AnFRA: Anonymous and Fast Roaming Authentication for Space Information Network

Qingyou Yang, Kaiping Xue, *Senior Member, IEEE*, Jie Xu, Jiajie Wang, Fenghua Li, and Nenghai Yu

***Abstract*— Nowadays, the Space Information Network (SIN) has been widely used in real life because of its advantages of communicating anywhere at any time. This feature is leading to a new trend that traditional wireless users are willing to roam to SIN to obtain a better service. However, the features of exposed links and higher signal latency in SIN make it difficult to design a secure and fast roaming authentication scheme for this new trend. Although some existing researches have been focused on designing secure authentication protocols for SIN or providing roaming authentication protocols for traditional wireless networks, these schemes cannot provide adequate requirements for the roaming communication in SIN and bring in critical issues, such as the privacy leakage or intolerable authentication delay. Observing these problems have not been well addressed, we design an anonymous and fast roaming authentication scheme for SIN. In our scheme, we utilize the group signature to provide the anonymity for roaming users, and assume that the satellites have limited computing capacity and make them have the defined authentication function to avoid the real-time involvement of the home network control center when authenticating the roaming users. The results of security and performance analysis show that the proposed scheme can provide the required security features, while providing a small authentication delay.**

***Index Terms*— Access authentication, anonymity, roaming, space information network.**

I. Introduction

With the acceleration of the globalization process, the demand for communicating anywhere at anytime is becoming more and more urgent [1]. Space information network (SIN) has been proposed in this background and also already been implemented in real life (e.g., Iridium, Globlastar), which uses artificial earth satellites as relay stations to transmit radio waves to achieve a wider range of communications. In the future, SIN can be developed as a Interplanetary Internet that connects spacecrafts with Earth's terrestrial Internet to support the future space exploration and ubiquitous Internet access [2]. Compared with the traditional wireless communication systems, such as cellular networks [3] and road networks [4], satellite communication system has the characteristics of global coverage, large capacity, bandwidth-on-demand flexibility and won't be limited by any complicated geographical conditions between two communication points [5]. Similarly, roaming service is also necessary to be provided by SIN: On the one hand, due to the above appealing features, users in traditional wireless networks are more willing to access SIN to obtain network services, including the roaming service, especially in some extreme conditions, such as in sea, desert, or in earthquake disaster areas, where there is no allocated base station for users to access traditional wireless networks. On the other hand, providing global roaming in current and next-generation networks to improve network accessibility and roaming quality is an important requirement for nowadays network development [6].

For the security and quality of roaming service, it is critical for SIN to deploy a secure roaming authentication protocol [7]. In traditional wireless networks, roaming authentication protocols can be classified into two types: three-party roaming authentication scheme and two-party roaming authentication scheme. Three-party roaming authentication schemes, such as [8] and [9], usually verify the roaming user at its home server, so that the foreign server cannot learn users' privacy. However, they need more interactions and cannot be implemented in the SIN architecture, as the SIN has a long propagation delay between satellites and the ground. Even for low earth orbit satellite (LEO) which is closer to the ground, there are still 500 to 2,000 kilometers [10] away from the ground, and accordingly with 10 to 40ms propagation delay. This long propagation delay will bring intolerable authentication delay to these three-party roaming authentication schemes. While two-party roaming authentication schemes authenticate roaming users without requiring the participation of its home server and usually require less interactions, which can reduce the authentication delay in theory. However, for existing two-party authentication schemes, they still cannot be deployed directly to SIN. Since they usually have some time-consuming operations (e.g., pairing) of checking revocation list in these schemes, such as [11] and [12]. Meanwhile, the long

Manuscript received April 12, 2018; revised May 17, 2018; accepted June 28, 2018. Date of publication July 10, 2018; date of current version August 8, 2018. This work was supported in part by the National Key Research and Development Program of China under Grant 2016YFB0800301, in part by the National Natural Science Foundation of China under Grant 91538203, in part by the Youth Innovation Promotion Association CAS under Grant 2016394, and in part by the Fundamental Research Funds for the Central Universities. The associate editor coordinating the review of this manuscript and approving it for publication was Dr. Eduard A. Jorswieck. *(Corresponding author: Kaiping Xue.)*

Q. Yang, K. Xue, J. Xu, and N. Yu 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).

J. Wang is with the China Information Technology Security Evaluation Center, Beijing 100085, China.

F. Li is with the State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China.

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

Digital Object Identifier 10.1109/TIFS.2018.2854740

propagation delay cannot be significantly reduced, as multiple interactions between satellites and ground devices still exist in these schemes.

In fact, with the development of satellite hardware technology, satellites have been able to carry complexity computation. Inspired by this new feature, we utilize the satellites as the verifier rather than ground servers, which can largely reduce interactions between the satellites and the ground, so as to lower authentication delay. However, except the long propagation delay challenge, security requirements for the roaming scenario in SIN are also hard to be guaranteed. Firstly, due to the vulnerability of SIN, some malicious attacks such as interception, modification, replay, and impersonation attacks can easily damage the system [13]–[16]. Secondly, the highly exposed links of SIN could be utilized by attackers to compromise users' privacy through eavesdropping the exposed channel [7]. Finally, even the foreign network entities could be potential adversaries, as they may easily disclose users' privacy by tracking users' identities and locations.

Observing the challenges that the long propagation delay and security vulnerability exist in SIN, and still no existing authentication scheme can be straightly implemented to better solve the problems. In this paper, we propose a group signature based authentication scheme to protect users' privacy and provide fast access authentication for roaming users. In our scheme, each LEO with certain computing power acts as a verifier to authenticate mobile users when they request to access the SIN, which can largely reduce the authentication delay and interaction messages. Meanwhile, the utilization of group signature can efficiently provide user anonymity, so that users' privacy won't be leaked to foreign network entities. Especially, our proposed scheme makes the following main contributions:

1) We strengthen the authentication function of LEO satellites, and proposed a fast roaming authentication scheme, named AnFRA, which can achieve a fast access authentication between users and satellites. Moreover, a pre-negotiation mechanism is implemented to faster the authentication.
2) Our proposed scheme is based on group signature, which not only makes it possible for satellites to authenticate users without the participation of the home server, but also provides a strong users anonymity and guarantees its security requirements.
3) Considering the distinctive features of SIN, a well-designed revocation mechanism is also incorporated into the design of AnFRA to support dynamic user's revocation. Although the revocation mechanism brings in some additional overhead, it avoids the time cost to implement the revocation list checking when authenticating users.

The rest of this paper is organized as follows: we first discuss related works in Section II. Then the preliminaries are demonstrated in Section III. We introduce the system model, security model and security requirements in Section IV. In Section V, we describe our proposed scheme in details, followed by the analysis of security and performance in Section VI and VII. Finally, Section VIII presents the overall conclusion.

II. Related Work

In this section, we discuss the related works in terms of *authentication schemes for SIN* and *authentication schemes for traditional networks*.

A. Authentication Schemes for SIN

In recent years, many studies have done a great deal of work on providing a secure access authentication scheme for space information network (SIN). In 1996, Cruickshank [17] first proposed a security system for satellite networks, which uses a combination of public-key and secret key systems to satisfy the security requirements of mutual authentication and data confidentiality. However, Cruickshank's scheme needs complex operations of encryption and decryption, and cannot provide user anonymity protection. In order to reduce the computation overhead, Hwang *et al.* [18] proposed a lightweight authentication in satellite networks, in which all the involved computing operations are just the hash function, the bitwise exclusive-or operation, and the string concatenation operation. The literatures [19] and [20] analyzed the security vulnerabilities in the existing schemes, and proposed their security-enhanced authentication for SIN, which can prevent user's privacy from compromising by malicious attackers. These schemes can provide secure protocols for authentication in SIN, but when implemented in the scenario of roaming to SIN, due to the untrustworthiness of the foreign network and long latency for signal propagation, these schemes may lead to privacy disclosure and intolerable authentication delay.

