IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received December 12, 2019, accepted January 3, 2020, date of publication January 8, 2020, date of current version January 17, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2964804

Fog Service in Space Information Network: Architecture, Use Case, Security and Challenges

JUNYAN GUO AND YE DU

Beijing Key Laboratory of Security and Privacy in Intelligent Transportation, Beijing Jiaotong University, Beijing 100044, China

Corresponding author: Ye Du (ydu@bjtu.edu.cn)

This work was supported by the Natural Science Foundation of China under Grant 61672092.

ABSTRACT As a large heterogeneous information infrastructure, space terrestrial coinformation network provides a reliable and effective services for all types of space-based users, aviation users, marine users and land-based users through satellite networks. However, the precious computing and storage resources of satellite nodes during the service life is not fully exploited, and the enormous potential of the space information network (SIN) needs to be tapped to provide personalized services to end users. In this paper, to improve the utilization of satellite node resources and better meet the real-time requirements of compute-intensive and delay-sensitive users, we propose the SIN fog service. SIN fog service is an extension of fog service paradigm. The visionary concept is to integrate the computing power of satellite network edge nodes, enabling a wide range of benefits, including enhanced computing power, decreased bandwidth, reduced latency and without the need to lay complex and expensive ground networks, which can be widely developed in location navigation, environmental detection, traffic management, anti-terrorism, etc. We present the architecture and a potential use case of the SIN fog service. Then we discuss several related key security and challenges and finally the anti-quantum and efficient mutual-authentication protocol is introduced.

INDEX TERMS Space information network, fog service, architecture, security.

I. INTRODUCTION

Space information network (SIN) is a globally heterogeneous network that includes satellite backbones, high-altitude platforms, aircraft, terrestrial control stations, and ground communications equipment. With the rapid development of satellite communication and computing power in recent years, SIN has been able to provide a globally reliable communication network for communication equipment via satellite networks [1]. Currently, the delay from terrestrial communication equipment to its visible Low earth orbit (LEO) satellites can be reduced to 1 to 4 ms [2], which can meet the user's quality of service (QoS) requirement. Compared with the traditional communication network, SIN has the natural advantage and is not restricted by the region. Even if the communication equipment is not connected to the traditional mode of communication in the ocean, desert or mountain areas, reliable communication can be established through visible satellites. During the operation of the SIN, the built-in computing and storage modules of satellites can provide users with navigation, ground observation and other stability services. Although SIN can provide a wide variety of services, the onboard computing and storage capabilities are not fully utilized during operation, and there are still idle resources to be exploited.

Currently, sensors and computing devices have been widely used in terminal devices, it is estimated that more than 20.8 billion smart devices will be available by 2020 [3]. The large-scale application of smart devices and sensors leads to the generation of big data and complex computing, and the additional requirements for storage and computing power are caused by the limitations of their own devices. Although the centralized cloud with unlimited computing and storage capacity can meet the on-demand supply resources of the device, it cannot meet the requirements for real-time and resource mobility. Fog service is the extension of cloud paradigm, which solves the above application requirements by integrating the resources of the network edge nodes to greatly reduce the delay.

In order to improve the utilization of satellite nodes in SIN and to meet the needs of compute-intensive and

The associate editor coordinating the review of this manuscript and approving it for publication was Jiafeng Xie.

delay-sensitive applications, we proposed SIN fog service. In SIN fog service, the user is the smart device that applies for the fog service through the satellite-ground link, and the LEO satellite that provides the service will act as the server of SIN fog service. The relative movement between satellites, between satellites and users leads to complex task exchange procedures and user access issues between fog nodes. To simplify the complexity caused by relative movement, we introduced the concept of logical regions and virtual nodes.

The reminder of this paper is organized as follows: The motivation is presented in Section II, the SIN fog service architecture and details of the proposed mechanism in Section III, and a potential use case in Section IV. We present the related work on security and challenges in Section V. In Section VI, we introduce the anti-quantum and efficient mutual-authentication protocol for SIN fog service. Finally, we make some concluding in Section VII.

II. MOTIVATION

Our proposal on SIN fog service is motivated by the fog service, global distribution of SIN and user-perceived delay.

A. FOG SERVICE

Cloud service solves the problem of insufficient computing and storage capacity of individuals or organizations by centralizing high-performance computing devices and storage units, and provides users with three levels of services, namely Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS). The cloud makes computing and storage resources have become cheaper, more available than ever before [4]. However, the cloud involves the following issues due to intrinsic properties.

- The cloud is usually far away from the user.
- Need a stable and high-quality communication environment.
- Communication delay that cannot be ignored.
- Cannot ensure the security of intermediate nodes of the transmission link.
- A large number of requests in a short period of time can cause excessive capacity of the network link, which cannot guarantee QoS, especially in near-cloud links.

Due to these shortcomings, the cloud cannot be effectively utilized by users for security and real-time requirements. The fog service was first introduced by Cisco to solve the shortcomings of the cloud. From another perspective, the fog service is an extension of the cloud. Distributed network edge devices are integrated into a highly virtualized platform to provide computing power to the user [5]. The edge device is closer to the data generating node, and the data are limited to being processed locally while the latency is greatly reduced. Fog service can significantly improve QoS, meet real-time, secure and location-sensitive application requirements. At present fog service has been proposed in IoT [6], Wearable devices [7], Smart Grid [5], Smart Home [8] and VANET [9]. Although the fog service is still in its early stage, it has proved to be an excellent solution to reduce network load, resource decentralization and make full use of network node resources in above application scenarios.

B. SPACE INFORMATION NETWORK

In recent years, China has launched a national key research project on the development of SIN [10]. As an integrated information infrastructure, SIN provides global coverage and information support for various types of services. It has been widely used in real life because of its communication advantages anytime and anywhere. As an important part of SIN, satellites are distributed in different orbits to support global wireless communications via inter-satellite links and satellite-terrestrial links. In an extreme geographical environment, the scope of the harsh geographical environment is large, and the communication environment complex, it is uneconomical to build a traditional ground communication system only for a small number of users under this region [11]. However, in sparsely populated areas, satellite communications are a relatively inexpensive means of communication compared with building a base station every few kilometers on the ground but not affected by earthquakes and floods. The global communication of device only needs to be within the coverage of the communication satellite. There are already several satellite communication networks supporting global communication such as: Iridium [12], ISICOM [13] and TSAT [14]. In addition, in the battlefield environment, terrestrial communication facilities are easily destroyed by adversaries, and satellite communications have more potential to support communication and provide services.

C. USER-PERCEIVED DELAY

We first try to consider the introduction of the cloud service in SIN, but the cloud in SIN has the following challenges:

- Satellite network bandwidth is heavily overloaded.
- Satellite nodes cannot afford long-term big data forwarding.
- The inherent properties of the cloud lead to the degradation of the performance and life-time of SIN.

In addition, latency is the most important for the user. In the case of the cloud service in SIN, the communication latency includes not only the transmission time between the end user to the satellite, the time of multi-hop transmission to the remote satellite but also the remote satellite to the cloud server. However, in the case of the fog service in SIN, the communication latency only includes the transmission time between the end user to the satellite, and the satellite to the adjacent satellites. When dealing with delay-sensitive tasks, the fog service can meet the QoS more than the cloud and greatly reduces the user-perceived delay. So we think the fog service as an effective solution to replace the cloud in SIN and proposed SIN fog service.

