreement and handover authentication scheme is shown in Fig. 2. The satellites of the same group at lower orbit, e.g., Low Earth Orbit (LEO) satellites, can negotiate a shared group key with the assistance of the satellites at higher orbit, i.e., GEO satellites. In order to protect the confidentiality of messages transmitted between satellites and group manager (GM) integrated in the network management center, we assume that each satellite shares a key with the GM. Each group member first sends a random selected point with a pair of values to the GEO satellite connecting with it. Then, each GEO satellite forwards its collected points to the GM in a secure manner. Upon receiving these n points, GM first chooses a group key GK and lets $f(0) = GK$. Then, GM constructs an interpolated polynomial $f(x)$ with degree N. Finally, GM regenerates n points on the polynomial $f(x)$ and returns them to each group member. Subsequently, these group members can recover the polynomial to share the group key GK.

The handover authentication protocol, as an important technology in mobile networking, makes mobile users able to securely and seamlessly roam across different access points. The handover scenario we will introduce is shown in Fig. 2, where a mobile user accesses LEO_2 to obtain network service

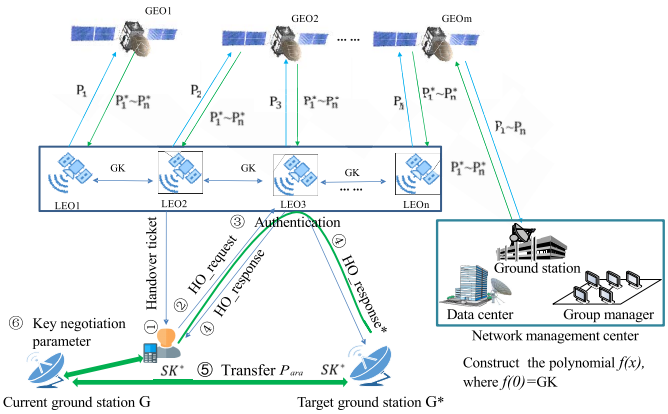


Fig. 2. Overview of the proposed scheme.

and LEO_2 will generate the handover ticket for this user by using group key GK. When the user is handing over from the current satellite LEO_2 to the target satellite LEO_3, the user first needs to send a handover request to LEO_3. Then, after the authentication is successful verified, the mobile user is allowed to access target satellite LEO_3. Moreover, there is another handover scenario where mobile users hand over between two ground stations. In this scenario, the session key must be changed to provide secure communication with forward security and backward security. With the help of LEO_2 and the old ground station G, a new session key SK^* will be established between the mobile user and the target ground station G^*.

IV. The Group Key Agreement Scheme

The group key agreement protocol needs the involvement of three entities: LEO satellites, GEO satellites, and GM. GM is the trust party integrated in NCC. GEO satellites are assistants for the communication between LEO satellites and GM. A LEO satellite is a group member (Leo_i) with constrained compute resource. The protocol is implemented to achieve group key agreement by using the secret sharing technology [40]. Our proposed group key agreement protocol consists of system initial phase and group key agreement phase.

A. System Initial Phase

In this phase, each LEO satellite (Leo_i) that has been authorized by the network management cente shares a secret value (x_i, y_i) with the network management center that acts as the group manager during the group key agreement process. From a security perspective, these secret values will be stored in trusted hardware configured in the satellite where the data stored is unreadable to adversaries.

B. Group Key Agreement Phase

The group key will be shared between GM and the group members in this phase. The process is described as follows:

Authorized licensed use limited to: University of Science & Technology of China. Downloaded on June 13,2020 at 04:55:55 UTC from IEEE Xplore. Restrictions apply.

1) Each group member Leo_i firstly generates the random challenge value R_i and the timestamp ts_i, and then enters them into the trusted hardware configured in the satellite. The trusted hardware module computes $h(x_i, ID_{Leo_i}, R_i, ts_i)$, where $h()$ is the hash function, and outputs it to Leo_i. Finally, Leo_i sends the group key agreement request message $GKA^i_{req} = \{h_i = h(x_i, ID_{Leo_i}, R_i, ts_i), ID_{Leo_i}, R_i, ts_i\}$ to network management center on the ground by using GEO satellite as the forwarding node.
2) Upon receiving the group key agreement request message $GKA^i_{req}(1 \leq i \leq N)$, GM first performs data source authentication and data integrity verification by checking whether the received h_i is equal to $h^*(x_i, ID_{Leo_i}, R_i, ts_i)$ calculated from the locally stored x_i and the received parameters $\{ID_{Leo_i}, R_i, ts_i\}$. Then, GM computes the point $(x_i, y_i + R_i)$ for Leo_i who have been successfully authenticated. For the convenience of description, we assume that all n LEO satellites have been successfully authenticated, thus obtaining n points $(x_i, y_i + R_i)_{(1 \leq i \leq N)}$. Then GM randomly chooses a group key GK, and constructs an interpolated polynomial $f(x)$ with degree N to pass through $(N + 1)$ points, $(0, GK)$, and $(x_i, y_i + R_i)$ for $i = 1, 2, \ldots, N$. Next, the GM reselects N additional points P^*_i on $f(x)$ for N members, Leo_i $(1 \leq i \leq N)$, and computes $Auth_i = h(GK, ID_{Leo_i}, R_i, P^*_1, \ldots, P^*_N)$. Finally, GM broadcasts the key agreement response message $\{Auth_i, ID_{Leo_i}, P^*_1, \ldots, P^*_N\}_{(1 \leq i \leq N)}$ to all group members.
3) Upon receiving the response message, each group member Leo_i firstly computes the point $(x_i, y_i + R_i)$ through the trusted hardware module. Subsequently, Leo_i can recover the polynomial $f(x)$ from point $(x_i, y_i + R_i)$ and other n received points $\{P^*_1, \ldots, P^*_N\}$, thus retrieving the group key $GK = f(0)$. Then, Leo_i computes $Auth^*_i = h(GK, ID_{Leo_i}, R_i, P^*_1, \ldots, P^*_N)$ and checks whether this hash value is identical to the received $Auth_i$. If these two values are identical, Leo_i believes that this group key is valid and accepts it; otherwise, Leo_i stops the group key agreement protocol.