B. Authentication Schemes for Traditional Networks

Although, public key infrastructure (PKI) has been widely used in traditional networks, its complicated and time-consuming certificates management has attracted the concerns of researchers. Therefore, some identity-based authentication schemes have been proposed, such as [21], [22], and [23]. In these schemes, users need to require and store lots of one-time pseudo identities, which is challenging for capacity-constrained mobile devices. For preventing illegal access, verifiers have to store each used and revoked pseudo identity in its local memory. However, the satellites have limited storage capacity, this makes identity-based authentication scheme hard to implement to SIN. Moreover, identity-based authentication schemes usually rely on a trusted third party (private key generator (PKG)), which may be a single point of bottleneck or be compromised. Thus, Menmon *et al.* [24], [25] utilized certificate-less public key cryptography (CL-PKC) to design authentication protocols for GSM, in which keys are generated from both the user and the key generation center (KGC). However, these schemes are not designed for the roaming scenario in which the foreign access points are usually untrusted and may compromise users' privacy. So these schemes are not suitable for the roaming scenario.

However, in traditional wireless networks, some roaming authentication schemes have been proposed to provide user authentication in different authentication domains and address

the privacy disclosure issue. In 2006, Jiang *et al.* [8] used the secret-splitting principle and self-certified technologies, and proposed a lightweight roaming authentication protocol for wireless mobile networks to provide the security property of identity anonymity. While some group signature based roaming authentication schemes [11], [26], [27] were proposed to preserve roaming user's privacy when roaming to an untrusted network. However, due to the long propagation latency between satellite and ground communication point in SIN, directly implementing these roaming protocols to SIN can not address the problems of long authentication delay, especially in [11], a time-consuming pairing operation of checking revocation list is required. Therefore, in this paper, we design a special access authentication protocol for roaming to SIN, which can not only guarantee the anonymity for roaming users, but also can largely reduce the authentication delay.

III. Preliminaries

In this section, we first give a review of background information on bilinear pairing and the security assumption defined on it, then we briefly describe the definition of elliptic curve digital signature algorithm.

A. Bilinear Pairing

Let $\mathbb{G}$ be additive cyclic group of the prime order p, and $\mathbb{G}_T$ be multiplicative cyclic group of the same prime order, and P be a generator of group of $\mathbb{G}$. Suppose $\mathbb{G}$ and $\mathbb{G}_T$ are equipped with a pairing, i.e., a non-degenerated and efficiently computable bilinear map $e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$ such that $e(aP_1, bQ_1) = e(P_1, Q_1)^{ab} \in \mathbb{G}_T$ for all a, b in $\mathbb{Z}_p^*$ and any $P_1, Q_1 \in \mathbb{G}$. We refer to [28] and [29] for a more comprehensive description of pairing technique.

Definition I: A bilinear parameter generator $\mathcal{G}en$ is a probabilistic algorithm that takes a security parameter κ as input and output a 5-tuple$(p, P, \mathbb{G}, \mathbb{G}_T, e)$.

Definition II (q-Strong Diffie-Hellman (q-SDH) Problem): Given a $(q+1)$-tuple $(g, \gamma \cdot g, \gamma^2 \cdot g, \ldots, \gamma^q \cdot g)$, it is difficult to compute a pair $(\frac{1}{\gamma+x} \cdot g, x)$, where $x, \gamma \in \mathbb{Z}_p^*$, g is a generator of $\mathbb{G}$. An algorithm $\mathcal{A}$ has advantage ϵ in solving q-SDH in $(\mathbb{G}, \mathbb{G})$ if $\Pr[\mathcal{A}(g, \gamma \cdot g, \gamma^2 \cdot g, \ldots, \gamma^q \cdot g) = (\frac{1}{\gamma+x} \cdot g, x)] \geq \epsilon$.

Definition III (Decision Linear Diffie-Hellman Problem): Given $u, v, h, u^a, v^b, h^c \in \mathbb{G}$ as input, output yes if $a + b = c$ and no otherwise. More precisely, the advantage algorithm $\mathcal{A}$ in deciding the Decision Linear problem in $\mathbb{G}$ is defined as: $\text{Adv Linear}_A = |\Pr[\mathcal{A}(u, v, h, u^a, v^b, h^{a+b}) = yes : u, v, h \leftarrow \mathbb{G}, a, b \leftarrow \mathbb{Z}_p] - \Pr[\mathcal{A}(u, v, h, u^a, v^b, \tau) = yes : u, v, \tau \leftarrow \mathbb{G}, a, b \leftarrow \mathbb{Z}_p]|$.

B. Elliptic Curve Digital Signature Algorithm (ECDSA)

ECDSA is the elliptic curve analogue of the Digital Signature Algorithm (DSA), which mainly contains the following three algorithms in ANSI standard [30]. It should be noted that the SHA-1 algorithm is not secure any more [31], and recommended to be replaced by other secure hash algorithms such as SHA-256 [32]:

- $EC.Keygen()$: The key pair of an entity is associated with a particular set of elliptic curve domain parameters, which consist of a suitable chosen elliptic curve E defined over a finite field $\mathbb{F}_q$ of characteristic p, and a base point $G \in E(\mathbb{F}_q)$. To generate the signing/verifying key pair, the entity first selects a random or pseudorandom integer d in the interval $[1, n-1]$ (where n is a sufficiently large prime), then computes $Q = d \cdot G$. Thus, the signing/verifying key pair is (d, Q).
- $EC.Sign(d, m)$: To sign a message m, an entity should implement the steps as follows:
  (1) Select a random integer k $(1 \leq k \leq n-1)$;
  (2) Compute $k \cdot G = (x_1, y_1)$ and $r = x_1 \mod n$. If $r = 0$, go to step (1);
  (3) Compute $k^{-1} \mod n$, $e = \text{SHA-1}(m)$ and $s = k^{-1}(e + d \cdot r) \mod n$. If $s = 0$, go to step (1);
  (4) The signature for the message m is $\sigma = (r, s)$.
- $EC.Verify(Q, \sigma)$: To verify the signature $\sigma = (r, s)$, an entity implements the following steps:
  (1) Verify whether r and s are two integers in the interval $[1, n-1]$. If yes, continue;
  (2) Compute $e = \text{SHA-1}(m)$, $w = s^{-1} \mod n$, $u_1 = e \cdot w \mod n$ and $u_2 = r \cdot w \mod n$;
  (3) Compute $X = u_1 \cdot G + u_2 \cdot Q$. If $X = \mathcal{O}$, reject the signature. Otherwise, compute $v = x_1 \mod n$ where $X = (x_1, y_1)$. Accept the signature if and only if $v = r$.

IV. System Model, Security Model and Security Requirements

In this section, we give the definitions of the system model, security model and security requirements of the roaming authentication scenario in SIN.

A. System Model

The trend of providing global roaming in kinds of networks makes it necessary for the SIN to provide roaming service for its roaming users. The roaming scenario in SIN is illustrated in Fig.1. Without loss of generality, we only consider the system model that user roams between the homogeneous SINs, and the scenario of roaming to SIN from other heterogeneous networks (e.g., cellular networks) is the same as this. The system model in our scheme consists of a global offline trusted third party (TTP) and several domains, and each domain contains a network control center (NCC), gateway stations (GSs), low earth orbit satellites (LEOs) and mobile users. Following illustrates the functions and duties of each entity:

- *TTP* is in charge of managing and distributing public/private key pairs for NCCs in different domains. These keys are used for authenticating among these NCCs, so that they can exchange information securely.
- *NCC* is the management of its network domain. It provides registration and certification for users to access the home/foreign network.

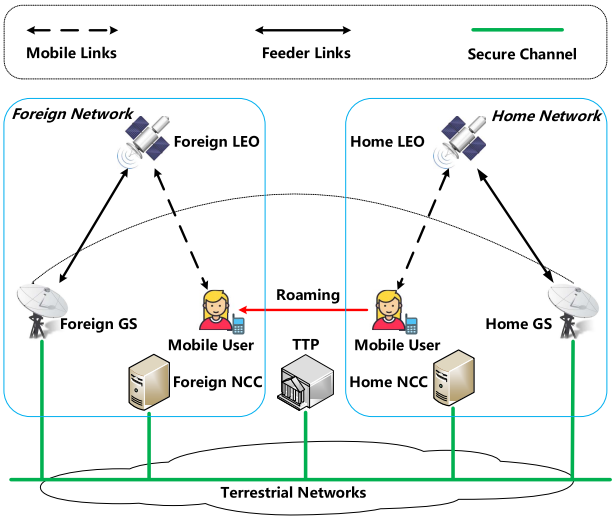


Fig. 1. System model.