While satellite resources (eg, energy, service life) are extremely scarce resources, it is worthwhile to pro-

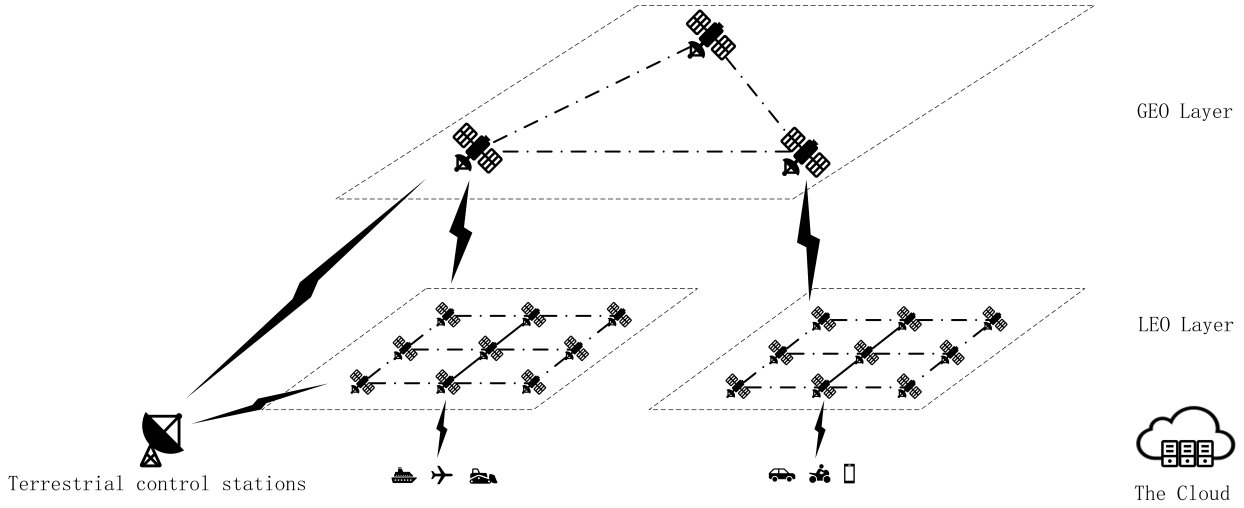


FIGURE 1. Architecture of SIN fog service.

vide much-needed computing, storage, and communication services to military actions or key government officials, especially for the user in an imperfect terrestrial infrastructure environment. In addition, each fog node can still act as the local cloud within the signal coverage, providing navigation, observation, and more services to local smart devices.

III. SIN FOG SERVICE ARCHITECTURE: OVERVIEW

A. ARCHITECTURE

As shown in Fig. 1, the architecture of SIN fog service includes a total of four types of entities: users, satellite nodes, the cloud and terrestrial control stations.

1) USER

The user in the SIN fog service is the smart device with sensors, computing, storage, and the ability to communicate with satellites. The smart device does not remain stationary in the SIN but mobile, which can be a slow-moving wearable device or an airplane flying at high speed of 200 meters per second. These devices continuously collect large amounts of data through sensors and network connections during operation. Non-latency-sensitive applications can be stored locally or uploaded to the cloud regardless of time overhead, and then analyze the data as the enough computing resources are available. For latency-sensitive applications, the large amounts of data need to be processed in real time to help decision-making. For example, in the construction machinery construction process, it is necessary to predict any possible accidents in a short period of time, the aircraft needs to predict the safety of the entire route and adjust the route in the flight process, and the mid-air command center needs to process a large amount of data for battlefield scheduling. Devices that do not have complex computing and big data storage are the primary users of SIN fog service.

2) SATELLITE NODE

SIN fog service treats satellite nodes as fog nodes, including two types: Geostationary orbit (GEO) satellites and LEO satellites. The LEO satellites periodically move around the Earth, closer to the ground, have lower communication delays, and use LEO satellites as an access for smart devices. In the SIN fog service, the LEO satellite has three functions:

- Establish a connection with the smart device through the satellite-ground link, and receive the computing tasks submitted by the smart device.
- Establish a connection with the adjacent satellite node, distribute the task to the adjacent satellite node and wait to receive the return result.
- Compute the submitted task and return the result.

The LEO layer fog nodes are classified into access point and idle neighbor node according to different functions.

The access point is the fog node that receives tasks of smart device in its coverage area through satellite-ground links. The idle neighbor node are the fog nodes with residual computing power connected to the nearby access point via an inter-satellite links. When the access point cannot complete the task of the smart device in a short time, the task needs to be decomposed into multiple smaller tasks. Then assign the small tasks to the idle neighbor node separately. The task undertaken by the idle neighbor node may also exceed the computing power. At this time, the idle neighbor node will act as the new access point to further divide the task and allocate it to the other idle neighbor node.

GEO node is the satellite far from the ground, which can cover a larger area, and is relatively static compared to the ground. More importantly, GEO satellite has stronger computing, communication and storage capacity than LEO satellite. Each GEO satellite as the fog node manager in its coverage area, assumes the following roles:

- Be responsible for coordinating task scheduling in the region.
- Monitor the LEO fog node in the management domain for any abnormality, and remove the abnormal node from the management area.
- When the LEO fog node breaks down, it coordinates another redundant LEO satellite to take over the function of the LEO fog node and the unfinished task.
- Report LEO fog nodes operation data to terrestrial control station.

3) THE CLOUD

The cloud has unlimited computing and storage capabilities. As a higher-level computing center, the cloud reduces the computational overhead of the SIN fog node. The task of non-delay-sensitive applications, the calculation and storage capabilities beyond the SIN fog layer can be handed over to the cloud to optimize network performance, improve the throughput and extend the life-time of SIN satellite nodes. The cloud can use a more complex, accurate and time-consuming algorithm to perform deeper analysis on the data received by the user or the fog node, and optimize the entire space information network from a holistic perspective.

4) TERRESTRIAL CONTROL STATION

Terrestrial control station has the ability to communicate with GEO satellites and LEO satellites, and monitors the entire space information network. It has the highest control level and can send control commands to the satellite. Terrestrial control station is not a single site but logically scattered on the ground.

B. OVERVIEW FOG SERVICE PROCESS IN SPACE INFORMATION NETWORK

As illustrated in Fig. 2, SIN fog service is divided into three layers according to its computing power: data generation layer, fog layer and cloud layer. The data generation layer is composed of a variety of smart devices which are responsible for collecting data through sensors and communication networks. Some simple calculations can be processed on the device itself. In case the device with finite computing and storage capabilities demands to process large amounts of data and complex calculations, it's necessary to upload data and computing tasks to the fog layer. The LEO fog node analyzes and processes the data sent by the smart device, and returns the result after the calculation is completed. When the data volume exceeds the fog layer computing capability, the data and computing tasks are submitted to the remote cloud. According to the computing power of each layer of equipment, the order should be: data generation layer $<$ fog layer $<$ cloud layer.

C. VIRTUAL LOCATION

Before the smart device requests the fog service, it needs to establish a continuous connection with the LEO fog node. Since the LEO satellite moves at a high-speed relative to the

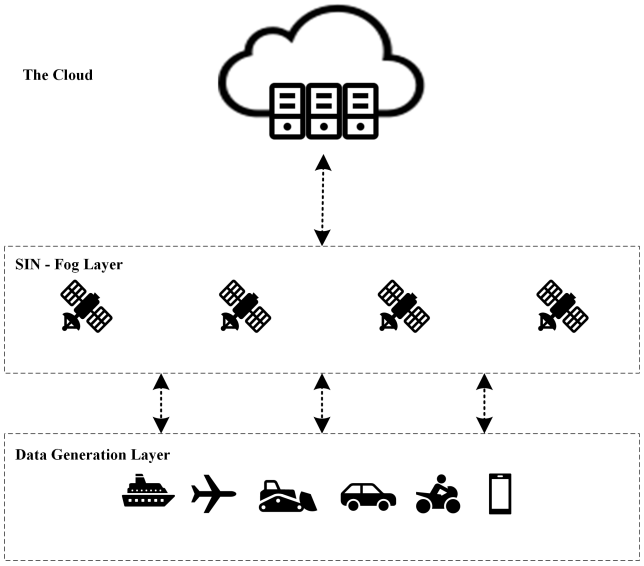


FIGURE 2. Space information network fog service three-layer structure.