After the group key agreement procedure is completed, the n group members will use key GK as their shared group key. Thus, they can use this GK to protect data confidentiality in subsequent group communications.

V. Handover Authentication Based on the Shared Group Key

In SIN, satellites move with a higher speed relative to mobile users in terrestrial networks, which results in a high dynamic feature of the network topology. This dynamic topological feature poses a major challenge on the continuous and secure communication of end users. Therefore, it is essential to provide a secure and efficient seamless handover scheme to provide satisfactory quality of service (QoS) for some services while keeping security protection, especially, for the real-time ones.

A. Initial Authentication Phase

In this phase, user U implements the initial authentication process before he/she starts to access SD-SIN and obtains a handover ticket from the satellite. For satisfying high security and performance requirements, the user can implement the low-latency authentication scheme proposed in [35] to achieve the initial authentication between the user and the satellite/ground station. For simplicity, it is assumed that the authentication scheme proposed in [35] has been implemented in the initial authentication process. After the mutual authentication is completed, user U can share secret keys K_{US} and SK with the satellite and the ground station, respectively. In addition, the satellite currently providing access services issues handover tickets for all users connected to it. The details are described as follows. Let CS be the current satellite access point and NS be the new satellite access point. The current satellite access point CS first generates a temporary group key TGK by computing $TGK = KDF(GK)$, where KDF represents a key derivation function, which is a one-way function. Then, CS computes a handover ticket HT_U according to Eq. (1) for U and sends HT_U encrypted by using key K_{US}.

$$HT_U = ENC_{TGK}(ID_U, K_{US}, T_{exp}), \tag{1}$$

where ENC is a symmetric encryption algorithm and T_{exp} is the expiration time of HT_U. Finally, U stores the received HT_U for achieving secure and seamless handover in the subsequent communication.

B. Handover Authentication Phase

In this phase, the user and the target satellite (NS) accomplish the handover authentication process and negotiate a session key between them when the user moves away from the CS to the NS. The procedure is described in details as follows:

1) U first chooses a random number R_U and generates $MAC^1_U = H(K_{US}, ID_U, R_U, HT_U, ts_1)$, where ts_1 is a timestamp used to resist replay attacks. Then, U sends handover request message $HO_{req} = \{ID_U, ID_{NS}, R_U, HT_U, ts_1, MAC^1_U\}$ to NS, the target satellite access point.
2) Upon receiving the handover request message HO_{req}, the NS first checks whether the timestamp ts_1 is within the allowable time range compared with the current time. If it is right, the NS computes a temporary group key $TGK = KDF(GK)$ to decrypt the receiving HT_U to obtain K_{US} and T_{exp}. If T_{exp} is valid, the NS utilizes K_{US} to verify the correctness of MAC^1_U. If MAC^1_U is not correct, the NS rejects the handover request; otherwise, the NS trusts that the received MAC^1_U is from the legal user. Then, it chooses a random number R_{NS} and computes $MAC_{NS} = H(K_{US}, ID_{NS}, R_{NS}, ts_2)$, and sends the handover response message $HO^1_{res} = \{ID_U, ID_{NS}, R_{NS}, ts_2, MAC_{NS},$ "satellite handoff"$\}$ or $HO^2_{res} = \{ID_U, ID_{NS}, R_{NS}, ts_2, MAC_{NS},$ "ground station handoff"$\}$ to the user. Subsequently, the NS computes the new secret key

$$K_{US_{new}} = KDF(K_{US}, ID_U, ID_{NS}, R_{NS}, R_U).$$

Authorized licensed use limited to: University of Science & Technology of China. Downloaded on June 13,2020 at 04:55:55 UTC from IEEE Xplore. Restrictions apply.

3) Upon receiving the handover response message, the user first determines whether the HO^1_{res} or HO^2_{res} is received. (1) If message HO^1_{res} is received, it represents that the handover has happened between the satellite access point, and the ground station unchanged. Then, the user performs the following operations: he/she verifies the validity of timestamp ts_2 and the correctness of MAC_{NS}. If they are valid, the user computes secret key $K_{US_{new}} = KDF(K_{US}, ID_U, ID_{NS}, R_{NS}, R_U)$ and sends the handover confirmation message $HO_{cof} = \{MAC^2_U\}$, where $MAC^2_U = H(K_{US_{new}}, ID_U, ID_{NS}, R_{NS}, ts_3)$. Upon the receipt of the handover confirmation message, NS confirms MAC^2_U to complete and end the handover protocol. Thus, a new secret key $K_{US_{new}}$ can be shared between the user and the NS.
(2) If message HO^2_{res} is received, it represents the handover has happened between ground stations (between the current ground station CG and the new ground station NG). After $K_{US_{new}}$ is shared between the user and the NS as described above in (1), the following steps still need to be performed: (a) NS sends the handover request message $HO^*_{req} = \{ID_U, ID_{NG}, ID_{NS}\}$ to the new ground station ID_{NG}; (b) Upon receiving HO^*_{req}, the NG sends the authentication request message to the CG to request the user context; (c) On the receipt of the message, the current ground station CG sends the authentication response message including the user context, which consists of user's key negotiation parameters and other relevant parameters, to NG; (d) The CG forwards the key negotiation parameters to the user via the secure channel. Subsequently, the user can generate the new session key SK^*.