- *GS* is a middle entity between the NCC and LEOs. It connects to the NCC through the terrestrial networks, and provides a ground interface for LEOs.
- *LEO* is the access point for users to access the network. With the satellite manufacturing technology advancement, nowadays LEO satellites can have certain computing capacities to execute some complex functions [2].
- *Users* access the network to obtain its subscription services. In this paper, we consider the scenario where a roaming user is out of its home network and visiting a foreign network.

B. Security Model

The proposed scheme has the following security assumptions:

- The proposed scheme assumes that the TTP is trustworthy for both home network entities and foreign network entities. It is infeasible for any adversary to compromise.
- We assume that there exists a secure channel between NCCs and TTP, NCC and its domain GS, respectively. This secure channel can be constructed by the TLS or SSL protocol.
- We assume that a polynomial time adversary, who can modify or interrupt the interaction messages among the users, FGSs and foreign LEOs (FLEOs), tries to break the proposed anonymous authentication protocol when roaming users access to the foreign network.
- Foreign entities (i.e., FLEOs, FGSs, and FNCC) may be malicious adversaries in our scheme, they may intend to break the proposed scheme to retrieve the roaming user's identity from user's access request.

C. Security Requirements

A well-designed roaming authentication should satisfy the following security requirements, which includes not only the security but also the privacy.

- ***Mutual Authentication***: The system should have the ability to detect unauthorized users' accessing and abort the requests. Meanwhile, users should have the ability to check the legitimacy of the specific access point.
- ***Anonymity***: Except HNCC, no one could learn user's real identity from the authentication interactions. The preservation of anonymity should also protect user's location privacy.
- ***Unlinkability***: To associate multiple authentications cannot get the knowledge whether they are from the same user.
- ***Key Establishment***: The authentication scheme should provide a key agreement protocol to construct a random session key that is only shared between the FGS and the user.
- ***Forward/Backward Secrecy***: It requires that the disclosure of the current session key would not affect the security of its future and previous session keys.

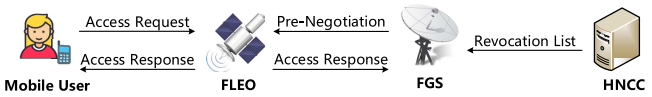


Fig. 2. Overview of AnFRA.

V. Proposed Scheme: AnFRA

In this section, we first give the overview of the proposed anonymous and fast roaming authentication system. In the following, we give a detailed description of the protocol, which mainly consists of five phases: *System Initialization*, *Pre-Negotiation*, *User Authentication*, *User Identity Reveal*, and *Dynamic User Enrollment and Revocation*.

A. Overview

The overview of the proposed protocol is shown in Fig.2. After the system initialization, in each domain, the gateway station (GS) sends a pre-negotiation message to each of its maintained LEOs in advance, which contains a parameter for key negotiation. A mobile user who wants to access the foreign network first needs to request to its home network control center (HNCC) to obtain associated access keys. When the user roams to a foreign network, he/she first sends an access request to the access point of foreign network (i.e., FLEO), which includes a signature that can verify the legality of the user. If the verification is passed, FLEO will send an access response to the user and FGS at the same time. The access response contains two key negotiation parameters that can then be used to build a secure channel between the user and FGS. Additionally, HNCC periodically publishes the revocation list to users, so that the unrevoked users can update their private key to the latest.

To verify the legitimacy of roaming users, group signature is introduced in our scheme, in which the HNCC acts as the group manager, and authorizes FLEOs as the verifiers to check whether the access request is signed by an authorized roaming user (a group member). Therefore the HNCC can be offline during the authentication procedures. Thus, the authentication delay and interactions can be largely reduced. Additionally,

group signature can provide good anonymity for the roaming users, so that the untrusted foreign network entities are unable to compromise users' privacy.

In addition to verifying the legitimacy of roaming users, a secure protocol also requires to verify the legitimacy of FLEO and FGS. For this purpose, we utilize a conventional digital signature scheme, i.e., Elliptic Curve Digital Signature Algorithm (ECDSA) [30] which is more efficient when compared to RSA signature [33].

B. Details of Our Proposed Scheme

1) System Initialization Phase: In the system initialization phase, each NCC can be seen as key distribution center (KDC) in its domain, which first generates and assigns ECDSA's signing/verifying key pairs for its GS and LEO. For clarity and without loss of generality, in the following description, we simplify the system model with only one LEO and GS that are associated with the user's communication in each domain. And we denote the key pairs for the GS and LEO are (sk_{GS}, pk_{GS}) and (sk_{LEO}, pk_{LEO}) respectively. Then each NCC works as the group manager, and initializes its group by implementing **Algorithm 1**.

Algorithm 1 Group Initialization

Input: the number of users N;
Select a random generator $g \in_R \mathbb{G}$;
Select a random number $h \in_R \mathbb{G}$;
Select $\xi_1, \xi_2 \in_R \mathbb{Z}_p^*$;
Set $u, v \in \mathbb{G}$, such that $\xi_1 \cdot u = \xi_2 \cdot v = h$;
Select $\gamma \in_R \mathbb{Z}_p^*$;
Set $\omega = \gamma \cdot g$;
set the group public key as $gpk = (g, h, u, v, \omega)$;
set the group private key as $gmsk = (\xi_1, \xi_2)$;
foreach *user* U_i $(1 \le i \le N)$ **do**
  Select $x_i \in_R \mathbb{Z}_p^*$;
  Set $A_i = \frac{1}{\gamma + x_i} \cdot g$;
  set the private key tuple as $gsk[i] = (A_i, x_i)$;
  Send gpk, $gsk[i]$, pk_{LEO}, pk_{GS}, ID_{NCC} to U_i;
  Store the tuple (ID_{U_i}, x_i, A_i) in the user index table;
end

The algorithm takes as input a parameter N, the number of members of the group, and process as follows. Firstly, NCC selects a generator g in the group $\mathbb{G}$ at uniformly at random. Then selects random numbers $h \in \mathbb{G}$ and $\xi_1, \xi_2 \in \mathbb{Z}_p^*$, and sets $u, v \in \mathbb{G}$ such that $u \cdot \xi_1 = v \cdot \xi_2 = h$. Finally NCC selects a random number $\gamma \in \mathbb{Z}_p^*$ and computes $\omega = \gamma \cdot g$. Therefore, the group public key is $gpk = (g, h, u, v, \omega)$ which can be broadcast to all LEOs in its domain. And the corresponding private key of the group manager is $gmsk = (\xi_1, \xi_2)$. When a mobile user U_i registers to its NCC, the NCC first generates a private key tuple $gsk[i] = (A_i, x_i)$, where $x_i \in_R \mathbb{Z}_p^*$ and $A_i = \frac{1}{\gamma + x_i} \cdot g$. Then NCC sends gpk, $gsk[i]$, pk_{GS}, pk_{LEO} and its identity ID_{NCC} to U_i securely. Finally, NCC stores the tuple (ID_{U_i}, x_i, A_i) in a user index table for revealing user's identity. It should be noted that **Algorithm 1** is only performed once at the beginning of the deployment of system. So we can ignore the computation cost for this phase.

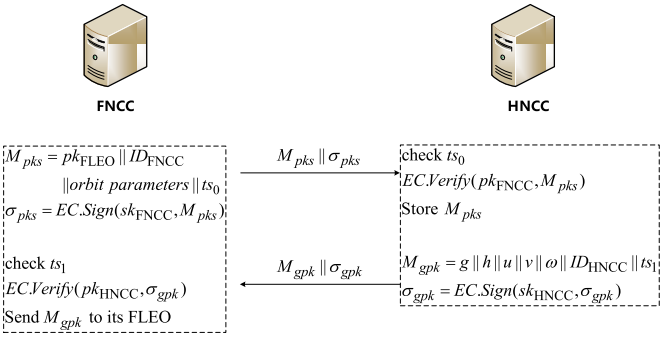


Fig. 3. Information exchange between HNCC and FNCC.

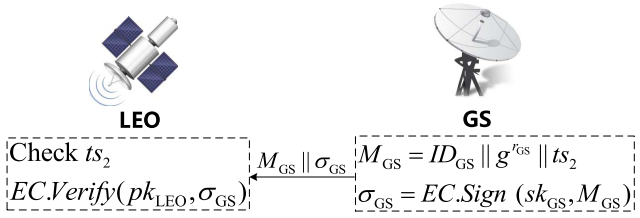


Fig. 4. Pre-negotiation phase.