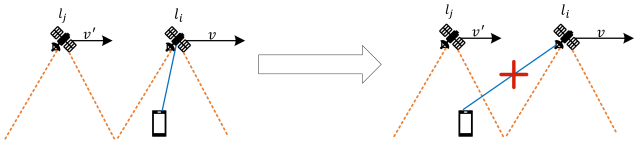


FIGURE 3. Relative motion between satellite and smart device.

smart device, there are issues of access switching and task delivery. As shown in Fig. 3, the smart device first establishes connection with the satellite l_i, submits the computing task. However, continuous movement of the satellite l_i at a relative speed v causes the smart device to be disconnected because it is not within the coverage of the satellite signal. In order to continuously obtain fog service, smart devices will involve access handoff, that is, re-access the next LEO fog node l_j whose signal covers the smart devices. But when the l_i disconnects from the smart device, it still stores the data and computing tasks of the smart device and soon receive the computing and storage tasks of other smart devices in the new service area. In the event of the satellite l_i cannot transfer the computational and storage tasks to l_j before disconnecting from the smart device, during the periodic motion of satellite l_i around the earth, it will cause the satellite l_i to contain calculation and storage tasks of multiple regions, resulting in the satellite l_i nodes overload, and even the whole SIN fog service disorder. With thousands of LEO satellites in SIN and a variety of end users, the relative mobility between satellites and users can lead to complex, messy task delivery. For this reason, the concept of virtual node is introduced, which was originally proposed by [15] to construct satellite network routing. In this paper, we introduce virtual nodes to simplify the complexity of task delivery with the following advantages:

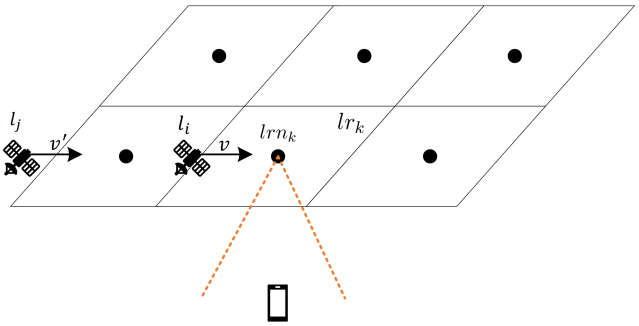


FIGURE 4. Virtual node.

- It facilitates the task management of fog nodes.
- Virtual node represents the calculation and storage tasks of the fixed area.
- Shield the high-speed motion of LEO satellite nodes.

Assume that the surface of the earth is completely covered by the logical area and is represented by $LR = \{lr_1, lr_2, \ldots, lr_m\}$, m is the number of logical regions. The principle of logical area division is that when the satellite is operating in a logical area, it has a stable communication link with satellites in adjacent logical areas. As shown in Fig. 4, the midpoint of the logical region lr_k is the virtual node of this region, which is represented by lrn_k. The LEO satellite l_i nearest to the lrn_k represents the logical region lr_k. Due to mobility, LEO satellite l_i move between logical areas and serve smart devices in their logical area. When the LEO satellite l_i moves out of the logical area lr_k, the unprocessed task from the smart device is timely transmitted to the next satellite l_j representing the virtual node during the task handover time. There are two situations in the satellite l_i delivery task:

- To the next satellite l_j. The satellite l_i successfully establishes the connection with the next satellite l_j representing the region and delivers the tasks to l_j within the allowed time. Finally, the tasks are completed by l_j.
- To the GEO manager node. When the GEO manager node detect the next satellite l_j failure within the time limit, and it is necessary to report the fault about l_j to l_i. l_i then will transmit the computing and storage tasks to the GEO manager node which next act as the user's access node and as an intermediate node to transfer the tasks to another redundant LEO satellite. After the task is completed, the redundant LEO satellite sends the result to GEO manager node, and finally returns to the user by GEO manager node.

Using static virtual nodes to represent dynamic mobile LEO satellites, can more intuitively observe the transfer of tasks in fog service of space information network. If the smart device does not leave the range of the logical area lr_k, the smart device remains logically connected to the fixed virtual node lrn_k. The LEO satellite which representing the virtual node lrn_k contains all the data and computing tasks in the logical region. In addition, the use of virtual nodes has the advantage of saving satellite scarce resources. In the

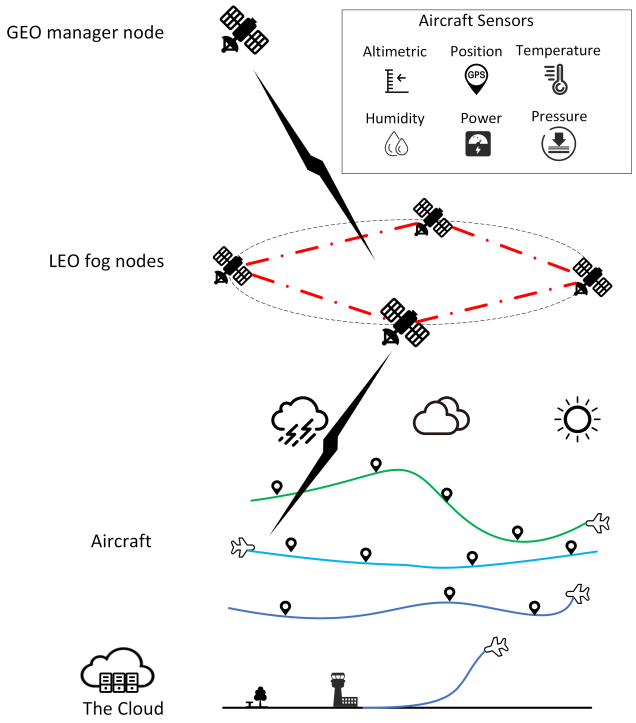


FIGURE 5. Example application of SIN fog service.

satellite network without virtual nodes, due to the high-speed relative motion between satellites, the communication link is not always reliable. In order to ensure that the message can reach the destination node, it is necessary to detect the link reachability and evaluate the link quality before each message is transmitted, which will increase the energy cost of the communication satellite and reduce the service life of the satellite. In satellite networks that introduce virtual nodes, every LEO satellites have reliable communication links with satellites in adjacent logical areas, and do not require extra overhead for link diagnosis.

IV. A POTENTIAL USE CASE: A FOG-ASSISTED FLIGHT SYSTEM

The flight system of the aircraft is to measure whether the aircraft deviates from the route during flight, analyzes the route and the safety hazard during the flight. For higher flight reliability, safety and accuracy, these measurements must be computed in real time or in small time slices. As shown in Fig. 5, there are a wide variety of sensor devices on the aircraft: altimetric sensor, position sensor, temperature sensor, humidity sensor, power sensor, pressure sensor, and so on, utilizing these sensors to obtain weather conditions, latitude and longitude, GPS position and operating data of the fuselage components. In a single flight, the engine sensor generates more than 1 TB of data, while all other sensors generate more massive amounts of data. It is of utmost importance to analyze some of the key data on the aircraft during the flight.

For small computing, such as calculating whether the flight path deviates from the predetermined route, the computing

device on the aircraft can be used, and only the GPS position information and the flight altitude need to be acquired in real time and compared on the route. However, for a safer flight, accurate weather forecasting of the route, safety assessment of flight components needs precise computing of a large amount of data, which cannot meet the real-time requirement only depending on the computing power of the aircraft. SIN fog service can be used to reduce the computing and time overhead of the aircraft, and the data and computing tasks are sent to LEO fog nodes serving the region through satellite-ground links. By analyzing aircraft sensor data, the LEO fog node predicts route weather, engine and other component failure probabilities, alerts the aircraft that is about to encounter bad weather or flight safety hazards, and lets the aircraft land directly at the nearby airport. There are usually multiple aircraft flying in the LEO fog node coverage area. By integrating multiple aircraft data, the limitations on single-source data can be broken, and a higher level of range control can be achieved. LEO fog node can analyze the weather conditions and safety hazards in a larger area. When the aircraft on the route encounters or predicts that it will face thunderstorms, the LEO fog node can also timely adjust the flight trajectories of other aircraft in the LEO coverage area. When the number of aircraft covered by LEO fog node is small, the single LEO node can be processed by its own computing and storage capabilities. However, when the LEO satellite serves too many aircraft, the LEO satellite will collect too many data and take on more computational tasks. If the task is still computed by a single LEO fog node, it will exceed the computation amount of the satellite, increasing the power consumption and the time consuming of the task. In order to solve real-time demand for the aircraft, the LEO fog nodes form a fog group according to the link quality and distance with adjacent LEO satellites. The LEO fog node requesting other satellite assisted computing acts as the access point, and the other LEO nodes of the fog group act as the idle neighbor node. The tasks will be divided by the access point and distributed to the idle neighbor node through the inter-satellite link.