Finally, after the handover authentication procedure is completed, legitimate users will be allowed to switch to new satellite/ground station. Meanwhile, the keys shared between the user and the new satellite/ground station are renegotiated.

VI. Security Evaluation

In this section, we first show that the proposed handover authentication scheme can achieve mutual authentication, key agreement, and resistance of several typical attacks. Then, we apply BAN Logic [41] to prove the correctness of the handover authentication protocol.

A. Security Analysis

1) Mutual Authentication: The proposed handover authentication scheme can achieve the mutual authentication between user U and the target satellite access point NS. In our proposed scheme, only the legitimate user can access to the SIN via NS. The NS authenticates U by checking the received $MAC^1_U = H(K_{US}, ID_U, R_U, HT_U, ts_1)$, where $K_{US} = DEC_{TGK}(HT_U)$. Only the legitimate user knows the secret key K_{US} and thus can generate the legal $MAC^1_U = H(K_{US}, ID_U, R_U, HT_U, ts_1)$. Besides, U verifies the NS by checking if the received $MAC_{NS} = H(K_{US}, ID_{NS}, R_{NS}, ts_2)$ because only the legitimate NS can derive the temporary group key TGK and then decrypt HT_U to obtain the secret key K_{US}. Therefore, the mutual authentication between the user and the target satellite can be accomplished.

2) Key Agreement: In the proposed handover authentication scheme, user U negotiates a session key $K_{US_{new}}$ with the target satellite access point NS, which is derived from the secret key K_{US} and the random number R_U and R_{NS} dynamically generated by U and NS, respectively. Only the legitimate user knows the correct key K_{US} and only the legitimate NS can derive the temporary group key TGK and then extract the secret key K_{US} by decrypting HT_U. In addition, in the handover scenario where the user hands over between ground stations, the secret session key SK^* can be negotiated between the user and the target ground station. Furthermore, any adversaries cannot obtain keying materials because the handover session key is not transmitted over any links and is computed on each side independently.

3) Resistance of Eavesdropping Attack: The secret key K_{US} is encrypted and encapsulated in HT_U by NS by using the temporary group key TGK. Even if an adversary could intercept HT_U through eavesdropping attack, he/she cannot obtain the secret key K_{US} because TGK is unknown. Besides, the keys used to protect the sensitive data are not transmitted over communication links. Therefore, our scheme can prevent adversaries from launching the eavesdropping attack to obtain the sensitive information.

4) Resistance of Replay Attack: An adversary always tries to intercept messages and further replay them. However, he/she still cannot be authenticated successfully when the timestamp value in the reply message is checked as invalid. Moreover, the timestamp value cannot be modified and replaced because they are hashed to get the message authentication code MAC_U and MAC_{NS}, respectively. Thus, the replaying message can be easily detected by checking the validation of the timestamp and message authentication code.

5) Resistance of Man-in-the-Middle (MitM) Attack: A MitM attacker cannot derive the new session key $K_{US_{new}}$ by eavesdropping the public parameters from the wireless communication channel since $K_{US_{new}}$ is derived based on the secret values K_{US} after successful mutual authentication. Therefore, it is infeasible for an adversary to launch MitM attack to invade the existing connection. Furthermore, it is infeasible for the attacker to create a correct message authentication code without the secret key K_U. Thus, no one can impersonate the legitimate NS or the legitimate U.

B. Authentication Proof Based on BAN Logic

The BAN logic [41] is a formal model widely used to analyze the security of authentication schemes. In this subsection, using the BAN logic, we provide an authentication proof, and demonstrate how the proposed handover authentication achieves the security goals. Some notations and logical postulates used in the BAN logic analysis are described in TABLE I.

Authorized licensed use limited to: University of Science & Technology of China. Downloaded on June 13,2020 at 04:55:55 UTC from IEEE Xplore. Restrictions apply.

TABLE I
NOTATIONS AND LOGICAL POSTULATES IN BAN LOGIC

Notations	Description
$P \mid\equiv X$	Principal P believes statement X
$P \lhd X$	P sees the statement X
$\sharp X$	The formula X is fresh
$P \mid\sim X$	P once said X
$P \mid\Rightarrow X$	P has jurisdiction over statement X
(X, Y)	Formula X or Y is one part of formula (X, Y)
$\{X\}_K$	Formula X is encrypted with key K
$P \overset{K}{\longleftrightarrow} Q$	P and Q use the shared key K to communicate

The rules introduced below describe the main logical postulates of the BAN logic.

According to the analytic procedures of the BAN logic, our proposed protocol should satisfy the following security goals:

G1. $NS \mid\equiv U \overset{K_{US}}{\longleftrightarrow} NS$

G2. $NS \mid\equiv U \mid\equiv U \overset{K_{US_{new}}}{\longleftrightarrow} NS$

To facilitate the derivation, we first transfer the communication message of our proposed handover authentication scheme into idealized form as follows.

Message 1: $U \rightarrow NS$: Handover request message

$$NS \lhd \Big\{ ID_U, ID_{NS}, R_U, ts_1, \big\{ ID_U, U \overset{K_{US}}{\longleftrightarrow} NS, T_{exp} \big\}_{TGK}, \big\{ ID_U, R_U, ts_1, \{ ID_U, U \overset{K_{US}}{\longleftrightarrow} NS, T_{exp} \}_{TGK} \big\}_{K_{US}} \Big\}.$$

Message 2: $NS \rightarrow U$: Handover response message

$$U \lhd \big\{ ID_U, ID_{NS}, R_{NS}, ts_2, \{ ID_{NS}, R_{NS}, ts_2, U \overset{K_{US_{new}}}{\longleftrightarrow} NS \}_{K_{US}} \big\}.$$

Message 3: $U \rightarrow NS$: Handover confirm message

$$NS \lhd \{ ID_{NS}, R_{NS}, ts_3, U \overset{K_{US_{new}}}{\longleftrightarrow} NS \}_{K_{US_{new}}}.$$

The initial assumptions ensure that the logical analysis of the proposed solution can be successfully conducted. Therefore, in order to analyze the proposed scheme, we make the following assumptions about the initial state of the scheme.