Additionally, the global trusted third party (TTP) also generates ECDSA's signing/verifying key pairs for all NCCs in different domains. We denote the key pairs for FNCC and HNCC as (sk_{FNCC}, pk_{FNCC}) and (sk_{HNCC}, pk_{HNCC}) respectively, which is used for exchanging information between different domains. The information exchange steps in this phase are presented in Fig.3.

Firstly, FNCC generates the message M_{pks} which contains FLEO's public key pk_{FLEO}, FNCC's identity ID_{FNCC}, FLEO's orbit parameters that are used for computing the location of FLEO, and a timestamp ts_0. Then FNCC signs M_{pks} by ECDSA's signing algorithm $EC.Sign(sk_{FNCC}, M_{pks})$. Finally FNCC sends the message and the signature to HNCC. If the timestamp ts_0 is within an allowed range compared to current time, and the signature is verified successfully by HNCC, the message will be stored by the HNCC. If a registering user has the roaming requirement, its NCC needs to securely deliver M_{pks} to the registering user in this phase. Then the HNCC generates message $M_{gpk} = g||h||u||v||\omega||ID_{HNCC}||ts_1$, where the ID_{HNCC} is the identity of HNCC, ts_1 is a new timestamp. Then HNCC signs it with its private key sk_{HNCC} and sends to FNCC. If the verification for timestamp and signature are passed, FNCC delivers the group public key gpk to all LEOs in its domain.

2) Pre-Negotiation Phase: The pre-negotiation phase as shown in Fig.4 will be implemented between each LEO and GS in each domain. In this phase, each GS sends a pre-negotiation message M_{GS} to the LEO. This message contains a parameter $g^{r_{GS}}$ (r_{GS} is a random number selected by the GS), which will be utilized in the authentication phase for session key negotiation. A timestamp ts_2 is also involved for resisting replay attacks. Moreover, the GS signs the pre-negotiation

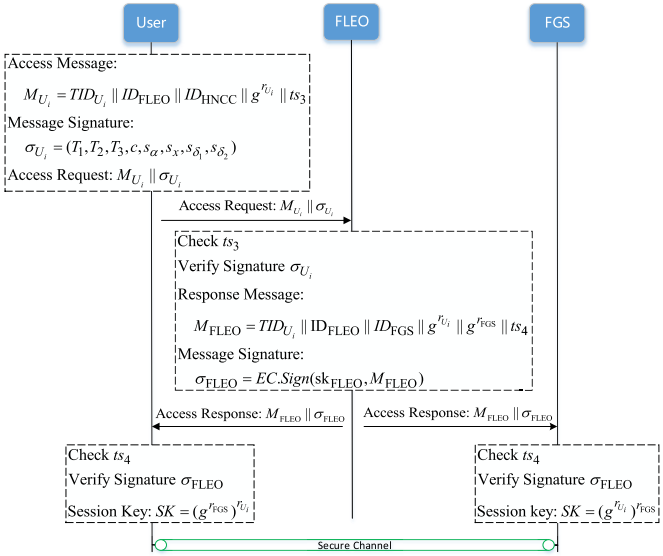


Fig. 5. User authentication phase.

message with its private signing key sk_{GS} by ECDSA's signature algorithm as $EC.Sign(sk_{GS}, M_{GS})$. Then the GS sends the signed message to LEO. After receiving this message, LEO first checks whether the timestamp ts_2 is within an allowed range compared with its current time, and verifies the signature σ_{GS} by ECDSA's verifying algorithm $EC.Verify(pk_{GS}, \sigma_{GS})$. If both two verifications are passed, the LEO caches M_{GS}. Additionally, this phase can be periodically implemented to update the negotiation parameters for further reducing the possibility of the session key leakage.

3) User Authentication Phase: This phase is implemented when a mobile user (e.g., U_i) roams to a foreign network, and wants to access the network for obtaining services. In this phase, the FLEO needs to verify the legitimacy of roaming user's identity from the user's access request. If the verification is passed, a secure channel can be further established between the roaming user and FGS. We illustrate this procedure in Fig. 5, and the detailed steps are described as follows. (It is noted that, in this paper, we mainly focus on roaming authentication scheme for SIN, the authentication for accessing home network can also be achieved by implementing the following authentication processes with replacing entities of FLEO and FGS as its local domain LEO and GS.)

(1) As in **Algorithm 2**, U_i firstly generates an access request, which contains an access request message and the corresponding signature. The access request message is $M_{U_i} = TID_{U_i}||ID_{FLEO}||ID_{HNCC}||g^{r_{U_i}}||ts_3$, where TID_{U_i} is a temporary identity (not correlated in any way with the user's real identity), r_{U_i} is a random number selected by U_i, ID_{HNCC} is the identity of U_i's home NCC, ID_{FLEO} is the identity of the FLEO that U_i is going to communicate to. U_i can infer the FLEO's identity by utilizing their orbit parameters [34] which are obtained in the system initialization phase. And a timestamp ts_3 is also generated and added to resist the replay attacks. The signature is $\sigma_{U_i} = (T_1, T_2, T_3, c, s_\alpha, s_\beta, s_x, s_{\delta_1}, s_{\delta_2})$, in which, T_1, T_2, T_3 are different computing results, c is a hash value, s_α, s_β, s_x, s_{δ_1}, s_{δ_2} are selected random numbers. The detailed signature generation process is shown in **Algorithm 2** which is based on the group signature algorithm as that in [35]. After generating the access request $M_{U_i}||\sigma_{U_i}$, the user sends it to the corresponding FLEO. It should be noted that some operations (e.g., $e(h, w)$, $e(h, g)$, $e(g, g)$) in the algorithm can be pre-computed and cached by the user to speed up user authentication.

Algorithm 2 Access Request Generation

Input: group public key gpk, U_i's group private key $gsk[i]$, home NCC's identity ID_{HNCC};
Output: Access request $M_{U_i}||\sigma_{U_i}$;

Select a random number r_{U_i};
Compute $g^{r_{U_i}}$;
Select a temporary identity TID;
Generate timestamp ts_3;
Set the access request message as $M_{U_i} = TID_{U_i}||ID_{FLEO}||ID_{HNCC}||g^{r_{U_i}}||ts_3$;
Select random numbers $\alpha, \beta, r_\alpha, r_\beta, r_x, r_{\delta_1}$ and r_{δ_2};
Set $\delta_1 = x_i\alpha, \delta_2 = x_i\beta$;
Set $T_1 = \alpha u, T_2 = \beta v, T_3 = A + (\alpha + \beta)h$;
Select random numbers $r_\alpha, r_\beta, r_x, r_{\delta_1}$ and r_{δ_2};
Set
  $R_1 = r_\alpha u$,
  $R_2 = r_\beta v$,
  $R_3 = e(T_3, g)^{r_x} \cdot e(h, (-r_\alpha - r_\beta)\omega + (-r_{\delta_1} - r_{\delta_2})g)$,
  $R_4 = r_x T_1 - r_{\delta_1} u$,
  $R_5 = r_x T_2 - r_{\delta_2} v$;
Set $c = H(M, T_1, T_2, T_3, R_1, R_2, R_3, R_4, R_5) \in \mathbb{Z}_p$;
Set $s_\alpha = r_\alpha + c\alpha, s_\beta = r_\beta + c\beta, s_x = r_x + cx, s_{\delta_1} = r_{\delta_1} + c\delta_1, s_{\delta_2} = r_{\delta_2} + c\delta_2$;
Set $\sigma_{U_i} = (T_1, T_2, T_3, c, s_\alpha, s_\beta, s_x, s_{\delta_1}, s_{\delta_2})$;
return Access request $M_{U_i}||\sigma_{U_i}$;

(2) For each received access request, the specific FLEO verifies the message and generates the access response message by implementing **Algorithm 3**. Firstly, the FLEO checks whether the timestamp ts_3 is within an allowed range compared with its current time. If it is positive, the FLEO then checks whether the signature is valid. If the verification isn't passed, the FLEO will reject the access request; otherwise, the FLEO reads the corresponding pre-negotiation message which has been cached in the pre-negotiation phase, and generates an access response message as $M_{FLEO} = TID_{U_i}||ID_{FLEO}||ID_{FGS}||g^{r_{U_i}}||g^{r_{FGS}}||ts_4$, where ts_4 is a new timestamp, ID_{FLEO} is FLEO's identity. Then FLEO signs the response message M_{FLEO} by its private key sk_{FLEO}. Finally, the FLEO sends the access response message with the corresponding signature to the roaming user and FGS.

