A Survey on Authentication in Satellite Internet

Jianing Wang[1,2], Yuanyu Zhang[1,2*], Shuangrui Zhao[1,2], Ji He[1,2], Yulong Shen[1,2], and Xiaohong Jiang[3]
[1]School of Computer Science and Technology, Xidian University, Xi'an, Shaanxi, 710071, China
[2]Network and System Security Key Laboratory of Shannxi Province, Xidian University, Xi'an, 710071, China
[3]School of Systems Information Science, Future University Hakodate, 116-2
Kamedanakano-cho, Hakodate, Hokkaido, 041-8655, Japan

Satellite Internet is a promising technology that provides global connectivity and has attracted widespread attention from both industry and academia. However, the open nature of wireless communication links renders Satellite Internet vulnerable to signal spoofing and illegal access attacks. Authentication has been recognized as an effective countermeasure to these attacks. Therefore, this paper presents a comprehensive survey of existing authentication schemes in Satellite Internet for the first time. We categorize existing authentication schemes into two main scenarios, i.e., the Satellite-based Communication (SATCOM) system and the Global Navigation Satellite System (GNSS) scenario. We further divide the literature in the SATCOM scenario into five sub-categories and that in the GNSS scenario into two sub-categories. Finally, we discuss the challenges that existing authentication schemes are facing and will face and further present some future research directions.

***Index Terms*—Authentication, cryptography-based authentication, physical layer authentication, GNSS anti-spoofing.**

I. Introduction

In the past few decades, terrestrial networks have been fully deployed, especially the commercial use of fifth-generation (5G), making traditional terrestrial wireless communications experience explosive growth in terms of the number of users and support services. With the widespread application of technologies such as the Internet of Things (IoT) and unmanned driving, there is an increasing demand for ubiquitous global network access. However, the terrestrial network infrastructure is vulnerable to disasters and cannot be deployed in harsh environments such as oceans and mountains. Therefore, it is difficult to meet the explosive demand for high-speed and reliable network access anywhere in the world. Interconnecting space, air, and ground network segments, the Satellite Internet has drawn widespread attention from both the academia and industry [1], [2]. Satellite Internet is a new type of network based on satellite communication technology, which forms a large-scale network by deploying a specific number of satellites. It provides services such as navigation and seamless broadband Internet access to ground and air terminals. Satellite Internet is playing a vital role in many fields, including radio broadcasting, weather forecasting, maritime communications, aided navigation, and military operations [3], and is considered one of the most promising technologies to support the development of the future sixth-generation (6G) networks [4].In recent years, major countries and technology companies have established various satellite constellation projects for global coverage, such as StarLink [5], OneWeb [6], Telesat [7], and HongYan [8].

With the rapid development of Satellite Internet, network security cannot be overlooked. Similar to other wireless networks, the information in Satellite Internet is also transmitted over the air directly. The highly exposed links make Satellite Internet vulnerable to various attacks, including spoofing attacks, replay attacks, impersonation attacks, and man-in-the-middle attacks. If the data in Satellite Internet was illegally accessed, eavesdropped, or tampered with, serious consequences may affect national security and social stability [9], [37]. Moreover, compared with traditional wireless networks, Satellite Internet has some special characteristics, such as extremely long propagation delay and limited on-satellite computing and storage capacity. In addition, the complex and dynamic network topology makes satellite links difficult to maintain stability and handover frequently. Authentication has been proven to be an effective approach to verifying the legitimacy of entities in the Satellite Internet which enhance the security and reliability of the network, thus avoiding malicious attacks.

In the last few years, several contributions have been proposed to review the security issues in the Satellite Internet. Li *et al.* [10] reviewed the state-of-art research activity on physical-layer security in satellite communications. However, they only focused on the physical layer and did not take authentication into consideration. Studies in [11], [12], and [13] present comprehensive investigations of spoofing attacks and the adopted solutions for Global Navigation Satellite Systems (GNSSs). However, none of them considered satellite-based communication (SATCOM) systems. Liu *et al.* [14] reported the security issues and key technologies, such as cross-domain key distribution and update and efficient access authentication. However, they only considered the upper-layer authentication schemes. Recently, Tedeschi *et al.* [3] investigated the security threats, solutions, and challenges faced in deploying and operating the SATCOM system from two aspects, namely, physical layer security and cryptographic schemes. However, they only considered the GNSS anti-spoofing schemes in terms of physical layer authentication (PLA), and only the authentication scheme using public key infrastructure (PKI).

Although existing surveys have presented security issues related to Satellite Internet, there is still a lack of a comprehensive survey of the authentication in Satellite Internet. In this paper, we provide a comprehensive survey of the state-

Manuscript received November 8, 2022; revised December 26, 2022.
*Corresponding author: Yuanyu Zhang (email: yyuzhang@xidian.edu.cn).