V. SECURITY AND CHALLENGE

Although in recent years, the technology of SIN has been the focus of research, it still focuses on the usability research of SIN, and the research on the security is often neglected. In addition, the fog service is still in the early stage and the security mechanism is not sound. Without considering the mobility and geo-distribution of fog nodes, the cloud security mechanisms are directly applied in fog service, which will cause fog node crash and network congestion, and even lead to new security issues. Even if there have been studies on the security of fog services, such as: [16]–[19] etc., due to the faster mobility, higher heterogeneity and global coverage of SIN, these mechanisms still require a lot of experimentation to verify the security, confidentiality, and reliability in SIN fog service. In this section, we first discuss SIN fog service places the requirements on the security baseline and some possible solutions to enhance security for physical security, access authentication, secure communication, privacy preservation and non-repudiation. Next the challenges is introduced. Finally, we propose an anti-quantum and efficient mutual-authentication protocol between nodes for SIN fog service.

TABLE 1. Threat model in sin fog service.

Entity	Trust level
Terrestrial control station	Trusted
The cloud	Semi-trusted
The fog node	Semi-trusted
End user	Malicious

Before discussing security requirements in detail, we still need to give the threat model in SIN fog service. As shown in table 1, SIN fog service defines threat models for four types of entities: terrestrial control station, the cloud, satellite fog node and end user. The terrestrial control station is a trusted entity equipped with the highest level of deployment defense mechanisms for detecting abnormal behaviors, and any abnormal behavior can be detected and resisted. The cloud and satellite fog nodes are assumed to be a semi-trusted entity [16] that performs computing, storage, or communication tasks according to a pre-defined protocol, but is curious about the privacy information in the data. Since the end user is usually a smart device with weak computing power, it is easy to be attacked by adversary, so the end user is considered malicious. If the end user is compromised, the device will perform unauthorized access to the fog node according to the instructions of the adversary, and even obtain the fog node service as a legitimate internal user.

A. PHYSICAL SECURITY

Physical security is mainly to protect satellite nodes, terrestrial control stations and other facilities in SIN fog service from signal jamming, eavesdropping and destruction [20].

Signal jamming is the artificial or natural electromagnetic interference of a communication device while transmitting data, and sometimes inevitably affects data transmission and even damages to satellites, such as jamming between satellite signals [21], sunspot outbreaks, etc. The anti-jamming technology mainly processes the data, the data carrier and the propagation mode to improve the signal-to-noise ratio of the receiving end, so that the receiving end can correctly receive the desired signal. At present, automatic gain control and frequency hopping has been adopted an important means of anti-jamming communication in the constellation of Milstar, AEHF and VSAT satellites [22]. Besides, [23] proposed a novel anti-jamming scheme by vector tracking loop and blind beamformer which can improve the reliability of satellite signal transmission and suppress interference. Reference [24] uses a naive Bayesian classifier to classify signals and detect jamming signals. The proposed algorithm can separate the required signals with low overhead.

The satellite channel is open, and eavesdroppers may be appearing in the satellite channel or terrestrial channel,

increasing the risk of information transmission [25]. Reference [26] attempts to improve the secrecy rate by decode-and-forward relay beams under multi-eavesdropper and imperfect channel state information. Preventing physical layer eavesdropping can also mainly achieved by frequency hopping spread spectrum, direct sequence spread spectrum, etc., but with new attack technology continues to develop, these key information protected by traditional technology has the possibility of being stolen.

Anti-destruction technology is the focus of research in SIN. It refers when satellite nodes and communication links fail or are attacked, they can continue to maintain network functions through adaptive adjustment. Anti-destruction technology research mainly focuses on the satellite constellation architecture and routing protocols. Reference [28] proposed a design method of anti-destruction network architecture. The method uses natural connectivity as an indicator to measure the invulnerability of the satellite network and the optimized network structure can be more reliable and robust than the traditional network structure. References [29], [30] proposed local repair routing protocols that restore network connectivity with as little network communication overhead and time as possible after a satellite node fails, increasing the availability of the network under frequent failures.

Satellite physical layer security issues can also occur in satellite internal components, [31] describes the message protocol vulnerabilities in the internal MIL-STD-15538 bus system and the three existing attack approaches. There are a large number of internal components in the satellite, and there may also be security issues.

B. ACCESS AUTHENTICATION

Access authentication is the first step for users to obtain services, which is not just the authentication of the user identity by the fog node, but the mutual authentication of both parties. The terrestrial control center is the trusted entity with the highest control right in SIN fog service. It has the right to grant access to other devices and to revoke the identity of the entity when it detects an intrusion. Access authentication is not only the authentication of legality, but also the entity's trusted level. Entities with higher levels of trust can obtain fog services with higher priority and higher privileges.

The constant change of the relative position between the satellite fog nodes causes the network to be re-established. In the re-establishing process, neighbor satellites are authenticated to prevent unauthorized satellites from accessing the SIN fog service and launching internal user attacks. The end user's computing power is scarce, and the satellite fog node needs to serve a whole area of the user, so the computational overhead of the access authentication algorithm needs to be limited. Similarly, in order to meet the real-time needs of users, the number of interactions in authentication process is necessary to reduced to meet the low latency. References [32]–[34] proposed three authentication schemes based on discrete logarithm, hash and XOR operation, bilinear pairing respectively. Among them, [34] is the first anonymous and roaming authentication for SIN. However, with the development of quantum computing, these authentication protocols have been proven to be compromised or the authentication protocol does not meet security requirements. In addition, considering that satellite fog services are often applied to sensitive key users, it is necessary to adopt anti-quantum authentication technology. At present, few scholars have proposed anti-quantum authentication protocols for SIN. The post-quantum cryptographic algorithm mainly relies on multivariate-based, code-based, and lattice-based, and these can be introduced into the authentication protocol to enhance the security and the anti-quantumity of the protocol.

C. SECURE COMMUNICATION

The characteristics of satellite wireless transmission expose the data and tasks transmitted between the end user and the fog node in space, therefore, attention should be paid to the protection of the data transmission process. Otherwise, any device with satellite signal receiving module can eavesdrop on the data. To protect the data security of end users and fog nodes, the cryptographic mechanism is applied to end-to-end data protection. The end user requests the service from anywhere, it is impossible to have the same symmetric key built in all the end users and the fog nodes to ensure the confidentiality of the data. In addition, due to the large number of end users, when a user is compromised, the entire network key update is required, which seriously increases the calculation and communication overhead of the network in a short time. References [34], [35] uses an asymmetric key to negotiate keys between nodes, and finally uses the symmetric key to encrypt inter-node interactive data. When communicating with a fixed node, only one key negotiation is needed, which can reduce the computational overhead and negotiation delay. However, in theory, one key at one time is the safest way, and using only a fixed key during the communication life cycle reduces the confidentiality. Reference [36] proposed a new one time key establishment protocol which can be used for three-party communication. The protocol only needs to exchange 4 times of information to negotiate a shared key. After performance analysis, the communication and computational cost of the protocol are reduced by about 20% compared to other protocols. In the SIN fog service, the computing resources of the satellite nodes are scarce and user-perceived delay should be as small as possible. This lightweight security communication protocols can be applied to the SIN to ensure more resources of the satellite to serve the users.

Secure communication not only guarantees the confidentiality of data but also protects data integrity. The end user storage capacity is limited, and it is impossible to store all the collected data for a long time. In order to ensure that the data are effectively utilized, the data are forwarded to the satellite fog node or the cloud. Once the data are transferred to other entities, the end user loses control of the data and cannot prevent other nodes from modifying the data. When the end user needs data previously stored in the fog node or the cloud,

it is difficult to verify the integrity of the downloaded data. The fog service is in the early stage of research and there are too few related studies, especially in the SIN environment. So the data integrity verification scheme in the cloud service can guide the data integrity research in the fog service environment. In the semi-trusted cloud service, [37] proposed a data integrity verification technology. The uploaded files are processed by attribute encryption and a cloud-based hash algorithm is used to generate a 512-bit hash values for each file. Only authorized users can access the required files by their own identity and hash value. Reference [38] describes a data integrity protection mechanism that utilizes crowdsourcing paradigm and does not require changes to the cloud service system. Although these mechanisms have some reference to the fog service, these mechanisms often do not focus on the overhead and cannot be directly applied to SIN fog service, there is still a need for a mechanism with less storage overhead and computational overhead.