A1. $U \mid\equiv U \overset{K_{US}}{\longleftrightarrow} NS$
A2. $U \mid\equiv CS \overset{GK}{\longleftrightarrow} NS$
A3. $NS \mid\equiv CS \overset{GK}{\longleftrightarrow} NS$
A4. $NS \mid\equiv \sharp(T_{exp})$
A5. $NS \mid\equiv (U/CS \mid\Rightarrow U \overset{K_{US}}{\longleftrightarrow} NS)$
A6. $U \mid\equiv \sharp(ts_2)$
A7. $NS \mid\equiv \sharp(ts_1)$
A8. $NS \mid\equiv \sharp(ts_3)$
A9. $U \mid\equiv \sharp(R_U)$
A10. $NS \mid\equiv \sharp(R_{NS})$

Finally, based on the idealized form of the messages and assumptions, we analyze the idealized form of the proposed scheme and provide the main procedures of proof as follows.

According to Message 1 and assumption A3, we apply the message-meaning rule $\frac{P \mid\equiv P \overset{K}{\longleftrightarrow} Q, P \lhd \{X\}_K}{P \mid\equiv Q \mid\sim X}$ to obtain

S1. $NS \mid\equiv U/CS \mid\sim \{ID_U, R_U, ts_1, ID_U, U \overset{K_{US}}{\longleftrightarrow} NS, T_{exp}\}$

According to S1 and assumptions A4 and A7, we apply the nonce-verification rule $\frac{P \mid\equiv \sharp(X), P \mid\equiv Q \mid\sim X}{P \mid\equiv Q \mid\equiv X}$ to obtain

S2. $NS \mid\equiv U \mid\equiv U \overset{K_{US}}{\longleftrightarrow} NS$

According to S2 and assumption A5, we apply the jurisdiction rule $\frac{P \mid\equiv (Q \mid\Rightarrow X), P \mid\equiv (Q \mid\equiv X)}{P \mid\equiv X}$ to obtain

S3. $NS \mid\equiv U \overset{K_{US}}{\longleftrightarrow} NS$

According to Message 2 and assumption A1, we apply the message-meaning rule $\frac{P \mid\equiv P \overset{K}{\longleftrightarrow} Q, P \lhd \{X\}_K}{P \mid\equiv Q \mid\sim X}$ to obtain

S4. $U \mid\equiv NS \mid\sim \{ID_{NS}, R_{NS}, ts_2, U \overset{K_{US}}{\longleftrightarrow} NS\}$

According to S4 and assumptions A6 and A9, we apply the nonce-verification rule $\frac{P \mid\equiv \sharp(X), P \mid\equiv Q \mid\sim X}{P \mid\equiv Q \mid\equiv X}$ to obtain

S5. $U \mid\equiv NS \mid\equiv U \overset{K_{US}}{\longleftrightarrow} NS$

According to Message 3 and S3, we apply the message-meaning rule $\frac{P \mid\equiv P \overset{K}{\longleftrightarrow} Q, P \lhd \{X\}_K}{P \mid\equiv Q \mid\sim X}$ to obtain

S6. $NS \mid\equiv U \mid\sim \{ID_{NS}, R_{NS}, ts_3, U \overset{K_{US_{new}}}{\longleftrightarrow} NS\}$

According to S6 and assumptions A8 and A10, we apply the nonce-verification rule $\frac{P \mid\equiv \sharp(X), P \mid\equiv Q \mid\sim X}{P \mid\equiv Q \mid\equiv X}$ to obtain

S7. $NS \mid\equiv U \mid\equiv U \overset{K_{US_{new}}}{\longleftrightarrow} NS$

As a result, the above logic proves that the contributed scheme achieves mutual authentication between U and NS.

VII. PERFORMANCE ANALYSIS

In this section, we will compare the proposed handover authentication scheme with existing schemes in terms of computation overhead, communication overhead, security functionality and performance comparison, and algorithm implementation efficiency.