TABLE I
LIST OF ABBREVIATIONS.

Abbreviations	Full Name	Abbreviations	Full Name
5G	Fifth Generation	6G	Sixth Generation
AKA	Authentication and Key Agreement	AGC	Automatic Gain Control
BDS	BeiDou Navigation Satellite System	CA	Certificate Authority
CNAV	Civil Navigation	CNN	Convolutional Neural Network
CRT	Chinese Remainder Theorem	C/N_0	Carrier-to-Noise Ratio
DFSD	Doppler Frequency Shift Difference	DoS	Denial of Service
DSA	Digital Signature Algorithm	DSSS	Direct Sequence Spread Spectrum
ECC	Elliptic Curve Cryptosystem	ECDSA	Elliptic Curve Digital Signature Algorithm
GEO	Geostationary Equatorial Orbit	GLONASS	Glodal Navigation Satellite System
GLRT	Generalized Likelihood Ratio Test	GNSS	Global Navigation Satellite System
GPS	Global Positioning System	GS	Ground Station
HAP	High-altitude Platform	HTS	High throughput satellite
IMU	Inertial Measurement Unit	IoT	Internet of Things
IRA	IRIDIUM Ring Alert	LAP	Low-altitude Platform
LEO	Low Earth Orbit	MAC	Message Authentication Code
MANET	Mobile Ad-Hoc Network	MEO	Medium Earth Orbit
NCC	Network Control Center	NMA	Navigation Message Authentication
PBS	Perfect Backward Secrecy	PFS	Perfect Forward Secrecy
PLA	Physical Layer Authentication	PKC	Public-Key Cryptosystem
PKI	Public Key Infrastructure	PKG	Public Key Generator
PVT	Positioning, Navigation, and Timing	QoS	Quality of Service
q-SDH	q-Strong Diffie-Hellman	QZSS	Quasi-Zenith Satellite System
RAIM	Receiver Autonomous Integrity Monitoring	RSA	Rivest-Shamir-Adleman cryptosystem
SAS	Signal Authentication Sequence	SATCOM	Satellite-based Communication
SCA	Spreading Code Authentication	SD-SIN	Software-Defined Space Information Network
SMA	Source Message Authentication	SKC	Secret-Key Cryptosystem
TESLA	Timed Efficient Stream Loss-tolerant Authentication	ToA	Time of Arrival
UAV	Unmanned Aerial Vehicle	USRP	Universal Software Radio Peripheral
VSD	Vestigial Signal Defense	WiMax	Worldwide Interoperability for Microwave Access
WLAN	Wireless Local Area Network		

of-the-art research on authentication schemes in the Satellite Internet, covering not only cryptographic authentication schemes but also PLA schemes in both SATCOM systems and GNSS. In particular, we survey the current authentication schemes from these two main scenarios, e.g., SATCOM and GNSS. We delve into each scenario and further categorize them into several sub-categories based on the applied approaches or the layer/data source on which authentication is implemented. For SATCOM authentication, we divide the literature into *source message authentication* (SMA), which verifies the authenticity of source messages with the help of satellites, *authentication and key agreement* (AKA), which deals with AKA between a satellite/user and a satellite/user, *handover authentication* including inter&intra-satellite, inter-ground station, inter-network handover authentication, *cross-domain authentication*, which verifies the identities of users when using services across domains, and *PLA*, which utilizes the inherent features of downlink channels or satellites for satellite authentication. For GNSS signal authentication, we divide existing works into *message-level authentication*, which verifies the authenticity of GNSS messages based on digital signature or spreading code, and *signal-level authentication*, which detects spoofing attacks based on the differences between authentic GNSS signals and spoofing signals. Finally, we identify potential challenges and some promising future research directions for authentication in Satellite Internet.

The remainder of this paper is organized as follows. In Section II, we present the system architecture and authentication architecture of the Satellite Internet. In Section III, we introduce authentication schemes in SATCOM, including SMA, AKA, handover authentication, cross-domain authentication and PLA. In Section IV, we introduce authentication schemes in GNSS, including message-level authentication and signal-level authentication. Then, we point out some challenges and future research directions in Section V. Finally, Section VI concludes the whole paper.

II. Background

In this section, we introduce the basic architecture of the Satellite Internet. Then, we provide a brief introduction to the authentication architecture of the Satellite Internet.