(3) Upon receiving the access response message from the FLEO, the user and FGS respectively implement

Algorithm 3 Access Response Generation

Input: FLEO's private key sk_{FLEO}, access request $M_{U_i}||\sigma_{U_i}$, pre-negotiation message M_{FGS}; group public key $gkp = (g, h, u, v, \omega)$;
Output: Access response $M_{FLEO}||\sigma_{FLEO}$;

Check whether timestamp ts_3 is within an allowed range;
if *the verification of* ts_3 *is not passed* **then**
  Reject the access request;
  return Failed;
else
  Set
  $R'_1 = s_\alpha \cdot u - c \cdot T_1$, $R'_2 = s_\beta \cdot v - c \cdot T_2$,
  $R'_3 = e_1 \cdot e_2 \cdot e_3 \cdot e_4 \cdot e_5$, where
    $e_1 = e(s_x T_3, g)$, $e_2 = e(cT_3, \omega)$,
    $e_3 = e(h, \omega)^{-s_\alpha - s_\beta}$, $e_4 = e(h, g)^{-s_{\delta_1} - s_{\delta_2}}$,
    $e_5 = e(g, g)^{-c}$,
  $R'_4 = -s_{\delta_1} \cdot u + s_x \cdot T_1$,
  $R'_5 = -s_{\delta_2} \cdot v + s_x \cdot T_2$;
  if $c \neq H(M, T_1, T_2, T_3, R'_1, R'_2, R'_3, R'_4, R'_5)$ **then**
    Reject the access request;
    return Failed;
  else
    Generate timestamp ts_4;
    Set the access response message as $M_{FLEO} = TID_{U_i}||ID_{FLEO}||ID_{FGS}||g^{r_{U_i}}||g^{r_{FGS}}||ts_4$;
    Generate the corresponding signature for M_{FLEO} as $\sigma_L = EC.Sign(sk_{FLEO}, M_{FLEO})$;
    return Access response $M_{FLEO}||\sigma_{FLEO}$;
  end
end

Algorithm 4 Secure Channel Establishing

Input: Access Response $M_L||\sigma_{FLEO}$, FLEO's public key pk_{FLEO}, parameter r_{U_i} or r_{FGS};
Output: Session key SK;

Check whether timestamp ts_4 is within an allowed range;
if *the verification of* ts_4 *is not passed* **then**
  Reject the access response;
else
  Check the signature by $EC.Verify(pk_{FLEO}, \sigma_{FLEO})$;
  if *not passed* **then**
    Drop the access response;
  else
    Set $SK = (g^{r_{FGS}})^{r_{U_i}}$ or $SK = (g^{r_{U_i}})^{r_{FGS}}$;
    return SK;
  end
end

Algorithm 4 to establish a secure channel between them. In this algorithm, the user and FGS first check the timestamp ts_4. Then they verify the signature σ_{FLEO} by implementing $EC.Verify(pk_{FLEO}, \sigma_{FLEO})$. If the verification is successfully passed, the user can compute the session key $SK = (g^{r_{FGS}})^{r_{U_i}}$, while the FGS obtains the session key SK by computing $SK = (g^{r_{U_i}})^{r_{FGS}}$.

Algorithm 5 Signature Reveal

Input: Login Request $M_{U_i}||\sigma_{U_i}$, group public key gpk, group manager's private key $gmsk$;
Output: Real identity ID_{U_i}

Check the signature σ_{U_i};
if σ_{U_i} *is not valid* **then**
  Stop the process;
  return Failed;
else
  Compute user's private key $A_i = T_3 - \xi_1 \cdot T_1 - \xi_2 \cdot T_2$;
  Retrieve user real identity ID_{U_i} by A_i in the user index table;
  return Real identity ID_{U_i};
end

4) User Identity Reveal Phase: To reveal U_i's identity, the HNCC collects the access message M_{U_i} and its signature $\sigma_{U_i} = (T_1, T_2, T_3, c, s_\alpha, s_\beta, s_{\delta_1}, s_{\delta_2})$ from the FLEO. By inputting the group public key $gpk = (g, h, u, v, \omega)$ and the corresponding group manager's private key $gmsk = (\xi_1, \xi_2)$, the signature reveal process can be implemented as that described in **Algorithm 5**. In this algorithm, HNCC first verifies whether the σ_{U_i} is a valid signature on M_{U_i}, if it returns false, the signature reveal process will be stopped; otherwise, HNCC can compute the user's private key A_i as $A_i = T_3 - \xi_1 \cdot T_1 - \xi_2 \cdot T_2$. Then HNCC can further retrieve the user real identity ID_{U_i} by looking up the user index table corresponding to the private key A_i recovered from the signature.

5) Dynamic User Enrollment and Revocation: Dynamic user's enrollment means the system allows a new user register to the system at anytime after system initialization. This is important for a practical roaming authentication system. In our proposed scheme, when a new user U_{new} registers to HNCC, the HNCC first selects a random number $x_{new} \in_R \mathbb{Z}_p^*$, and computes $A_{new} = \frac{1}{\gamma + x_{new}} \cdot g$. Then the HNCC sends U_{new}'s private key (A_{new}, x_{new}) and other system parameters (i.e., $g, u, v, h, \omega, pk_{FLEO}, ID_{HNCC}, orbit\ parameters$) to the user securely. It is worth noting that there is no additional operation for the original users in the system when a new user registers to the system.

However, some users may leave out of the system due to key loss, illegally usage, etc. To revoke these users, HNCC should periodically deliver a revocation lists which contains revoked users' private keys (e.g., (A_j, x_j)) to unrevoked users. Considering the dynamic and unstable users and topology of SIN, we design a mechanism for revocation lists distribution as the Fig. 6. Since satellites and mobile users are energy-limited, we adopt the incremental update of revocation lists (RL), that is, HNCC periodically broadcasts the increased entries to the FGS, which is then broadcast to the online users through FLEO as well. Meanwhile, FGS stores the full revocation lists in local memory during this process. To make sure

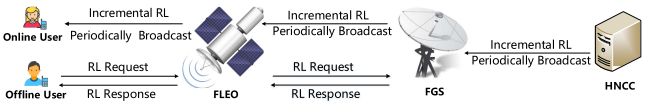


Fig. 6. Revocation list distribution.

the full revocation lists are synchronous among all FGSs in different domains, once a FGS doesn't receive the incremental revocation lists from other domain NCC at the broadcast time, it should request to the NCC for the incremental RL. However, some offline users who may miss one or several updates of incremental RL, should firstly request the missing part of revocation list entries from FGS. After receiving the request from the offline user, the FGS looks up its local full RL to retrieve the missing revocation list entries for user, and sends back to the offline user. After these procedures, both the online and offline users can accept the latest revocation list entries for them.

After obtaining the latest revocation lists, both the online and offline users can update their private key to the latest. Following process shows the updating operations for user U_i to revoke a user U_j in his/her revocation lists at a time. By repeating the process r times, the user can revoke r users on his/her revocation lists.

(1) Update g as $\hat{g} = A_j = \frac{1}{x_j+\gamma} \cdot g$.
(2) Update the public key ω as $\hat{\omega} = g - x_j \cdot A_j = \gamma \cdot \hat{g}$.
(3) Update A_i (for $i \neq j$) as $\widehat{A}_i = \frac{1}{x_i - x_j} \cdot A_j - \frac{1}{x_i - x_j} \cdot A_i = \frac{1}{x_i+\gamma} \cdot \hat{g}$
(4) Set the new private key as $(\widehat{A}_i, x_i)$.

Although the revocation-support mechanism brings in some additional overhead of communication and computation, users can perform the operations offline, and the performance analysis (shown in Section VII-C) also shows that our revocation mechanism is efficient. Since the number of GSs in each domain is very small and the foreign network entities FLEO and FGS only need to perform a few simple operations in our scheme, such as forwarding and storing RL, it is practical to deploy this revocation mechanism in actual SIN system. More importantly, the designing revocation mechanism helps to accelerate the authentication procedure, since the verifier (FLEO) is no longer necessary to perform the time-consuming operation of checking revocation list when verifying users (as in some existing schemes).

VI. Security Analysis

In this section, we analyze the security of the proposed AnFRA to verify whether the security requirements introduced in Section IV-C have been satisfied.