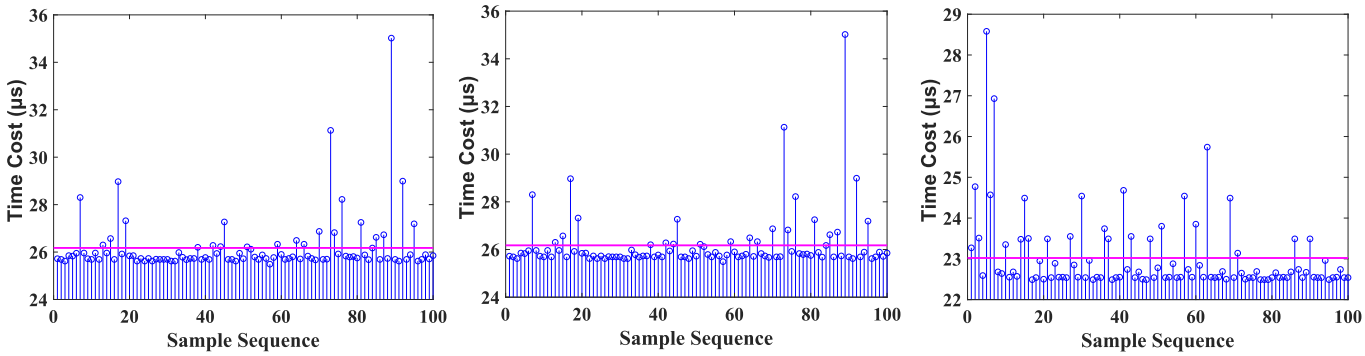
A. Computation Overhead

For the handover authentication overhead, we define it as the time cost of cryptography operations involved in the proposed scheme. We investigated the time costs of the primitive cryptography operations using the OpenSSL library [42] on an Intel P III Mobile 733 MHz processor. Meanwhile, the results in [43] show that the time costs for performing an RSA verification, point multiplication, modular exponentiation, and pairing operation are $T_{RV} = 0.435ms$, $T_{mul} = 1.082ms$, $T_{mexp} = 1.019ms$, and $T_{pair} = 33.584ms$, respectively. Note that the time costs of highly efficient operations (less than $0.001ms$) such as symmetric encryption/decryption operation T_{sy} and one one-way hash function T_h are omitted. TABLE II compares our proposed handover authentication scheme with some existing works, i.e., [29], [31], [32] and [33], in terms of computation complexity with authentication delay. From TABLE II, one can see that the total time required for a successful handover authentication in our work is much less than that of Choi's scheme, Cao's scheme, and He's scheme. This is because the operations adopted by our scheme are highly efficient operations (e.g., hash function), and the operation costs of which are significantly smaller than other

Authorized licensed use limited to: University of Science & Technology of China. Downloaded on June 13,2020 at 04:55:55 UTC from IEEE Xplore. Restrictions apply.

TABLE II
COMPARISON OF COMPUTATION OVERHEAD

	Cost of Initial Phase (ms)	Cost of Authentication (ms)	Total (ms)
Choi's [29]	$6T_{mexp} + 2T_{RV} + 2T_h$	$8T_{mexp} + 2T_{RV} + 6T_h + 8T_{mul} + 4T_{sy}$	$14T_{mexp} + 4T_{RV} + 8T_h + 8T_{mul} + 4T_{sy}$
Lai's [30]	$2T_{pair} + T_{mul}$	$4T_h + 6T_{mul} + 2T_{pair}$	$4T_{pair} + 7T_{mul} + 4T_h$
Cao's [31]	$4T_{mexp} + 2T_{sy}$	$10T_{mexp} + 4T_h + 6T_{mul} + 2T_{sy}$	$14T_{mexp} + 4T_h + 6T_{mul} + 4T_{sy}$
He's [32]	0	$2T_{pair} + 6T_h$	$2T_{pair} + 6T_h$
LTE-A [33]	0	$6T_h$	$6T_h$
Ours	$T_h + T_{sy}$	$6T_h + T_{sy}$	$7T_h + 2T_{sy}$



(a) Current satellite-side execution time (b) New satellite-side execution time (c) User-side execution time

Fig. 3. Time cost for different entities.

TABLE III
PARAMETER SIZE

Parameters	Size (bits)
Identity ($ID_U/ID_S/ID_G$)	128
Pseudo-ID (PID)	256
p/q	1024/160
Key	128
GUTI/TAI/PCI/ECGI/GUMMEI *	128
Hash/MAC	64
Random number (R)	128
ECDH key	192
Timestap (ts)/Expiration time (T_{exp})	17

* GUTI: Globally Unique Temporary ID, TAI: Tracking Area Identity, PCI: Physical Cell Identity, ECGI: E-UTRAN Cell Global Identifier, GUMME: source MME ID

operations (e.g., point multiplication, pairing operation). While LTE-A scheme has an equally low authentication overhead to our scheme, LTE-A scheme is not able to resist various attacks such as eavesdropping attack, replay attack, and MitM attack. Moreover, as what we analyzed in **Communication overhead**, the communication overhead of LTE-A scheme is far higher than that of our scheme.

B. Communication Overhead

For the communication overhead, we mainly evaluate the sizes of authentication messages in our proposed handover authentication scheme compared with some existing schemes. In order to better compare the communication overhead with the existing schemes, we give the relevant parameters used in these schemes in TABLE III. According to the sizes of all the messages, we also give a comparison of the communication overhead of the existing protocols as shown in TABLE IV. We can see that the communication overhead of our scheme is much lower than that in schemes [29]–[31], and [33]. Although the scheme in [32] has a little lower communication overhead than our scheme, its computation overhead is excessively high as shown in **Computation Overhead**.

TABLE IV
COMPARISON OF COMMUNICATION OVERHEAD

Scheme	communication overhead (bits)
Choi's [29]	9045
Lai's [30]	2432
Cao's [31]	6208
He's [32]	1408
LTE-A [33]	2048
Ours	1442

C. Security Functionality and Performance Comparison

Finally, TABLE V shows the security functionality and performance comparison of our proposed scheme and some existing protocols [29]–[31], [33]. It can be seen that our proposed handover authentication scheme has a better performance in security and efficiency compared with the existing protocols.

D. Algorithm Implementation Overhead

We construct experimental environment with Banana Pi R1 with 1.2GHz CPU speed and 1GB RAM using C language with OpenSSL library [42]. We further implement the

Authorized licensed use limited to: University of Science & Technology of China. Downloaded on June 13,2020 at 04:55:55 UTC from IEEE Xplore. Restrictions apply.