A. Architecture of Satellite Internet

As shown in Fig. 1, Satellite Internet is a heterogeneous network whose architecture mainly consists of three segments, including a space-based network, an air-based network, and a terrestrial-based network, respectively. The space-based network, the backbone of the Satellite Internet, consists of diverse types of satellites, constellations, and the corresponding ground infrastructures. According to the orbital altitudes, satellites are classified into three categories, i.e., Geostationary Equatorial Orbit (GEO) with an altitude above 35,786 km, Medium Earth Orbit (MEO) with an altitude from 2,000 to 25,000 km, and Low Earth Orbit (LEO) satellites with an altitude from 160 to 2,000 km [51]. In general, satellites with higher altitudes have a greater coverage area on the earth but longer transmission delay. Orbiting in the geosynchronous orbit with the largest earth coverage area, GEO satellites appear stationary in space, and only three of them are required for complete communication coverage. Hundreds of GEO satellites are in orbit today, traditionally supporting businesses of broadcast TV, weather data, and some low-speed data communication. MEO satellites are used for global positioning systems (GPS) and other navigation applications. More recently, high throughput satellites (HTS) MEO constellations have been deployed to deliver low-latency, high-bandwidth data connectivity to service providers, government agencies, and commercial enterprises [15]. As being closer to the earth, LEO satellites, which have attracted significant attention recently, tend to be smaller and have lower transmission delay than GEO and MEO satellites. Thus, they have lower costs and are more suitable for addressing imaging and low-bandwidth telecommunications needs. Companies like SpaceX and Iridium are planning to put tens of thousands of LEO satellites into orbit recently [16]. These huge mega constellations are expected to provide mobile users with global voice and data connections. However, due to the large signal propagation delay of satellite-terrestrial links, it is vulnerable to attack and destruction by malicious nodes during transmission, making it difficult to guarantee the quality of service (QoS).

The air-based network is composed of unmanned aerial vehicles (UAVs), low-altitude aircrafts, airships, and balloons. According to the distance from these aerial components to the ground, the air-based network can be separated into two platforms: high-altitude platforms (HAPs) and low-altitude platforms (LAPs), which are 17-22 km and 0-10 km above the ground, respectively [17]. The HAPs can exchange data with the satellite layer and enable bidirectional communications as well as data transmissions between aircraft and ground stations with minimal delays. The LAPs are mainly formed with UAVs, which have received great attention recently. Due to the advantages of lower communication costs, less transmission delay, higher flexibility and mobility, UAVs can be used for critical operations such as rescue, surveillance, and transportation in various types of fields, including agriculture, forestry, environmental protection, and security [18]. In addition, multiple UAVs can self-organize as an aerial subnet to provide network access services for terrestrial users.

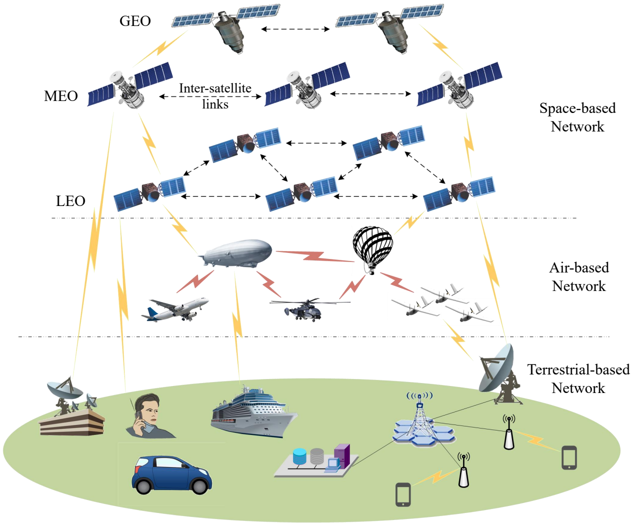

Fig. 1. Architecture of Satellite Internet.

The terrestrial network mainly consists of the ground communication facilities, such as base stations, mobile terminal users, and many sub-networks, including cellular networks, mobile ad-hoc networks (MANETs) [19], wireless local area networks (WLANs) [20], worldwide interoperability for microwave access (WiMax) [21], and so on. At present, terrestrial communication technologies have developed rapidly, which can provide a high data transmission rate, high throughput, and relatively low latency. However, the terrestrial network relies on infrastructures deployed on the ground, which are vulnerable to natural disasters and cannot provide high-quality services for remote areas such as rural areas and seas.