A. Mutual Authentication

User authenticates the identity of FLEO by the challenge-response pair $(g^{r_{U_i}}, \sigma_{FLEO})$, where $\sigma_{FLEO} = EC.Sign(sk_L, M_{FLEO})$. Since the Elliptic Curve Digital Signature Algorithm (ECDSA) has been proven secure under the assumption that the discrete logarithm problem is hard and that the hash function employed is a random function [30], without knowing the private key sk_L, it is infeasible to forge a valid signature on U_i's freshly generated challenge $g^{r_{U_i}}$ with non-negligible probability. Moreover, the identity of FLEO and its public key pk_{FLEO} have been bound and published to users by trusted TTP during the system initialization phase. Therefore, any other LEOs cannot cheat by using different public keys or different identities. And the user authentication is achieved by another challenge-response pair: $(g^{r_{U_i}}, ts_3, \sigma_{U_i})$. Only a legitimate group member can generate a valid group signature on U_i's challenge $\{g^{r_{U_i}}, ts_3\}$. Thus, mutual authentication is achieved between user and FLEO. And the mutual authentication between FLEO and FGS is also achieved through the challenge-response pairs: $(g^{r_{FGS}}, ts_2, \sigma_{FGS})$ and $(g^{r_{FGS}}, ts_4, \sigma_{FLEO})$. Because only the legitimate FGS and FLEO can generate a valid signature on challenge $\{g^{r_{FGS}}, ts_2\}$ and $\{g^{r_{FGS}}, ts_4\}$ respectively.

B. Conditional Anonymity and Unlinkability

In our protocol, the signature on the access message $M_{U_i} = \{TID_{U_i} || ID_{FLEO} || ID_{HNCC} || g^{r_{U_i}} || ts_3\}$ is the form of group signature [30], which satisfies the security requirements of anonymity, that is, given the group signature σ_{U_i} of the access message, it is computationally difficult to identify the actual signer by the entity who does not have the group manager private key $gmsk$. However, this anonymity is conditional. The real identity of signature can be revealed by HNCC by carrying out the *User Identity Reveal Phase*: given a signature $\sigma = \{T_1, T_2, T_3, c, s_\alpha, s_\beta, s_{\delta_1}, s_{\delta_2}\}$, HNCC uses its private key $gmsk = (\xi_1, \xi_2)$ to reveal the user's private key A by computing $A = T_3 - \xi_1 \cdot T_1 - \xi_2 \cdot T_2$, and retrieves the user's real identity ID_{U_i} by looking up the user index table. Thus, conditional privacy is achieved. Moreover, user unlinkability is achieved: given two group signature σ_1 and σ_2, according to the verification procedure, it is computationally hard to decide whether these two valid signatures are computed by the same group member.

C. Key Establishment and Forward/Backward Secrecy

In each session, the session key SK is computed from key negotiation parameters $g^{r_{U_i}}$ and $g^{r_{FGS}}$. Computing session key SK from these two parameters without knowing r_{U_i} and r_{FGS} is equivalent to solve the discrete logarithmic problem (DLP), which is known that it is computationally infeasible [36]. So the session key cannot be derived by any adversary. Besides, the key forward/backward secrecy is mainly achieved by the independence of the session key SK in different sessions. In our scheme, each session is used different fresh random number r_{U_i} for key establishment, which makes the independence of each session key possible, that means an attacker cannot acquire the next or the previous session key even though he/she has obtained the current session key.

D. Resistance of Modification Attacks

Suppose that an attacker intercepts the access request $M_{U_i} || \sigma_{U_i}$ and modifies it. On the one hand, since the attacker

TABLE I
COMPARISON OF FUNCTIONS AND AUTHENTICATION OVERHEAD

	Number of Parties	Conditional Anonymity	Unlinkability	Authentication Delay (ms)
[8]	4	Yes	Yes	$6 \cdot T_{U\text{-}FL} + 2 \cdot T_{FGS\text{-}HNCC} = 70.0$
[19]	4	No	Yes	$3 \cdot T_{exp} + 4 \cdot T_{U\text{-}FL} + 2 \cdot T_{FGS\text{-}HNCC} = 51.161$
[20]	≥ 3	Yes	No	$\geq 4 \cdot T_{U\text{-}FL}$ = 40.0
[21]	3	Yes	Yes	$T_{pair} + 6 \cdot T_{mul} + T_{exp} + 6 \cdot T_{U\text{-}FL} = 74.546$
[23]	3	Yes	Yes	$2 \cdot T_{pair} + 4 \cdot T_{mul} + 4 \cdot T_{exp} + 6 \cdot T_{U\text{-}FL} = 86.858$
[27]	3	Yes	Yes	$\geq 14 \cdot T_{pair} + 35 \cdot T_{mul} + 6 \cdot T_{U\text{-}FL} = 239.802$
AnFRA	3	Yes	Yes	$14 \cdot T_{mul} + 6 \cdot T_{exp} + 1 \cdot T_{pair} + 2 \cdot T_{U\text{-}FL} = 39.489$

does not possess the private key of the user, the attacker does not have any ability to compute a valid σ'_{U_i} on a modification message M'_{U_i}. Once the FLEO verifies the signature, the signature would be found to be invalid. On the other hand, if an attacker modifies the access response $M_{FLEO}||\sigma_{FLEO}$ as $M'_{FLEO}||\sigma'_{FLEO}$. Without FLEO's private key sk_{FLEO}, the forging signature σ'_{FLEO} could not be passed from the verification algorithm $EC.Verify(pk_{FLEO}, \sigma'_{FLEO})$. As a result, AnFRA successfully prevents the unauthorized modifications.

E. Resistance of Replay Attacks

It is noted that the access request message $M_{U_i} = TID_{U_i}||ID_{FLEO}||ID_{HNCC}||g^{r_{U_i}}||ts_3$ contains a timestamp ts_3, which is hashed to get $c = H(M, T_1, T_2, T_3, R_1, R_2, R_3, R_4, R_5)$. Then, it would be signed as $\sigma_{U_i} = (T_1, T_2, T_3, c, s_\alpha, s_\beta, s_x, s_{\delta_1}, s_{\delta_2})$. Because of the above steps, the timestamp cannot be modified and replaced. So the access request would be rejected if FLEO checks the timestamp ts_3 is invalid. And the access response message M_L is also appended a timestamp ts_4 and signed by $EC.Sign(sk_{FLEO}, M_{FLEO})$, which guarantees the timestamp cannot be modified and replaced. So the replaying messages could be found by checking the timestamps and signatures. Therefore, the proposed scheme is able to resist replay attacks.

F. Resistance of Impersonation and Man-in-the-Middle Attacks

An attacker may impersonate a legal user by forging an authentication request. However, available private keys (e.g., (x_i, A_i)) are only mastered by legal users, an attacker without a valid private key is unable to forge a valid signature (e.g., σ_{U_i}) with non-negligible probability. Therefore, the attacker cannot impersonate a legal user. In addition, FLEO makes a signature σ_{FLEO} for each message M_{FLEO}. The impersonation for a legal FLEO would be failed, when the user checks the signature by algorithm $EC.Verify(pk_{FLEO}, \sigma_{FLEO})$, where the signing key for σ_{FLEO} is only held by legal FLEO. Thus, AnFRA is secure against impersonation attacks.

A man-in-the-middle attacker tries to trick two parties into a three-party communication. According to the proof of impersonation attacks, a man-in-the-middle attacker fails to impersonate both a legal user to FLEO and a legal FLEO to the user. Therefore, our protocol is secure against the man-in-the-middle attacks.