D. PRIVACY PRESERVATION

The data collected by the end user through the sensor are the user-centered data, which can reveal where the user is, where the user is going, which areas are frequently accessed, and regular daily trajectories [39]. The semi-trusted fog node and the cloud can estimate the important privacy information of the user through the data uploaded by the terminal user, such as: the user's home address, preferences, religious beliefs, physical conditions and social relations, etc. If these sensitive-information is abused by semi-trusted or untrusted nodes in SIN fog service, it can trigger a wide range of serious social panic. The privacy preservation can be reflected in the phases of authentication access and data analysis. In the authentication access phase, in order to avoid the fog node identifying the user, an anonymous authentication scheme should be adopted, not only to authenticate the user's legal identity but also make the fog node unable to distinguish the specific user [34]. In the data analysis phase, the satellite node provides specific services through user-uploaded data. However, the data uploaded by the user may contain private information. If the sensitive data are not eliminated, the semi-trusted fog node can use the statistical methods, machine learning and other methods to mine the existing sensitive data. Introducing k-anonymity [40], l-diversity [41], and differential privacy [42] methods into the data-removal sensitivity process can effectively protect user privacy. K-anonymity and l-diversity need to define the background knowledge of the adversary, while the differential privacy does not rely on the background knowledge of the attacker but provides a rigorous proof of privacy theory [43], which has more application prospects in the SIN fog service.

E. NON-REPUDIATION

Non-repudiation requires that the trusted nodes have the ability to identify and track node behavior by collecting and analyzing data from end users and fog nodes. Even if the user requests pseudo-name or anonymous authentication when requesting SIN fog service for the purpose of privacy protection, the highest-permission terrestrial control station still has the ability to distinguish the specific identity of the user. For non-repudiation, it is also required that entities cannot deny what they have done and cannot acknowledge things that have not been done. If the entity in the SIN fog service is invaded to make destructive behavior, according to the non-repudiation, the terrestrial control station can take evidence and penalize the compromised nodes.

F. CHALLENGES

1) RESOURCE MANAGEMENT

In SIN fog service, the basic object of resource management is the computing, storage, and communication mobile resources that are carried on the satellite. However, due to the high heterogeneity of SIN and the high mobility of satellites, it poses a daunting challenge to network performance improvement. Reference [44] proposed to achieve an efficient multi-dimensional network resources and task QoS requirements in SIN, three aspects considered. First, the QoS requirements of the task need to be analyzed. Second, resources need to be classified according to different tasks. Finally, resources are allocated based on the QoS and type of the task. In SIN fog service, it is necessary to consider not only the above problems but also the mobile resources of the end users and the resource management under conditions of trusted and semi-trusted fog nodes, which will make the resource management more complicated.

2) ROUTING ALGORITHM

Globally distributed satellite fog nodes establish communications over inter-satellite links, requiring a network configuration that maintains high bandwidth levels, flexibility and scalability. The SIN routing algorithm should be able to establish and maintain network connectivity in two situations. First, a single satellite leaves the satellite network due to a fault or being compromised. Second, new satellites were launched and joined the satellite network. The routing algorithm of SIN should be able to calculate the communication paths with low computation and communication overhead, and update the routing in real time according to the network topology change. Many scholars in satellite networks have proposed many classical routing algorithms such as [45]–[47]. These routing algorithms can be applied to traditional single-layer and multi-layer satellite networks, but the computational and communication overhead is still high for delay sensitivity and computationally intensive application in SIN fog service.

3) COMMUNICATION TECHNOLOGY

One of the most fundamental issues in SIN fog service is how to serve more users while maintaining an uninterrupted, seamless, high-throughput and continuous connection of satellites. Besides, the satellite's spaceborne energy is limited, and communication energy consumption is another crucial issue. At present, many scholars have improved the

on-board communication technology from Mesh Reflectivity, Optical [48], MIMO [49], Frequency Selective Surfaces [50] and Mechanical Aspects [51]. These new technologies have enabled satellite communications to achieve the highest possible quality of service while reducing energy consumption, but there is still a need for future efforts to reduce costs and large-scale production [52].

VI. ANTI-QUANTUM AND EFFICIENT MUTUAL-AUTHENTICATION PROTOCOL FOR SIN FOG SERVICE

In this section, we propose a lattice-based(RLWE) post-quantum authentication protocol. The protocol can be used not only for authentication between fog node and users but also for authentication between fog nodes. In addition, the proposed protocol meets the security requirements set forth in the following subsection.

A. PRELIMINARIES

We briefly describe the mathematical problem used in the security of the proposed protocol and then the security requirements are presented in this subsection.

1) RING LEARNING WITH ERRORS (RLWE)

Let $n = 2^k$ and $k \in \mathbb{Z}$. $\mathbb{Z}[x]$ and $\mathbb{Z}_q[x]$ respectively denote the rings of polynomials over $\mathbb{Z}$ and $\mathbb{Z}_q$, where q is an odd prime number and $q \bmod 2n = 1$. Considering the two rings $\mathbb{R} = \mathbb{Z}[x]/(x^n + 1)$ and $\mathbb{R}_q = \mathbb{Z}_q[x]/(x^n + 1)$. For any polynomial element y in $\mathbb{R}$ or $\mathbb{R}_q$, denote it by its coefficient vector in $\mathbb{Z}^n$ and $\mathbb{Z}_q^n$, respectively. The discrete Gaussian distribution over $\mathbb{R}_q$ is denoted by χ_β, where β is a fixed positive real. We refer to [53] for more description of RLWE with the following lemmas.

Lemma 1: For any two elements $\boldsymbol{a}, \boldsymbol{b} \in \mathbb{R}$, there have $\|\boldsymbol{a} \cdot \boldsymbol{b}\| \leq \sqrt{n} \cdot \|\boldsymbol{a}\| \cdot \|\boldsymbol{b}\|$ and $\|\boldsymbol{a} \cdot \boldsymbol{b}\|_\infty \leq \sqrt{n} \cdot \|\boldsymbol{a}\|_\infty \cdot \|\boldsymbol{b}\|_\infty$.

Lemma 2: Given any positive real $\beta = \omega(\sqrt{\log n})$, the $Pr_{\boldsymbol{X} \leftarrow \chi_\beta}[\|\boldsymbol{X}\| > \beta \cdot \sqrt{n}] \leq 2^{-n+1}$.

Let $\mathbb{Z}_q = \{-\frac{q-1}{2}, \ldots, \frac{q-1}{2}\}$ and the subset $E = \{-\lfloor \frac{q}{4} \rfloor, \ldots, \lfloor \frac{q}{4} \rfloor\}$ as the middle set of $\mathbb{Z}_q$, where the odd prime $q > 2$. For any $x \in \mathbb{Z}_q$, the characteristic function Cha of the set E complement is defined as:

$$Cha(x) = \begin{cases} 0, & x \in E \\ 1, & x \notin E \end{cases} \tag{1}$$

The auxiliary modular function $Mod_2 : \mathbb{Z}_q \times \{0, 1\} \to \{0, 1\}$ is defined as $Mod_2(v, b) = ((v + b \cdot \frac{q-1}{2}) \bmod q) \bmod 2$, where $v \in \mathbb{Z}_q$ and $b = Cha(v)$, with the following lemma for these two functions.

Lemma 3: Given an odd prime number q, two ring elements $v, e \in \mathbb{Z}_q$ such that $|e| < \frac{q}{8}$. Then, the equation $Mod_2(v, cha(v)) = Mod_2(w, cha(v))$ holds, where $w = v + 2 \cdot e$.