B. Authentication Architecture of Satellite Internet

The reference authentication architecture of Satellite Internet, as shown in Fig. 2, is generally characterized by three segments, e.g., the space segment, the ground segment, and the user segment, as well as some links, including inter-satellite links, satellite-to-ground links, satellite-to-user links, user-to-satellite-to-ground links and user-to-satellite-to-user links. In SATCOM scenario, SMA always happens on user-to-satellite-to-user links. The user-GS AKA and user-satellite AKA are implemented on user-to-satellite-to-ground links and satellite-satellite AKA on inter-satellite links. Handover authentication and cross-domain authentication are also performed on user-to-satellite-to-ground links or satellite-to-user links. Moreover, PLA is implemented on satellite-to-user links. In GNSS scenario, all authentication schemes are performed on satellite-to-user links. The space segment in the authentication architecture

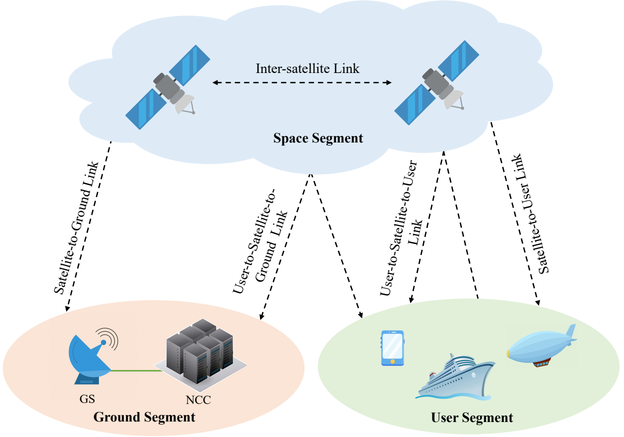

Fig. 2. Authentication architecture of Satellite Internet.

of Satellite Internet comprises GEO, MEO, and LEO satellites, which nowadays can have a certain capacity for computation and storage. It also provides communication, access, and global navigation services for terminals in the user segment. The ground segment is made up of ground stations (GSs) and network control centers (NCCs). Globally distributed ground stations can provide both a ground interface for satellites and an interface to the terrestrial network for users. The NCC is responsible for generating, distributing, storing and updating keys, registration and authorization for users. The user segment consists of terminals that want to obtain services in the Satellite Internet, such as mobile phones, aircraft, and ships. Various attacks can be launched in any of these segments. Thus, authentication in these segments can resist plenty of attacks and strengthen the security of the Satellite Internet.

III. Authentication in SatCom

In this section, we provide a taxonomy of authentication schemes in the SATCOM scenario. In this scenario, various entities involved in service provisioning need to establish trust relationships through authentication. We divide the existing works in the SATCOM authentication scenario into five subcategories based on the authentication models and approaches: source message authentication, authentication and key agreement, handover authentication, cross-domain authentication and physical-layer authentication.

A. Source Message Authentication (SMA)

SMA is an effective method of securing multicast communications, which enables receiving users of multicast data to verify that the received data originates from the source and has not been modified. In satellite-based SMA, users authenticate source messages over the user-to-user link relayed by a satellite. The satellite acts as a Certificate Authority (CA) and distributes Message Authentication Code (MAC) keys to the users. Roy-Chowdury *et al.* [22] first proposed a lightweight SMA scheme for group communication in satellite networks. In this scheme, source authentication is achieved by the Timed Efficient Stream Loss-tolerant Authentication (TESLA) method [23], where the disclosure of symmetric keys used to compute the MACs is delayed such that asymmetric key-based authentication can be realized. Since MACs are based on symmetric encryption, this scheme requires less computing power. Later, they proposed an improved scheme in [24], which modifies the TESLA certificate to the extended TESLA certificate. The extended TESLA certificate and the source authentication scheme are suitable for wireless devices with limited energy availability.

B. Authentication and Key Agreement (AKA)

AKA is a mechanism that enables mutual authentication and session key agreement between two entities in SATCOM. Based on cryptographic primitives, AKA is effective in dealing with certain attacks. According to the difference between the authentication parties, we divide the AKA mechanisms into user-GS AKA, user-satellite AKA and satellite-satellite AKA.