VII. PERFORMANCE ANALYSIS

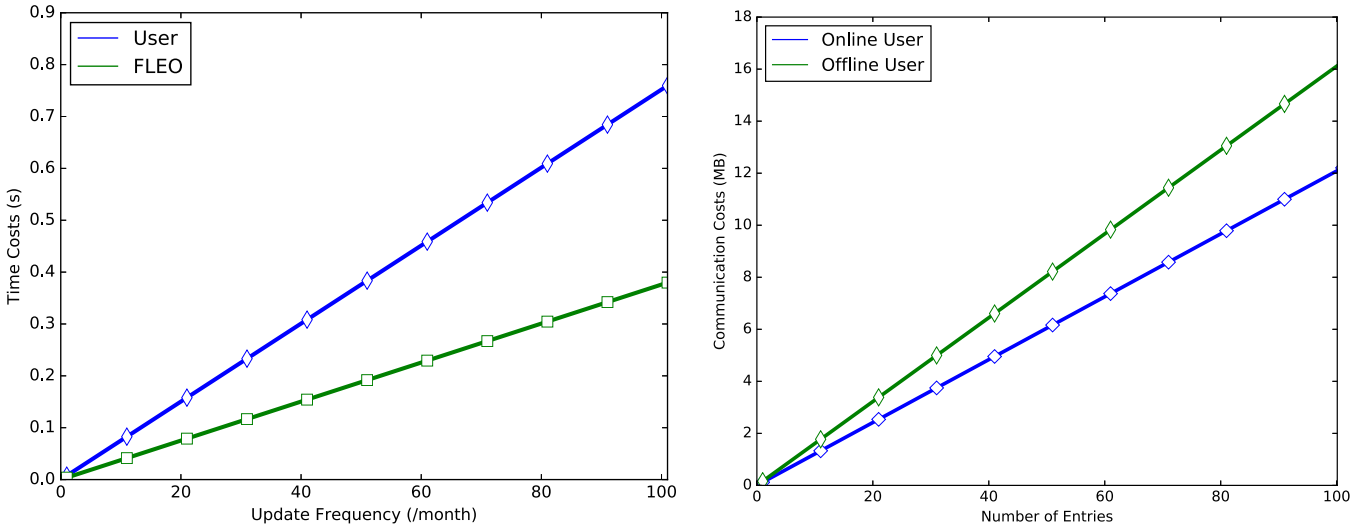
In this section, we analyze the performance of our scheme for authentication delay, communication overhead and revocation overhead.

A. Authentication Delay

The authentication delay is defined as the total time costs during the whole authentication process, including the time costs of computations and signal propagation. In this paper, we denote the time costs of signal propagation between the user and FLEO, FLEO and FGS, FGS and HNCC as $T_{U\text{-}FL}$, $T_{FL\text{-}FGS}$, $T_{FGS\text{-}HNCC}$, respectively. Since the FLEOs are 500 to 2,000 kilometers away from ground [10], it is reasonable to set $T_{U\text{-}FL} = T_{FL\text{-}FGS} = 10ms$ and $T_{FGS\text{-}HNCC} = 5ms$. We investigate the time costs of the primitive cryptography operations using OpenSSL library [37] on Intel P IV 3 GHz processor. And the experiment results in [26] show that the time costs for performing a pairing operation, multiplication, and exponentiation are $T_{mul} = 0.376\ ms$, $T_{exp} = 0.387ms$ and $T_{pair} = 11.903ms$, respectively.

Based on these information, we compares the authentication delay in AnFRA and the related work [8], [19]–[21], [23], [27] in Table I. It is noted that all these related works are not originally designed for roaming authentication in SIN, so we make some appropriate modifications for them. In general, the verifier in [8], [19], and [20] is moved to HNCC so that users' sensitive information (e.g., real identity) won't be leaked to foreign network entities, and the verifier in [21], [23], and [27] is moved to FGS to reduce the authentication delay while protecting users' privacy. From the table, it can be seen that a successful roaming authentication in AnFRA needs 14 multiplication operations, 6 exponentiation operations, 1 pairing operation, and 2 signal propagation time between user and FLEO. Totally, it requires almost $40ms$ for a roaming authentication, which is significantly faster than the related works.

Additionally, we give the comparison of the computation costs for components with the related works. Most three-party authentication schemes only use the lightweight cryptography



(a) (b)

Fig. 7. Revocation overhead. (a) Computation costs of revocation. (b) Communication costs of revocation.

TABLE II
COMPARISON OF COMPUTATION COSTS FOR COMPONENTS

	User	FLEO	FGS	Total
[21]	1.139ms	-	13.407ms	14.546ms
[23]	1.548ms	-	25.31ms	26.858ms
[27]	101.992ms	-	77.81ms	179.802ms
AnFRA	4.169ms	14.546ms	0.774ms	19.489ms

TABLE III
COMPARISON OF COMMUNICATION OVERHEAD

	User-FLEO	FLEO-FGS	FGS-HNCC	Total
[8]	3272	3272	3172	9716
[19]	2248	2248	2348	6844
[20]	3272	3472	≥ 0	≥ 6744
[21]	3812	3812	0	7624
[23]	3568	3568	0	7136
[27]	940	940	0	1880
AnFRA	1600	880	0	2480

*The communication overhead is represented in bits.

algorithm, such as hash, symmetric encryption. Their computation costs can be negligible when compared to pairing operation. Therefore, we just compare our work with some two-party authentication schemes as in Table II. From the table, we can see that the total computation costs for our scheme is more efficient than [23] and [27], and closer to [21].

B. Communication Overhead

To compare our scheme with the above different authentication schemes in terms of communication overhand, we set the length of all identities and timestamps as 100 bits, the length of random numbers and encryption messages as 1024 bits, and all signatures and $|\mathbb{G}|$ are 160 bits. Based on these assumptions, we compare the communication overhead in terms of User-FLEO, FLEO-FGS, FGS-HNCC and Total respectively. The results are shown in Table III. It can be seen that the proposed AnFRA is more efficient than most of the related works in terms of User-FLEO, FLEO-FGS, FGS-HNCC, or Total.

C. Revocation Overhead

As shown in the dynamic user enrollment and revocation phase in Section V-B.5, a user needs to perform 2 multiplication operations to update its private key, while a FLEO requires one multiplication operation to update the public verifying key. And the FGS and HNCC do not need to perform any computing operation. Fig. 7(a) shows the computation overhead of revocation for a user and FLEO (assume 10 users are revoked one time). It is noted that our scheme is efficient for the user and FLEO, only $0.75s$ will be cost for a user during a month when the update frequency is 100 per month, and FLEO is less. For evaluating the total communication costs for revocation overhead of the whole system, we depict Fig. 7(b) to show the variation of total communication costs in terms of the number of revocation entries in RL, where the elements in $\mathbb{G}$ and $\mathbb{Z}_p$ are 160 bits, and an additional index in RL is 10 bits. It can be seen that the whole system's communication costs are increasing with the increase of entries number. However, it is acceptable since only approximately 12 MB costs for an online user and 16 MB costs for an offline user when the number of entries in RL is 100.

VIII. CONCLUSION

Space information network (SIN) can break regional restrictions and provide wider coverage comparing with traditional Internet. The trend of roaming to SIN will be a new feature of the future network, which calls for designing a new roaming authentication scheme for SIN. While challenges exist for designing a roaming authentication system for SIN due to its special environment (e.g., the dynamic and unstable topology,

the highly exposed links, the long latency). Motivated by the importance of user authentication delay and anonymity for roaming in SIN, we design an anonymous and fast roaming authentication protocol (named AnFRA). In AnFRA, we utilize the group signature and emphasize the authentication of foreign LEO (FLEO), that means the FLEO can directly authorize roaming users to access the foreign network without the realtime involvement of home network control center (HNCC) and without privacy disclosure. Moreover, a revocation mechanism designed specifically for the system is incorporated into the roaming authentication scheme to support users revocation. Although a small amount of overhead is brought in owing to the revocation mechanism, it can largely reduce the authentication delay. In addition, the system satisfies a set of more strict security features, while enjoys a lower authentication delay and less communication overhead.

ACKNOWLEDGMENT

The authors sincerely thank the anonymous referees for their valuable suggestions that have led to the present improved version of the original manuscript.

REFERENCES

[1] M. Perry, K. O'hara, A. Sellen, B. Brown, and R. Harper, "Dealing with mobility: Understanding access anytime, anywhere," *ACM Trans. Comput.-Hum. Interact.*, vol. 8, no. 4, pp. 323–347, 2001.

[2] 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.

[3] G. Miao, J. Zander, K. W. Sung, and S. B. Slimane, *Fundamentals of Mobile Data Networks*. Cambridge, U.K.: Cambridge Univ. Press, 2016.

[4] Q. A. Arain *et al.*, "Privacy preserving dynamic pseudonym-based multiple mix-zones authentication protocol over road networks," *Wireless Pers. Commun.*, vol. 95, no. 2, pp. 505–521, 2017.

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

[6] T. B. Zahariadis, K. G. Vaxevanakis, C. P. Tsantilas, N. A. Zervos, and N. A. Nikolaou, "Global roaming in next-generation networks," *IEEE Commun. Mag.*, vol. 40, no. 2, pp. 145–151, Feb. 2002.