The two functions Cha and Mod_2 can also be extended to the ring $\mathbb{R}_q$ by applying coefficient-wise to ring elements and can still follow the lemmas mentioned above [54].

Definition 1: Ring Learning with Errors (RLWE) Assumption. Let $\mathbb{R}_q$ and χ_β be defined as above. $\boldsymbol{v}$, $\boldsymbol{e}$ are randomly selected from $\mathbb{R}_q$ and χ_β respectively. The RLWE assumption states that it is hard for any *PPT* algorithm to distinguish $\mathbb{R}_q \times \chi_\beta$ from the uniform distribution on $\mathbb{R}_q^2$. The hardness of the RLWE assumption can be reduced to the Shortest Independent Vectors Problem (SIVP) over ideal lattices [55].

2) SECURITY REQUIREMENTS

- Mutual authentication: Both parties involved in the implementation of the authentication protocol should be able to authenticate each other's legal identity.
- Identity anonymity: The user's true identity is private information, and no information about the user's identity can be revealed during the authentication process.
- Key establishment: After both parties authenticate the other party's legal identity, they should negotiate a shared key to protect the future communication.

B. THE PROPOSED PROTOCOL

In this subsection, we detailed present our protocol in the order of initialization phase, registration phase and authentication phase.

1) INITIALIZATION PHASE

In initialization phase, terrestrial control station following steps to generates the master key pair and the public parameters.

- Terrestrial control station chooses an odd prime number q and an integer n, where n is a power of 2 and $q \bmod 2n = 1$.
- Terrestrial control station generates the discrete Gaussian distribution χ_β and a random ring element $\boldsymbol{a}$, where β is a fixed positive number and $\boldsymbol{a} \in \mathbb{R}_q$.
- Terrestrial control station randomly samples $\boldsymbol{s}, \boldsymbol{e} \leftarrow \chi_\beta$ and computes the master public key $\boldsymbol{p} = \boldsymbol{a} \cdot \boldsymbol{s} + 2 \cdot \boldsymbol{e}$, where $\boldsymbol{s}$ is the master private key.
- Terrestrial control station chooses a security hash function $h : \{0, 1\}^* \to \{0, 1\}^k$, where k is security parameter. Then publishes the public parameters $\{q, n, \chi_\beta, \boldsymbol{a}, \boldsymbol{p}, h\}$.

2) REGISTRATION PHASE

In registration phase, terrestrial control station only registers trusted users and SIN fog nodes. Users need to submit their own true identity to the terrestrial control station as the SIN fog node and additionally submit the identity of the SIN fog node that needs to be accessed. For a clearer representation, we simplify the system model with only one user u_i and two SIN fog nodes L_1, L_2. L_1 and L_2 are the neighbor fog nodes and both are nodes that the user needs to establish communication with. It is worth reminding that the messages in this phase are transmitted in the secure channel.

- L_1 randomly samples $\boldsymbol{s}_{L_1}, \boldsymbol{e}_{L_1} \leftarrow \chi_\beta$ and computes the master public key $\boldsymbol{p}_{L_1} = \boldsymbol{a} \cdot \boldsymbol{s}_{L_1} + 2 \cdot \boldsymbol{e}_{L_1}$ and then sends the

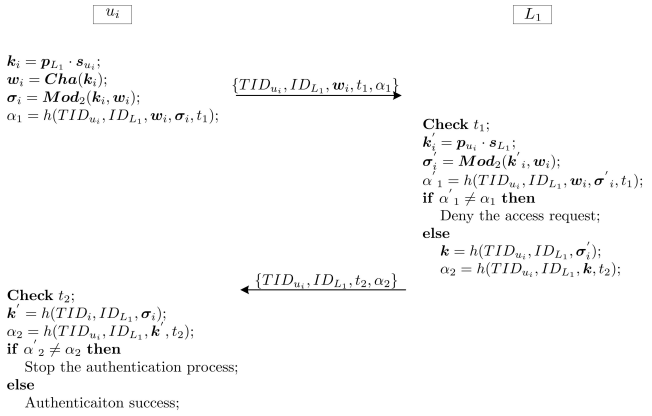


FIGURE 6. Authentication phase.

message $\{ID_{L_1}, p_{L_1}\}$ to terrestrial control station, where ID_{L_1} is the true identity of L_1.

- L_2 and u_i do the same steps as L_1 to generate their own public-private key pairs, denoted by $\{s_{L_2}, p_{L_2}\}$ and $\{s_{u_i}, p_{u_i}\}$, and then send the message $\{ID_{L_2}, p_{L_2}\}$ and $\{ID_{u_i}, p_{u_i}, ID_{L_1}, ID_{L_2}\}$ to terrestrial control station, respectively.
- Terrestrial control station computes $TID_{u_i} = h(ID_{u_i}, s)$, and sends the message $\{TID_{u_i}, p_{L_1}, p_{L_2}\}$ to u_i. For L_1 and L_2, terrestrial control station sends the message $\{TID_{u_i}, p_{u_i}, ID_{L_2}, p_{L_2}\}$ and $\{TID_{u_i}, p_{u_i}, ID_{L_1}, p_{L_1}\}$, respectively.

3) AUTHENTICATION PHASE

As shown in Fig.6, the following steps take the mutual authentication and negotiation key between u_i and L_1 as an example, and the authentication method between L_1 and L_2 is the same.

- u_i computes $k_i = p_{L_1} \cdot s_{u_i}$, $w_i = \boldsymbol{Cha}(k_i)$, $\sigma_i = \boldsymbol{Mod_2}(k_i, w_i)$ and $\alpha_1 = h(TID_{u_i}, ID_{L_i}, w_i, \sigma_i, t_1)$, where t_1 the is timestamp. Finally, u_i sends the message $\{TID_{u_i}, ID_{L_1}, w_i, t_1, \alpha_1\}$ to L_1.
- After L_1 receiving the message, first check whether the timestamp t_1 within the time allowed range. If t_1 is out of the allowed range, L_1 will reject the connection. Otherwise L_1 continues to compute $k_i' = p_{u_i} \cdot s_{L_1}$, $\sigma_i' = \boldsymbol{Mod_2}(k_i', w_i)$ and $\alpha_1' = h(TID_{u_i}, ID_{L_i}, w_i, \sigma_i', t_1)$ according to the protocol. Then verifies whether α_1' and α_1 are equal. If not equal, the user that sends the access request is not a legitimate user of the system and L_1 will reject the access request. Otherwise continues to computes the shared key $k = h(TID_{u_i}, ID_{L_i}, \sigma_i')$ and $\alpha_2 = h(TID_{u_i}, ID_{L_i}, k, t_2)$, where t_2 is the timestamp. Finally, L_1 sends the message $\{TID_{u_i}, ID_{L_1}, t_2, \alpha_2\}$ to u_i.
- After u_i receiving the message, u_i also needs to first check if the timestamp t_2 is within the time allowed. Then computes $k' = h(TID_{u_i}, ID_{L_i}, \sigma_i)$ and $\alpha_2' = h(TID_{u_i}, ID_{L_i}, k', t_2)$ and verifies α_2' and α_2 are equal. If equal, L_1 communicating with u_i is a legal node and the shared key after negotiation is k'.

TABLE 2. Execution times of RLWE-related operations.

Notation	Satellite Node (ns)	End user (ns)
T_{mul}	0.307	13.052
T_{Cha}	0.689	35.515
T_h	14.09	180.964

4) SECURITY ANALYSIS

- Mutual authentication: In the second step of the authentication phase, L_1 authenticates the legal identity of the user u_i by verifying $\alpha_1' = \alpha_1$. Since L_1 received the temporary identity of the user u_i and the public key p_{u_i} during the registration phase and only the user who has public and private key pairs $\{p_{u_i}, s_{u_i}\}$ can obtain the same σ_i with L_1. No one can obtain the private key s_{u_i} only through public data unless RLWE assumption is resolved in polynomial time. Similarly, in the third step, by verifying whether $\alpha_2' = \alpha_2$, it can be verified whether the peer is L_1. In addition, since each message contains the timestamp t and the message hash-value α, the attacker's replay attack and message tampering attack can be easily detected.
- Identity anonymity: In the whole authentication process, the user's true identity ID_{u_i} is replaced by the temporary identity TID_{u_i}. The attacker can only obtain the true identity of the user in two ways. The first is to invade terrestrial control statin. However, terrestrial control station as a trusted entity deploys the highest level of defense system, which is difficult for attackers to invade the terrestrial control station. Another way is to perform the hash collision to get the true ID_{u_i} through the TID_{u_i}. Due to the unidirectional nature of the hash function, it is also very difficult for the attacker to implement.
- Key establishment: In the second and third steps of the authentication agreement, user u_i and L_1 can independently generate the shared keys $k = h(TID_{u_i}, ID_{L_i}, \sigma_i)$, where σ_i is computed by both parties and avoids the shared key being generated by a single entity.