1) User-GS AKA

In the user-GS AKA scenario, users and GSs perform mutual authentication via satellites, which are simply responsible for forwarding authentication messages between users and GSs, rather than participating in the authentication process. Chen *et al.* [25] proposed an AKA mechanism for mobile SATCOM systems based on a public-key cryptosystem (PKC) and a secret-key cryptosystem (SKC) which can remove the complexity of PKI. However, this mechanism is vulnerable to a denial of service (DoS) attack, where an attacker interrupts the authentication phase by jamming a single message. This vulnerability was later overcome by an improved AKA mechanism in [26]. Chang *et al.* [27] found that the scheme in [26] cannot resist impersonation attacks when the smart card is lost or stolen, and then proposed a new AKA scheme using a one-way hash function with low computational overheads. Lee *et al.* [28] proposed a simple and efficient AKA scheme for SATCOM systems and claimed that their scheme could resist various attacks and achieve several functionality requirements. However, Jurcut *et al.* [29] pointed out that Lee's scheme is susceptible to desynchronization attacks and proposed an improved scheme, which incorporates a resynchronization phase. Altaf *et al.* [30] and Xu *et al.* [31] proposed anonymous AKA schemes based on a one-way hash function and elliptic curve cryptography, respectively. However, neither of the above two schemes can defend against offline password-guessing attacks [32], [33]. In recent years, the rapid development of quantum computers has rendered it possible to effortlessly crack traditional cryptographic schemes based on number theory, such as Rivest-Shamir-Adleman cryptosystem (RSA) algorithm and elliptic curve cryptosystems (ECC) algorithm. Therefore, Kumar *et al.* [34] and Dharminder *et al.* [35] proposed AKA schemes based on ring learning with error, respectively, which are secure against quantum attacks.

2) User-Satellite AKA

In the user-GS schemes, satellites are only used as relays between the users and the GSs. Thus, the user-GS AKA schemes require at least four signal transmission delays between the ground and the satellite (back and forth between user/satellite and NCC/satellite, respectively), leading to a long authentication delay. Therefore, as satellite computing and storage capabilities advance, some AKA schemes employ satellites for authentication to reduce the authentication delay. We term such schemes user-Satellite AKA schemes. In 2018, Meng *et al*. [36] first proposed a low-latency AKA scheme for SATCOM systems based on the proxy signature, enabling the satellite to authenticate users directly without the real-time involvement of the ground segment nodes. Xue *et al*. [37] proposed a secure and efficient AKA scheme for the IoT-based SATCOM systems, which reduces verification delay and avoids the single-point bottleneck of the NCC. However, the schemes in [36] and [37] fail to achieve some critical security properties, such as unlinkability and perfect forward/backward secrecy (PFS/PBS). Yi *et al*. [38] and Ma *et al*. [39] respectively proposed two AKA schemes using lattice-based cryptography to overcome the insufficiencies of existing access authentication methods in SATCOM system, such as high computational complexity, large authentication delay and no resistance to quantum attack. In 2020, Yao *et al*. [40] proposed an identity-based mutual authentication scheme (IMAS) with the adoption of multicast authentication, which greatly reduced the authentication computation delay and signalling overhead. However, these identity-based AKA schemes [36], [37], [38], [39], [40] face the potential threats from Private Key Generator (PKG) and private key escrow problems. Therefore, based on this fact, Guan *et al*. [41] proposed a blockchain-assisted secure and lightweight authentication (BSLA) scheme which introduces the blockchain to solve the key escrow problem caused by the centralized PKG in the registration phase of the traditional identity-based AKA mechanisms.

3) Satellite-Satellite AKA

In the space segment, satellites can cooperate with each other to provide better services. In addition, it is challenging to obtain high-capacity communications over satellite-to-ground links, due to high transmission delay and rain attenuation. In contrast, inter-satellite links can overcome these issues. Moreover, the collaboration between satellites through inter-satellite links can reduce SATCOM systems' reliance on the ground and the number of GSs, which will reduce deployment costs. However, since the inter-satellite links are vulnerable to illegal attacks and different satellites do not trust each other, communication security is difficult to ensure. In 2020, Huang *et al*. [42] proposed a mutual authentication and key update scheme between satellites. Recently, Xiong *et al*. [43] proposed a blockchain-based trusted and privacy-preserved AKA scheme for inter-constellation cooperation in SATCOM systems, which focuses on the authentication process among satellites of different constellations. In 2022, Yang *et al*. [44] pointed out that the scheme in [42] cannot achieve PFS and protect the true identity of the satellite, and then proposed a lightweight location key-based AKA (LK-AKA) scheme for satellite-satellite communication and also an enhanced authentication scheme with PFS/PBS property, based on elliptic curve Diffie-Hellman (ECDH) key exchange algorithm.

C. Handover Authentication

Due to the ever-changing network topology of satellite constellations and the high mobility of users, handover frequently occurs in SATCOM systems. Moreover, the great coverage of Satellite Internet will cause a huge number of user handovers at the same time, which will degrade the communication performance. Due to the long communication links in SATCOM systems, re-performing a complete access authentication will not ensure a seamless handover of users. Also, using some lightweight but weak security mechanisms to implement fast handover provides more opportunities for attackers to compromise the confidentiality of past/future communications. Through handover authentication, users can ensure the legitimacy of the access point and secure subsequent communications. Consequently, handover authentication is always a significant issue in SATCOM systems, ensuring users seamlessly and securely switch between access points. According to the handover scenario, we divide the handover authentication schemes in SATCOM systems into inter&intra-satellite, inter-GS, and inter-network handover authentication.