[7] F. Li, L. Yang, W. Wu, L. Zhang, and Z. Shi, "Research status and development trends of security assurance for space-ground integration information network," *J. Commun.*, vol. 37, no. 11, pp. 156–168, 2016.

[8] Y. Jiang, C. Lin, X. Shen, and M. Shi, "Mutual authentication and key exchange protocols for roaming services in wireless mobile networks," *IEEE Trans. Wireless Commun.*, vol. 5, no. 9, pp. 2569–2577, Sep. 2006.

[9] P. Gope and T. Hwang, "Lightweight and energy-efficient mutual authentication and key agreement scheme with user anonymity for secure communication in global mobility networks," *IEEE Syst. J.*, vol. 10, no. 4, pp. 1370–1379, Dec. 2016.

[10] I. F. Akyildiz, H. Uzunalioğlu, and M. D. Bender, "Handover management in low earth orbit (LEO) satellite networks," *Mobile Netw. Appl.*, vol. 4, no. 4, pp. 301–310, 1999.

[11] D. He, J. Bu, S. Chan, C. Chen, and M. Yin, "Privacy-preserving universal authentication protocol for wireless communications," *IEEE Trans. Wireless Commun.*, vol. 10, no. 2, pp. 431–436, Feb. 2011.

[12] G. Yang, Q. Huang, D. S. Wong, and X. Deng, "Universal authentication protocols for anonymous wireless communications," *IEEE Trans. Wireless Commun.*, vol. 9, no. 1, pp. 168–174, Jan. 2010.

[13] J. S. Warner and R. G. Johnston, "GPS spoofing countermeasures," *Homeland Secur. J.*, vol. 25, no. 2, pp. 19–27, 2003.

[14] J. Lei, Z. Han, M. Á. Vazquez-Castro, and A. Hjorungnes, "Secure satellite communication systems design with individual secrecy rate constraints," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 661–671, Sep. 2011.

[15] J. A. Larcom and H. Liu, "Modeling and characterization of GPS spoofing," in *Proc. IEEE Int. Conf. Technol. Homeland Secur. (HST)*, Nov. 2013, pp. 729–734.

[16] 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.

[17] H. Cruickshank, "A security system for satellite networks," in *Proc. 5th Int. Conf. Satell. Syst. Mobile Commun. Navigat.* Edison, NJ, USA: IET, May 1996, pp. 187–190.

[18] M.-S. Hwang, C.-C. Yang, and C.-Y. Shiu, "An authentication scheme for mobile satellite communication systems," *ACM SIGOPS Oper. Syst. Rev.*, vol. 37, no. 4, pp. 42–47, 2003.

[19] C.-L. Chen, K.-W. Cheng, Y.-L. Chen, C. Chang, and C.-C. Lee, "An improvement on the self-verification authentication mechanism for a mobile satellite communication system," *Appl. Math.*, vol. 8, no. 1L, pp. 97–106, 2014.

[20] W. Zhao, A. Zhang, J. Li, X. Wu, and Y. Liu, "Analysis and design of an authentication protocol for space information network," in *Proc. Mil. Commun. Conf. (MILCOM)*, Nov. 2016, pp. 43–48.

[21] J.-L. Tsai and N.-W. Lo, "Provably secure anonymous authentication with batch verification for mobile roaming services," *Ad Hoc Netw.*, vol. 44, pp. 19–31, Jul. 2016.

[22] D. Wang, H. Cheng, D. He, and P. Wang, "On the challenges in designing identity-based privacy-preserving authentication schemes for mobile devices," *IEEE Syst. J.*, vol. 12, no. 1, pp. 916–925, Mar. 2018.

[23] H. J. Jo, J. H. Paik, and D. H. Lee, "Efficient privacy-preserving authentication in wireless mobile networks," *IEEE Trans. Mobile Comput.*, vol. 13, no. 7, pp. 1469–1481, Jul. 2014.

[24] I. Memon, M. R. Mohammed, R. Akhtar, H. Memon, M. H. Memon, and R. A. Shaikh, "Design and implementation to authentication over a GSM system using certificate-less public key cryptography (CL-PKC)," *Wireless Pers. Commun.*, vol. 79, no. 1, pp. 661–686, 2014.

[25] I. Memon, I. Hussain, R. Akhtar, and G. Chen, "Enhanced privacy and authentication: An efficient and secure anonymous communication for location based service using asymmetric cryptography scheme," *Wireless Pers. Commun.*, vol. 84, no. 2, pp. 1487–1508, 2015.

[26] 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.

[27] J. K. Liu, C.-K. Chu, S. S. M. Chow, X. Huang, M. H. Au, and J. Zhou, "Time-bound anonymous authentication for roaming networks," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 1, pp. 178–189, Jan. 2015.

[28] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," in *Proc. Annu. Int. Cryptol. Conf.* Berlin, Germany: Springer, 2001, pp. 213–229.

[29] S. D. Galbraith, K. G. Paterson, and N. P. Smart, "Pairings for cryptographers," *Discrete Appl. Math.*, vol. 156, no. 16, pp. 3113–3121, 2008.

[30] *Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)*, document ANSI X9.62, 1999.

[31] X. Wang, Y. L. Yin, and H. Yu, "Finding collisions in the full SHA-1," in *Proc. Annu. Int. Cryptol. Conf.* Berlin, Germany: Springer, 2005, pp. 17–36.

[32] N. Sklavos and O. Koufopavlou, "On the hardware implementations of the SHA-2 (256, 384, 512) hash functions," in *Proc. Int. Symp. Circuits Syst. (ISCAS)*, May 2003, pp. V-153–V-156.

[33] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Commun. ACM*, vol. 21, no. 2, pp. 120–126, Feb. 1978.

[34] M. Horemuž and J. V. Andersson, "Polynomial interpolation of GPS satellite coordinates," *GPS Solutions*, vol. 10, no. 1, pp. 67–72, 2006.

[35] D. Boneh and X. Boyen, "Short signatures without random oracles," in *Proc. Int. Conf. Theory Appl. Cryptograph. Techn.* Berlin, Germany: Springer, 2004, pp. 56–73.

[36] W. Diffie and M. E. Hellman, "New directions in cryptography," *IEEE Trans. Inf. Theory*, vol. IT-22, no. 6, pp. 644–654, Nov. 1976.

[37] OpenSSL. Accessed: 2018. [Online]. Available: http://www.openssl.org

Qingyou Yang received the B.S. degree in information security from the School of the Gifted Young, University of Science and Technology of China (USTC), in 2016, where he is currently a graduate student in communication and information system with the Department of Electronic Engineering and Information Science. His research interests include network security and cryptography.

Kaiping Xue (M'09–SM'15) received the B.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 2012 to 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 Department of Information Security and the Department of EEIS, USTC. His research interests include next-generation Internet, distributed networks, and network security.

Jie Xu received the B.S. degree from the Department of Information Security, University of Science and Technology of China (USTC), in 2017. She is currently a graduate student in communication and information system with the Department of Electronic Engineering and Information Science, USTC. Her research interests include network security and cryptography.

Jiajie Wang received the B.S. degree from the Department of Information Security, University of Science and Technology of China (USTC), in 2004, and the Ph.D. degree from the Department of Computer Science and Technology, USTC, in 2009. He is currently an Associate Researcher with the National Engineering Laboratory for Mobile Network Security and the China Information Technology Security Evaluation Center. His research interests include mobile security, next-generation mobile network, and artificial intelligence.

Fenghua Li received the B.S. degree in computer software, and the M.S. and Ph.D. degrees in computer systems architecture from Xidian University in 1987, 1990, and 2009, respectively. He is currently a Professor and a Doctoral Supervisor with the State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences. He is also a Doctoral Supervisor with Xidian University. His current research interests include network security, system security, privacy computing, and trusted computing.

Nenghai Yu received the B.S. degree from the Nanjing University of Posts and Telecommunications, Nanjing, China, in 1987, the M.E. degree from Tsinghua University, Beijing, China, in 1992, and the Ph.D. degree from the University of Science and Technology of China (USTC), Hefei, China, in 2004. Since 1992, he has been a Faculty Member with the Department of Electronic Engineering and Information Science, USTC, where he is currently a Professor. He is the Executive Director of the Department of Electronic Engineering and Information Science, USTC, and the Director of the Information Processing Center, USTC. He has authored or co-authored over 130 papers in journals and international conferences. His research interests include multimedia security, multimedia information retrieval, video processing, and information hiding.