5) PERFORMANCE ANALYSIS

Performance analysis mainly considers the computational overhead in the authentication phase. To make it easier to analyze the computational overhead, we use the following notation to represent the average time overhead for different operations. T_{mul} represent multiplication time in $\mathbb{R}_q$. T_{Cha} and T_h represent the time for $\boldsymbol{Cha}$ and hash values, respectively. We quote the overhead time of these computation operations in [56] and shown in table 2. It is worth reminding that the computational overhead of $\boldsymbol{Mod}_2$ is small enough to be ignored.

In the whole authentication process, the computing overhead of the user is $T_{mul} + T_{Cha} + 3 \cdot T_h = 591.46\ ns$ and the computing overhead of the satellite node is $T_{mul} + 3 \cdot T_h = 42.58\ ns$. The computing overhead of the whole authentication is only 634.04 ns, which can greatly meet the security and low overhead requirements of SIN fog service.

VII. CONCLUSION

In this article, we have proposed SIN fog service considering the global coverage of satellite network and advantages of fog service. The key idea of SIN fog service is to turn moving satellites with spare capacity into mobile fog nodes to provide computing, storage and communication services for users in satellite coverage areas. Then the architecture of SIN fog service, a potential use case and the requirement of security and challenge are elaborated. Finally, we proposed an anti-quantum and efficient mutual-authentication protocol, which can be used for mutual authentication between users and SIN nodes or mutual authentication between fog nodes. For future research, we plan to develop the more secure mechanisms that can provide access authentication, secure transmission and privacy protection. Although there are still challenges to be solved, we believe that SIN fog service has a higher potential to play a more important role in environments with inadequate ground communication and computing power.

REFERENCES

[1] M. Arti and V. Jain, "Relay selection-based hybrid satellite-terrestrial communication systems," *IET Commun.*, vol. 11, no. 17, pp. 2566–2574, Nov. 2017.

[2] Z. Zhang, W. Zhang, and F.-H. Tseng, "Satellite mobile edge computing: Improving QoS of high-speed satellite-terrestrial networks using edge computing techniques," *IEEE Netw.*, vol. 33, no. 1, pp. 70–76, Jan. 2019.

[3] M. S. de Brito, S. Hoque, R. Steinke, A. Willner, and T. Magedanz, "Application of the fog computing paradigm to smart factories and cyber-physical systems," *Trans. Emerg. Telecommun. Technol.*, vol. 29, no. 4, p. e3184, 2018.

[4] Q. Zhang, L. Cheng, and R. Boutaba, "Cloud computing: State-of-the-art and research challenges," *J. Internet Services Appl.*, vol. 1, no. 1, pp. 7–18, 2010.

[5] F. Y. Okay and S. Ozdemir, "A fog computing based smart grid model," in *Proc. Int. Symp. Netw., Comput. Commun. (ISNCC)*, May 2016, pp. 1–6.

[6] M. Chiang and T. Zhang, "Fog and IoT: An overview of research opportunities," *IEEE Internet Things J.*, vol. 3, no. 6, pp. 854–864, Dec. 2016.

[7] D. Borthakur, H. Dubey, N. Constant, L. Mahler, and K. Mankodiya, "Smart fog: Fog computing framework for unsupervised clustering analytics in wearable Internet of Things," in *Proc. IEEE Global Conf. Signal Inf. Process. (GlobalSIP)*, Nov. 2017, pp. 472–476.

[8] B. R. Stojkoska and K. Trivodaliev, "Enabling Internet of Things for smart homes through fog computing," in *Proc. 25th Telecommun. Forum (TELFOR)*, Nov. 2017, pp. 1–4.

[9] C. Huang, R. Lu, and K.-K.-R. Choo, "Vehicular fog computing: Architecture, use case, and security and forensic challenges," *IEEE Commun. Mag.*, vol. 55, no. 11, pp. 105–111, Nov. 2017.

[10] 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.

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

[12] R. Leopold, "The Iridium Communications Systems," in *Proc. Singapore ICCS/ISITA*, Jan. 2003, pp. 451–455.

[13] A. Vanelli-Coralli, G. E. Corazza, M. Luglio, and S. Cioni, "The ISICOM architecture," in *Proc. Int. Workshop Satellite Space Commun.*, Sep. 2009, pp. 104–108.

[14] J. N. Ptasinski and Y. Congtang, "The automated digital network system (ADNS) interface to transformational satellite communications system (TSAT)," in *Proc. MILCOM IEEE Military Commun. Conf.*, Oct. 2007, pp. 1–5.

[15] E. Ekici, I. Akyildiz, and M. Bender, "A distributed routing algorithm for datagram traffic in LEO satellite networks," *IEEE/ACM Trans. Netw.*, vol. 9, no. 2, pp. 137–147, Apr. 2001.

[16] Y. Yao, X. Chang, J. Misic, and V. Misic, "Reliable and secure vehicular fog service provision," *IEEE Internet Things J.*, vol. 6, no. 1, pp. 734–743, Feb. 2019.

[17] Y. Guan, J. Shao, G. Wei, and M. Xie, "Data security and privacy in fog computing," *IEEE Netw.*, vol. 32, no. 5, pp. 106–111, Sep. 2018.

[18] H. A. Al Hamid, S. M. M. Rahman, M. S. Hossain, A. Almogren, and A. Alamri, "A security model for preserving the privacy of medical big data in a healthcare cloud using a fog computing facility with pairing-based cryptography," *IEEE Access*, vol. 5, pp. 22313–22328, 2017.

[19] B. Huang, X. Cheng, Y. Cao, and L. Zhang, "Lightweight hardware based secure authentication scheme for fog computing," in *Proc. IEEE/ACM Symp. Edge Comput. (SEC)*, Oct. 2018, pp. 433–439.

[20] D. Ma, X. Liu, X. Wang, J. Xiong, and W. Li, "On the performance indexes of physical layer security for multi-beam satellite networks," in *Proc. Int. Conf. Wireless Commun. Signal Process. (WCSP)*, Oct. 2015, pp. 1–6.

[21] C. D. Flynn, A. M. McCaffrey, P. Jayachandran, and R. B. Langley, "Discovery of new code interference phenomenon in GPS observables," *GPS Solutions*, vol. 23, no. 3, p. 65, 2019.

[22] L. Rong and L. Ruimin, "An anti-jamming improvement strategy for satellite frequency-hopping communication," in *Proc. Int. Conf. Wireless Commun. Signal Process.*, Nov. 2009, pp. 1–5.

[23] Q. Li, Z. Han, W. Wang, X. Wang, and D. Xu, "Anti-jamming scheme for GPS receiver with vector tracking loop and blind beamformer," *Electron. Lett.*, vol. 50, no. 19, pp. 1386–1388, Sep. 2014.

[24] M. O. Mughal and S. Kim, "Signal classification and jamming detection in wide-band radios using Naïve Bayes classifier," *IEEE Commun. Lett.*, vol. 22, no. 7, pp. 1398–1401, Jul. 2018.

[25] D. Zhai, X. Da, H. Hu, Y. Liang, R. Xu, and L. Ni, "Satellite anti-interception communication system based on WFRFT and MIMO," in *Proc. 10th Int. Conf. Commun. Softw. Netw. (ICCSN)*, Jul. 2018, pp. 305–310.