1) Inter&Intra-Satellite Handover Authentication

Due to the mobility of satellites, a user terminal may change beams and eventually the satellite during the session with satellites [45]. The transfer of an ongoing session from one beam to the next one is named intra-satellite handover, and the transfer from a satellite to the next one is named inter-satellite handover. In 2019, Xue *et al*. [37] proposed a secure and efficient inter-satellite handover authentication scheme, which can support batch verification when a group of users switches to another satellite. They pointed out that the scheme in [37] was still not efficient and general enough, because it requires a satellite to send to the subsequent satellite the access control list of the identities of all legal users currently attached to it. In light of this, they proposed an improved scheme based on a group key shared among the satellites in [46]. Yao *et al*. [40] later proposed a multicast inter-satellite handover scheme, which has greatly reduced the computational delay and signalling overhead when a large number of users are involved in inter-satellite handover authentication. Furthermore, Guo *et al*. [47] mentioned that the scheme in [46] will lead to the possibility of impersonation attacks on users or satellites when the group key is lost, thus cannot meet the security requirements of device loss attacks and PFS. To address this issue, they proposed an inter-satellite handover authentication scheme based on ECC. Recently, Wang *et al*. [48] proposed a blockchain-based inter-satellite and intra-satellite handover authentication scheme, which takes the advantage of certificateless encryption and consortium blockchain to provide efficient signature querying and verification and lightweight key pair computation without revealing devices' information.

2) Inter-GS Handover Authentication

In the previous handover scenario, users switch between satellites instead of GSs. Consequently, there is no need to renegotiate a new session key with the GS. However, for users travelling at high speeds, such as trains and aircraft, handover will also occur between GSs, which called inter-GS handover.

In this scenario, a new session key must be renegotiated to avoid the previous communication content being captured by the new GS and ensure communication security between the user and the new GS. In [36], Meng *et al.* provided an extended mechanism for inter-GS handover authentication. Xue *et al.* [37] addressed the problem that high-speed users not only switch from the current satellite to a new satellite, but also from the current GS to a new GS, and proposed an efficient handover authentication mechanism based on ECC. Also, their scheme in [46] the inter-GS has achieved handover authentication for the Software-Defined Space Information Network (SD-SIN). Guo *et al.* [47] designed a multi-user batch handover authentication scheme in the inter-GS handover scenario, which can greatly reduce the computation overhead and delay.

3) Inter-Network Handover Authentication

Satellite Internet is a heterogeneous network, where users may switch between different types of access networks according to ever-changing communication requirements and environments. For example, users can switch to the space-based network to maintain a continuous network connection, or switch to the terrestrial-based network to obtain a high-throughput and low-latency communication service. The inter-network handover authentication ensures seamless and secure switching of users between different access networks. Cui *et al.* [49] proposed a new edge-computing-enabled, unified authentication framework for heterogeneous beyond 5G systems, which integrate terrestrial networks, aerial networks and satellite networks. It supports a secure inter-network handover authentication scheme that fully protects users' identity privacy. Wang *et al.* [50] proposed a lightweight and secure handover authentication scheme between heterogeneous networks based on the Chinese Remainder Theorem (CRT). This method, however, only considers switching from the ground network to the satellite network, while it does not take switching from the satellite network to the ground network into consideration. Recently, Liu *et al.* [51] proposed an efficient and secure handover authentication method for heterogeneous networks using a hierarchical group key distribution scheme. In this method, the combination of ECC and blind factors can achieve user anonymity and traceability, effectively preventing the leakage of users' private data.

D. Cross-Domain Authetication

Cross-domain authentication refers to the authentication performed when users obtain services between different domains, such as between foreign domains and home domains or between different companies, so as to prevent unauthorized users from accessing shared resources between different domains.In 2019, Yang *et al.* [52] first proposed an anonymous and fast roaming authentication protocol for SATCOM systems based on the q-Strong Diffie-Hellman (q-SDH) problem and elliptic curve digital signature algorithm (ECDSA), which realizes cross-domain authentication between a foreign domain and a home domain. However, Guo *et al.* [53] pointed out that Yang *et al.*'s scheme not only has some security problems, such as lack of user login authentication and dynamic temporary identity update mechanisms but also takes the satellite as a key node to bear the main cost of verifying the legitimacy of the user, which will affect the reliability and service life of the satellite. Then they proposed a new and more secure three-factor authentication scheme that supports not only the home domain but also cross-domain authentication. The three factors are smart card, password, and user biometrics. Liu *et al.* [54] also found that Yang *et al.*'s scheme requires all the remaining users to be involved in updating their private keys if they leave the group, which brings additional computation and communication overheads to users. To address this issue, they proposed a new decentralized cross-domain authentication scheme for SATCOM systems, where the authentication task is delegated to the satellites and a user only needs to keep one account to enjoy services from multiple companies. In this method, authentication delay can be significantly reduced due to less interaction, and the single point of failure can be prevented with a threshold signature technique. In addition, user privacy, including anonymity and unlinkability, can be achieved with zero-knowledge proof of knowledge techniques while malicious users can be detected.