TABLE V
COMPARISON OF SECURITY AND PERFORMANCE FEATURES

	Choi's [29]	Lai's [30]	Cao's [31]	He's [32]	LTE-A [33]	Ours
Mutual Authentication	Yes	Yes	Yes	Yes	No	Yes
Resistance of Eavesdropping Attack	No	Yes	Yes	Yes	No	Yes
Resistance of Replay Attack	Yes	Yes	Yes	Yes	No	Yes
Resistance of Man-in-the-Middle (MitM) Attack	Yes	Yes	Yes	Yes	No	Yes
Key derivation	Yes	Yes	Yes	Yes	Yes	Yes
Computational cost	High	High	High	High	Low	Low
Communication overhead	High	Low	High	Low	Low	Low

algorithms executed in the user side, the current satellite side, and the new satellite side, respectively. In the experiment, the symmetric encryption/decryption algorithm used in our protocol adopt the AES algorithm, the key sizes of which is set to 128 bits. To ensure the reliability of the experiment, we repetitively conduct the same experiments 100 times. Meanwhile, in each time, the algorithm in our scheme is run for 100 times, and further get the average time cost of a single algorithm running. Furthermore, we use scatter plots to describe these 100 experimental results. As shown in in Fig. 3, we can obtain three scatter plots for the three algorithms, which are implemented on the user side, the current satellite side, and the new satellite side in our scheme. The current satellite-side and new satellite-side algorithm execution time are about 8.079 μs and 26.035 μs on average, respectively. And the average time of user-side algorithm execution is about 22.987 μs. Therefore, from the experiment results, we can draw a conclusion that our proposed protocol is more efficient in terms of computation and communication costs, which makes it feasible in practical implementations.

VIII. CONCLUSION

The integration of space information network (SIN) and software-defined networking (SDN) has been treated as a promising method to enhance the operation of satellite networks and the development and management of communication services in SIN. Although the study of network architecture of software-defined space information network (SD-SIN) has been brought into research and discussed for years, some security challenges posed on ensuring secure communication for SD-SIN have been overlooked. In order to guarantee the confidentiality of information flow in SD-SIN, a lightweight group key agreement protocol based on the secret sharing technology was presented in this paper, which can establish a secure channel between satellites and between the controller and satellite for protecting the information flow in SD-SIN. Moreover, an efficient and secure handover authentication mechanism was proposed based on the group key shared among the satellites, which satisfies a set of essential security features, while it only needs lower computation cost and less communication overhead compared with the existing schemes.

ACKNOWLEDGMENT

The authors sincerely thank the editor, Dr. George Alexandropoulos, and the anonymous referees for their invaluable suggestions that have led to the present improved version.

REFERENCES

[1] Y. Hu and V. O. K. Li, "Satellite-based Internet: A tutorial," *IEEE Commun. Mag.*, vol. 39, no. 3, pp. 154–162, Mar. 2001.

[2] J. Li, K. Xue, D. S. Wei, J. Liu, and Y. Zhang, "Energy efficiency and traffic offloading optimization in integrated satellite/terrestrial radio access networks," *IEEE Trans. Wireless Commun.*, to be published, doi: 10.1109/TWC.2020.2964236.

[3] J. Li, H. Lu, K. Xue, and Y. Zhang, "Temporal netgrid model-based dynamic routing in large-scale small satellite networks," *IEEE Trans. Veh. Technol.*, vol. 68, no. 6, pp. 6009–6021, Jun. 2019.

[4] G. Zheng, P.-D. Arapoglou, and B. Ottersten, "Physical layer security in multibeam satellite systems," *IEEE Trans. Wireless Commun.*, vol. 11, no. 2, pp. 852–863, Feb. 2012.

[5] J. Li, K. Xue, J. Liu, Y. Zhang, and Y. Fang, "An ICN/SDN-based network architecture and efficient content retrieval for future satellite-terrestrial integrated networks," *IEEE Netw.*, vol. 34, no. 1, pp. 188–195, Jan. 2020.

[6] L. Bertaux *et al.*, "Software defined networking and virtualization for broadband satellite networks," *IEEE Commun. Mag.*, vol. 53, no. 3, pp. 54–60, Mar. 2015.

[7] N. Zhang, S. Zhang, P. Yang, O. Alhussein, W. Zhuang, and X. S. Shen, "Software defined space-air-ground integrated vehicular networks: Challenges and solutions," *IEEE Commun. Mag.*, vol. 55, no. 7, pp. 101–109, 2017.

[8] 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.

[9] Y. Miao, Z. Cheng, W. Li, H. Ma, X. Liu, and Z. Cui, "Software defined integrated satellite-terrestrial network: A survey," in *Proc. Int. Conf. Space Inf. Netw. (SINC)*. Springer, 2016, pp. 16–25.

[10] M. Yu, J. Rexford, M. J. Freedman, and J. Wang, "Scalable flow-based networking with DIFANE," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 40, no. 4, p. 351, Aug. 2010.

[11] M. Al-Fares, S. Radhakrishnan, B. Raghavan, N. Huang, and A. Vahdat, "Hedera: Dynamic flow scheduling for data center networks," in *Proc. 7th USENIX Conf. Netw. Syst. Design Implement. (NSDI)*, 2010.

[12] Z. Han, D. Niyato, W. Saad, T. Başar, and A. Hjørungnes, *Game Theory in Wireless and Communication Networks: Theory, Models, and Applications*. Cambridge, U.K.: Cambridge Univ. Press, 2012.

[13] Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, "A survey on security and privacy issues in Internet-of-Things," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1250–1258, Oct. 2017.

[14] D. Li, J. Liu, and W. Liu, "Secure and anonymous data transmission system for cluster organised space information network," in *Proc. IEEE Int. Conf. Smart Cloud (SmartCloud)*, Nov. 2016, pp. 228–233.

[15] Q.-Y. Yu, W.-X. Meng, M.-C. Yang, L.-M. Zheng, and Z.-Z. Zhang, "Virtual multi-beamforming for distributed satellite clusters in space information networks," *IEEE Wireless Commun.*, vol. 23, no. 1, pp. 95–101, Feb. 2016.

[16] S.-H. Seo, J. Won, S. Sultana, and E. Bertino, "Effective key management in dynamic wireless sensor networks," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 2, pp. 371–383, Feb. 2015.