[26] S. Vishwakarma and A. Chockalingam, "Decode-and-forward relay beamforming for secrecy with imperfect CSI and multiple eavesdroppers," in *Proc. IEEE Int. Workshop Signal Process. Adv. Wireless Commun.*, Jun. 2012.

[27] S. Kan, "China's anti-satellite weapon test," Library Congr., Congressional Res. Service, Washington, DC, USA, Tech. Rep. RS22652, 2007.

[28] F. H. Dong, L. V. Jing, X. W. Gong, and L. I. Chao, "Optimization design of structure invulnerability in space information network," *J. Commun.*, vol. 35, no. 10, pp. 50–58, 2014.

[29] X. Ji, L. Liu, P. Zhao, and D. Wang, "A destruction-resistant on-demand routing protocol for LEO satellite network based on local repair," in *Proc. 12th Int. Conf. Fuzzy Syst. Knowl. Discovery (FSKD)*, Aug. 2015, pp. 2013–2018.

[30] D. Li, X. Mao, J. Yu, and G. Wang, "A destruction-resistant dynamic routing algorithm for LEO/MEO satellite networks," in *Proc. 4th Int. Conf. Comput. Inf. Technol. (CIT)*, 2004, pp. 522–527.

[31] D. He, X. Li, S. Chan, J. Gao, and M. Guizani, "Security analysis of a space-based wireless network," *IEEE Netw.*, vol. 33, no. 1, pp. 36–43, Jan. 2019.

[32] T.-H. Chen, W.-B. Lee, and H.-B. Chen, "A self-verification authentication mechanism for mobile satellite communication systems," *Comput. Elect. Eng.*, vol. 35, no. 1, pp. 41–48, 2009.

[33] G. Zheng, H.-T. Ma, C. Cheng, and Y.-C. Tu, "Design and logical analysis on the access authentication scheme for satellite mobile communication networks," *IET Inf. Secur.*, vol. 6, no. 1, pp. 6–13, 2012.

[34] 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, Jul. 2018.

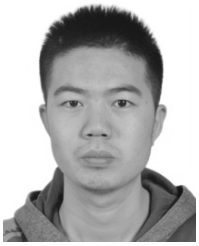
[35] Y. Liu, A. Zhang, J. Li, and J. Wu, "An anonymous distributed key management system based on CL-PKC for space information network," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2016, pp. 1–7.

[36] C. Lv, M. Ma, H. Li, and J. Ma, "An efficient three-party authenticated key exchange protocol with one-time key," in *Proc. INFOCOM IEEE Conf. Comput. Commun. Workshops*, 2010.

[37] S. K. S. V. A. Kavuri, G. R. Kancherla, and B. R. Bobba, "Data authentication and integrity verification techniques for trusted/untrusted cloud servers," in *Proc. Int. Conf. Adv. Comput., Commun. Informat. (ICACCI)*, Sep. 2014, pp. 2590–2596.

[38] G. Weintraub and E. Gudes, "Crowdsourced data integrity verification for key-value stores in the cloud," in *Proc. 17th IEEE/ACM Int. Symp. Cluster, Cloud Grid Comput. (CCGRID)*, May 2017, pp. 498–503.

[39] J. Ni, A. Zhang, X. Lin, and X. S. Shen, "Security, privacy, and fairness in fog-based vehicular crowdsensing," *IEEE Commun. Mag.*, vol. 55, no. 6, pp. 146–152, Jun. 2017.
[40] L. Sweeney, "k-anonymity: A model for protecting privacy," *Int. J. Uncertainty, Fuzziness Knowl.-Based Syst.*, vol. 10, no. 5, pp. 557–570, 2002.
[41] M. Ashwin, K. Daniel, G. Johannes, and V. Muthuramakrishnan, "l-Diversity: Privacy beyond k-anonymity," *ACM Trans. Knowl. Discovery Data*, vol. 1, no. 1, pp. 1–52, 2007.
[42] C. Dwork, "Differential privacy," in *Encyclopedia Cryptography Security*. 2011, pp. 338–340.
[43] T. Zhu, G. Li, W. Zhou, and P. S. Yu, "Differentially private data publishing and analysis: A survey," *IEEE Trans. Knowl. Data Eng.*, vol. 29, no. 8, pp. 1619–1638, Aug. 2017.
[44] M. Sheng, D. Zhou, R. Liu, Y. Wang, and J. Li, "Resource mobility in space information networks: Opportunities, challenges, and approaches," *IEEE Netw.*, vol. 33, no. 1, pp. 128–135, Jan. 2019.
[45] I. Akyildiz, E. Ekici, and M. Bender, "MLSR: A novel routing algorithm for multilayered satellite IP networks," *IEEE/ACM Trans. Netw.*, vol. 10, no. 3, pp. 411–424, Jun. 2002.
[46] E. Ekici, I. Akyildiz, and M. Bender, "A multicast routing algorithm for LEO satellite IP networks," *IEEE/ACM Trans. Netw.*, vol. 10, no. 2, pp. 183–192, Apr. 2002.
[47] C. Chen and E. Ekici, "A routing protocol for hierarchical LEO/MEO satellite IP networks," *Wireless Netw*, vol. 11, no. 4, pp. 507–521, Jul. 2005.
[48] L. Stampoulidis, J. Edmunds, M. Kechagias, G. Stevens, J. Farzana, M. Welch, and E. Kehayas, "Radiation-resistant optical fiber amplifiers for satellite communications," *Proc. SPIE*, vol. 10096, p. 100960H, Feb. 2017.
[49] A. I. Pérez-Neira, C. Ibars, J. Serra, A. Del Coso, J. Gómez-Vilardebó, M. Caus, and K. P. Liolis, "MIMO channel modeling and transmission techniques for multi-satellite and hybrid satellite–terrestrial mobile networks," *Phys. Commun.*, vol. 4, no. 2, pp. 127–139, Jun. 2011.
[50] A. C. Densmore, "Algorithms for rapid characterization and optimization of aperture and reflector antennas," Ph.D. dissertation, Dept. Elect. Eng., Univ. California, Los Angeles, VA, USA, 2014.
[51] A. G. Roederer and Y. Rahmat-Samii, "Unfurlable satellite antennas: A review," in *Annales des télécommunications*, vol. 44. Berlin, Germany: Springer, 1989, pp. 475–488.
[52] Y. Rahmat-Samii and A. C. Densmore, "Technology trends and challenges of antennas for satellite communication systems," *IEEE Trans. Antennas Propag.*, vol. 63, no. 4, pp. 1191–1204, Apr. 2015.
[53] J. Zhang, Z. Zhang, J. Ding, M. Snook, and Ö. Dagdelen, "Authenticated key exchange from ideal lattices." in *Proc. Annu. Int. Conf. Theory Appl. Cryptograph. Techn.* Berlin, Germany: Springer, 2015, pp. 719–751.
[54] J. Ding, S. Alsayigh, J. Lancrenon, R. V. Saraswathy, and M. Snook, "Provably secure password authenticated key exchange based on RLWE for the post-quantum world," in *Proc. Cryptograph. Track RSA Conf.*, 2017, pp. 183–204.
[55] V. Lyubashevsky, C. Peikert, and O. Regev, "On ideal lattices and learning with errors over rings," in *Proc. Int. Conf. Theory Appl. Cryptograph. Techn.*, 2010.
[56] Q. Feng, D. He, S. Zeadally, N. Kumar, and K. Liang, "Ideal lattice-based anonymous authentication protocol for mobile devices," *IEEE Syst. J.*, vol. 13, no. 3, pp. 2775–2785, Sep. 2019.



JUNYAN GUO received the B.Eng. degree from the North China University of Technology, Beijing, China, in 2017. He is currently pursuing the Ph.D. degree with the School of Computer and Information Technology, Beijing Jiaotong University, Beijing. His research interests include space information networks, fog computing, and privacy preserving.

YE DU received the Ph.D. degree in computer science from Harbin Engineering University, Harbin, China, in 2006. He is currently a Professor with the School of Computer and Information Technology, Beijing Jiaotong University, Beijing, China. His research interests include cyber-security, privacy preserving, big-data mining, and abnormal detection.