E. Physical Layer Authentication (PLA)

Traditional authentication schemes usually use upper-layer authentication mechanisms based on cryptographic algorithms. However, there are certain restrictions on the upper-layer authentication mechanisms [55], [56]. First, the security based on cryptographic algorithms is achieved based on the principle that the calculation required to break it using the best current methods far exceeds the attacker's computing resource level. However, with the rapid development of computing power, the cryptography-based algorithm may gradually be cracked. Second, cryptography-based algorithms will introduce excessive transmission overhead, communication delay and power consumption, which is not feasible for devices such as satellites, IoT, and UAVs. Third, cryptography-based algorithms require the process of key distribution and management, which introduces high costs. Timely sharing of security keys in a heterogeneous network supporting a large number of devices like SATCOM systems is challenging. Recently, PLA has attracted the interest of numerous researchers, which authenticates the identity of a transmitting device by verifying the unique characteristics of the physical communication links or the device itself [57]. In the SATCOM scenario, using PLA, ground users can validate the satellite's authenticity through the satellite-to-user link. PLA in SATCOM systems is significantly challenging due to the particular characteristics of satellite-to-user links, including high fading, multi-path fading, strong Doppler effect, short link durations, and non-standard electronics features of satellite radio transducers [58]. It is currently a hot and promising research direction in Satellite Internet authentication schemes. Accordingly, we classify the present PLA schemes in SATCOM systems as follows.

1) Device-Based PLA

Device-based PLA exploits devices' radiometric features (i.e., hardware imperfections) for authentication. Even if the transmitting devices are made by the same vendor, the radiometric features are distinct and exclusive to each device. PLA based on device features, also known as radio fingerprinting, refers to detecting and extracting features from received signals to identify the transmitter uniquely. Recently, Oligeri *et al.* [58] proposed a device-based PLA scheme to classify Iridium satellites through the obtained signals from the satellites. The authors used a Universal Software Radio Peripheral (USRP) to collect signals from Iridium satellites and extract I/Q samples from the signals. After transforming the I/Q samples to grayscale images, the proposed PLA scheme applies a Convolutional Neural Network (CNN)-based classifier to achieve Iridium satellite identification. In this method, they considered two different classification scenarios, i.e., intra-constellation satellite authentication and satellite authentication in the wild, which adopt a CNN and an autoencoder to train the classifier, respectively.

2) Channel-Based PLA

There is a strong spatial decorrelation between the channel features of different transmitting devices [56]. Therefore, when the distance between the legitimate transmitter and the adversary is greater than half the wavelength, the transmitter-authenticator channel and adversary-authenticator channel will exhibit different features. Also, it is impossible for the adversary to obtain features of the transmitter-authenticator channel. Channel-based PLA thus relies on this principle to achieve authentication. More specifically, channel-based PLA utilizes the reciprocity and spatial uniqueness of wireless channel characteristics and realizes authentication by checking the similarity of wireless channel features in coherence time. In 2021, Fu *et al.* [59] proposed to use Doppler frequency shift as an available physical channel feature to authenticate the satellite transmitting source. In this method, Doppler can be calculated aforehand based on ephemeris and user location without other prior information, which is used for initial authentication. Topal *et al.* [60] also proposed a PLA method for the inter-satellite communication links of the LEO satellites based on Doppler frequency shift. They use multiple receiving satellites to validate the identity of the transmitting satellite by comparing the Doppler frequency measurements with the reference mobility information of the legitimate transmitter and then fuse the decisions from the multiple satellites to reach a final decision.

IV. Authentication in GNSS

GNSS is a satellite-based system that can provide positioning, navigation and timing (PVT) services for users on the ground worldwide. Today, major countries are vigorously developing their own GNSS systems, such as Global Positioning System (GPS) in the United States, BeiDou navigation satellite system (BDS) in China, Galileo in Europe, and the Global Navigation Satellite System (GLONASS) in Russia [13]. GNSS is, in principle, vulnerable to kinds of attacks, especially spoofing attacks, like SATCOM systems. Therefore, designing authentication schemes to resist spoofing attacks has become a hot research topic in the GNSS field. Based on the existing literature, we briefly divide authentication schemes in GNSS into two sub-categories: message-level and signal-level authentication.