[17] A. Mehdizadeh, F. Hashim, and M. Othman, "Lightweight decentralized multicast–unicast key management method in wireless IPv6 networks," *J. Netw. Comput. Appl.*, vol. 42, pp. 59–69, Jun. 2014.

[18] T. R. Halford, T. A. Courtade, K. M. Chugg, X. Li, and G. Thatte, "Energy-efficient group key agreement for wireless networks," *IEEE Trans. Wireless Commun.*, vol. 14, no. 10, pp. 5552–5564, Oct. 2015.

Authorized licensed use limited to: University of Science & Technology of China. Downloaded on June 13,2020 at 04:55:55 UTC from IEEE Xplore. Restrictions apply.

[19] E. Klaoudatou, E. Konstantinou, G. Kambourakis, and S. Gritzalis, "A survey on cluster-based group key agreement protocols for WSNs," *IEEE Commun. Surveys Tuts.*, vol. 13, no. 3, pp. 429–442, 3rd Quart., 2011.

[20] T.-F. Lee and M. Chen, "Lightweight identity-based group key agreements using extended chaotic maps for wireless sensor networks," *IEEE Sensors J.*, vol. 19, no. 22, pp. 10910–10916, Nov. 2019.

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

[22] C. Wang, K. Mao, J. Liu, and J. Liu, "Identity-based dynamic authenticated group key agreement protocol for space information network," in *Proc. Int. Conf. Netw. Syst. Secur. (NSS)*. Springer, 2013, pp. 535–548.

[23] Y. Ding, X.-W. Zhou, Z.-M. Cheng, and Q.-W. Wu, "Key management in secure satellite multicast using key hypergraphs," *Wireless Pers. Commun.*, vol. 70, no. 4, pp. 1859–1883, Jul. 2012.

[24] 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.

[25] G. Maral, J. Restrepo, E. Del Re, R. Fantacci, and G. Giambene, "Performance analysis for a guaranteed handover service in an LEO constellation with a 'satellite-fixed cell' system," *IEEE Trans. Veh. Technol.*, vol. 47, no. 4, pp. 1200–1214, Nov. 1998.

[26] L. Zhang, "Key management scheme for secure channel establishment in fog computing," *IEEE Trans. Cloud Comput.*, to be published.

[27] Y. Zhang, R. Deng, E. Bertino, and D. Zheng, "Robust and universal seamless handover authentication in 5G HetNets," *IEEE Trans. Dependable Secure Comput.*, to be published, doi: 10.1109/TDSC.2019.2927664.

[28] *Technical Specification Group Services and System Aspects; Security Architecture and Procedures for 5G System, Release 15*, document TS 33.501, 3GPP, Dec. 2018.

[29] J. Choi and S. Jung, "A handover authentication using credentials based on chameleon hashing," *IEEE Commun. Lett.*, vol. 14, no. 1, pp. 54–56, Jan. 2010.

[30] C. Lai, H. Li, R. Lu, R. Jiang, and X. Shen, "SEGR: A secure and efficient group roaming scheme for machine to machine communications between 3GPP and WiMAX networks," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2014, pp. 1011–1016.

[31] J. Cao, H. Li, M. Ma, Y. Zhang, and C. Lai, "A simple and robust handover authentication between HeNB and eNB in LTE networks," *Comput. Netw.*, vol. 56, no. 8, pp. 2119–2131, May 2012.

[32] D. He, S. Chan, and M. Guizani, "Handover authentication for mobile networks: Security and efficiency aspects," *IEEE Netw.*, vol. 29, no. 3, pp. 96–103, May 2015.

[33] *(3GPP); Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Overall Description; Stage 2, Release 13*, document TS 36.300 version 13.3.0, 3GPP, Apr. 2016.

[34] 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.

[35] W. Meng, K. Xue, J. Xu, J. Hong, and N. Yu, "Low-latency authentication against satellite compromising for space information network," in *Proc. IEEE 15th Int. Conf. Mobile Ad Hoc Sensor Syst. (MASS)*, Oct. 2018, pp. 237–244.

[36] 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, no. 2, pp. 486–497, Feb. 2019.

[37] J. Mukherjee and B. Ramamurthy, "Communication technologies and architectures for space network and interplanetary Internet," *IEEE Commun. Surveys Tuts.*, vol. 15, no. 2, pp. 881–897, 2nd Quart., 2013.

[38] H. Yao, L. Wang, X. Wang, Z. Lu, and Y. Liu, "The space-terrestrial integrated network: An overview," *IEEE Commun. Mag.*, vol. 56, no. 9, pp. 178–185, Sep. 2018.

[39] T. Li, H. Zhou, H. Luo, and S. Yu, "SERvICE: A software defined framework for integrated space-terrestrial satellite communication," *IEEE Trans. Mobile Comput.*, vol. 17, no. 3, pp. 703–716, Mar. 2018.

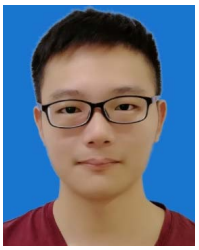
[40] A. Shamir, "How to share a secret," *Commun. ACM*, vol. 22, no. 11, pp. 612–613, 1979.

[41] M. Burrows, M. Abadi, and R. M. Needham, "A logic of authentication," *Proc. Roy. Soc. A, Math., Phys. Eng. Sci.*, vol. 426, no. 1871, pp. 233–271, 1989.

[42] *OpenSSL*. Accessed: Jan. 2020. [Online]. Available: http://www.openssl.org

[43] D. He, J. Bu, S. Chan, and C. Chen, "Handauth: Efficient handover authentication with conditional privacy for wireless networks," *IEEE Trans. Comput.*, vol. 62, no. 3, pp. 616–622, Mar. 2013.

Kaiping Xue (Senior Member, IEEE) received the bachelor's degree from the Department of Information Security, University of Science and Technology of China (USTC), in 2003, and the Ph.D. degree from the Department of Electronic Engineering and Information Science (EEIS), USTC, in 2007. From May 2012 to May 2013, he was a Post-Doctoral Researcher with the Department of Electrical and Computer Engineering, University of Florida. He is currently an Associate Professor with the School of Cyber Security, Department of EEIS, USTC. His research interests include next-generation Internet, distributed networks, and network security. He has authored and coauthored more than 80 technical artilces in the areas of communication networks and network security. His work won best paper awards in IEEE MSN 2017, IEEE HotICN 2019, and the Best Paper Runner-Up Award in IEEE MASS 2018. He serves on the Editorial Board of several journals, including the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS (TWC), the IEEE TRANSACTIONS ON NETWORK AND SERVICE MANAGEMENT (TNSM), *Ad Hoc Networks*, IEEE ACCESS, and *China Communications*. He has also served as a Guest Editor for the IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS (JSAC) and a Lead Guest Editor for the *IEEE Communications Magazine*. He is serving as the Program Co-Chair for the IEEE IWCMC 2020 and SIGSAC@TURC 2020. He is an IET Fellow.



Huancheng Zhou received the B.S. degree from the Department of Information Security, University of Science and Technology of China (USTC), in 2017, where he is currently pursuing the degree in communication and information system with the Department of Electronic Engineering and Information Science (EEIS). His research interests include network security protocol design and analysis.

Wei Meng received the B.S. degree from the Department of Information Security, School of Telecommunications Engineering, Xidian University, China, in 2016, and the M.S. degree from the Department of Electronic Engineering and Information Science (EEIS), USTC, in 2019. Her research interests include network security protocol design and analysis. Her work received the Best Paper Runner-Up Award in IEEE MASS 2018.

Authorized licensed use limited to: University of Science & Technology of China. Downloaded on June 13,2020 at 04:55:55 UTC from IEEE Xplore. Restrictions apply.

David S. L. Wei (Senior Member, IEEE) received the Ph.D. degree in computer and information science from the University of Pennsylvania in 1991. From May 1993 to August 1997, he was on the Faculty of Computer Science and Engineering, the University of Aizu, Japan (as an Associate Professor and then a Full Professor). He is currently a Full Professor with the Computer and Information Science Department, Fordham University. He has authored and coauthored more than 120 technical articles in the areas of distributed and parallel processing, wireless networks and mobile computing, optical networks, peer-to-peer communications, cognitive radio networks, big data, cloud computing, and the IoT in various archival journals and conference proceedings. He served on the program committee and was a session chair for several reputed international conferences. He was a Lead Guest Editor of the IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS for the special issue on Mobile Computing and Networking, a Lead Guest Editor of the IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS for the special issue on Networking Challenges in Cloud Computing Systems and Applications, a Guest Editor of the IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS for the special issue on Peer-to-Peer Communications and Applications, a Lead Guest Editor of the IEEE TRANSACTIONS ON CLOUD COMPUTING for the special issue on Cloud Security, a Guest Editor of the IEEE TRANSACTIONS ON BIG DATA for the special issue on Trustworthiness in Big Data and Cloud Computing Systems, and a Lead Guest Editor of the IEEE TRANSACTIONS ON BIG DATA for the special issue on Edge Analytics in the Internet of Things. He also served as an Associate Editor for the IEEE TRANSACTIONS ON CLOUD COMPUTING from 2014 to 2018 and an Associate Editor for the *Journal of Circuits, Systems and Computers* from 2013 to 2018. He is currently an Editor of the IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS for the Series on Network Softwarization & Enablers and a Lead Guest Editor of the IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS for the special issue on Leveraging Machine Learning in SDN/NFV-based Networks. He currently focuses his research efforts on cloud and edge computing, the IoT, big data, machine learning, and cognitive radio networks.

Mohsen Guizani (Fellow, IEEE) received the B.S. (Hons.) and M.S. degrees in electrical engineering, the M.S. and Ph.D. degrees in computer engineering from Syracuse University, Syracuse, NY, USA, in 1984, 1986, 1987, and 1990, respectively. He served in different academic and administrative positions at the University of Idaho, Western Michigan University, the University of West Florida, the University of Missouri-Kansas City, the University of Colorado at Boulder, and Syracuse University. He is currently a Professor with the CSE Department, Qatar University, Qatar. He has authored nine books and more than 500 publications in refereed journals and conferences. His research interests include wireless communications and mobile computing, computer networks, mobile cloud computing, security, and smart grid. He is a Senior Member of ACM. He also served as a member, a chair, and a general chair of a number of international conferences. Throughout his career, he received three teaching awards and four research awards. He also received the 2017 IEEE Communications Society WTC Recognition Award and the 2018 Ad Hoc Technical Committee Recognition Award for his contribution to outstanding research in wireless communications and *Ad-Hoc Sensor* networks. He is currently the Editor-in-Chief of the *IEEE Network Magazine*, serves on the editorial boards of several international technical journals and the Founder and an Editor-in-Chief of *Wireless Communications and Mobile Computing* journal (Wiley). He was the Chair of the IEEE Communications Society Wireless Technical Committee and the Chair of the TAOS Technical Committee. He guest edited a number of special issues in IEEE journals and magazines. He served as the IEEE Computer Society Distinguished Speaker and is currently the IEEE ComSoc Distinguished Lecturer.

Authorized licensed use limited to: University of Science & Technology of China. Downloaded on June 13,2020 at 04:55:55 UTC from IEEE Xplore. Restrictions apply.