A. Message-Level Authentication

1) Navigation Message Authentication (NMA)

In NMA, a sender encrypts the navigation message bits (partial navigation message parameters or all navigation message parameters) through an encryption algorithm and inserts the generated ciphertext information into the reserved bits of the navigation message. On the receiver side, the key is used to decrypt the received ciphertext and verify whether the sender is legal according to the decryption result, fulfilling the goal of resisting spoofing attacks. In general, NMA techniques rely on asymmetric cryptography, based on one-way functions [61].

Digital Signature. One of the most commonly used asymmetric encryption methods for NMA is the digital signature. In this method, NMA uses digital signature techniques based on PKI to prove the authenticity of GNSS signals by periodically embedding signatures in unencrypted navigation messages. Digital signature algorithms, such as RSA, digital signal algorithm (DSA), and ECDSA, are often used for this purpose. Wesson *et al.* [62] provided an evaluation of the potential digital signature algorithms that could generate the signed navigation message, which helps to find the most effective and practical algorithm for GPS signal authentication. They proposed a scheme that embeds digital signatures generated by the ECDSA algorithm in GPS civil navigation (CNAV) messages and exploited a statistical hypothesis test to secure civil GPS receivers against replay-type spoofing attacks. Chino *et al.* [63] proposed an NMA scheme using the RSA algorithm to generate ciphertext information for the quasi-zenith satellite system (QZSS) and then built an experimental platform for spoofing attacks to detect anti-spoofing performance. However, they do not take some security aspects, such as key management and signal transmission protocol, into account. In 2019, Wu *et al.* [64] proposed an NMA scheme for BeiDou-II Navigation Satellite System based on the ECDSA algorithm. Furthermore, the overall process of key update and transmission is also designed through the short message service or digital certificate. Simulation results were also provided to show the anti-spoofing performance. Later, they proposed a new NMA scheme [65] based on certificateless signature, which effectively solves the key escrow problem, for BeiDou Navigation Satellite System. However, digital signatures based on asymmetric encryption are more computationally expensive than symmetric encryption, especially for GNSS with a large amount of data.

TESLA. TESLA [66] is a protocol that adopts a symmetric encryption algorithm and utilizes a delayed key disclosure technology to realize asymmetric encryption. It addresses the issue of the high authentication overhead of asymmetric encryption and the low security of symmetric encryption.The core idea of TESLA is the delayed disclosure of keys, where a symmetric key is disclosed at a time interval later after the message and the MAC generated using the key is broadcast to the receivers. Using the disclosed key, the receivers can authenticate the message. Fernández-Hernández *et al.* [67] presented an NMA scheme based on a modified TESLA for the Galileo Open Service. In this scheme, a single one-way chain is used for all satellites, which allows for cross-authentication of neighbouring satellites by a given satellite. The receiver only needs to receive this key from any satellite to perform identity authentication. Their scheme enhances the robustness to data loss, but cannot resist replay spoofing attacks in some scenarios. Ghorbani *et al.* [68] proposed an NMA scheme based on TESLA for GPS in which two techniques of TESLA were implemented using reserved bits for GPS L1 data. Wu *et al.* [69] proposed an NMA scheme based on the combination of SM commercial cryptographic algorithms and TESLA for the BeiDou navigation system. In this method, they use the SM2 algorithm to protect and encrypt time information in the TESLA key chain to prevent replay attacks. In 2021, Fernández-Hernández *et al.* [70] provided an analysis of the length of MACs and hash-derived cryptographic keys for TESLA applied to GNSS. A key size of 96 or more is suggested. However, the TESLA-based NMA schemes require strict time synchronization between the sender and receiver.

Combination of Digital Signature and TESLA. In order to improve the performance of the NMA schemes and the reliability of the transmissions, some researchers focus on the combination of the digital signature algorithm and the TESLA protocol. Kerns *et al.* [71] first proposed a hybrid ECDSA-TESLA NMA scheme for GPS CNAV messages. They also compared the advantages and disadvantages of ECDSA and TESLA. Due to the combination of these two methods, the hybrid ECDSA-TESLA NMA scheme greatly reduces the overhead while preserving cryptographic authentication of navigation data for all users. Yang *et al.* [72] also proposed an NMA scheme based on the combination of ECDSA and TESLA to protect BeiDou civilian navigation information. In this scheme, the ECDSA algorithm is used to ensure the reliability of information during transmission, and the TESLA protocol is used to improve authentication efficiency. Combining the digital signature algorithm with the TESLA protocol has achieved outstanding performance, but how to combine these two to optimize the anti-spoofing effect still needs further research.

2) Spreading Code Authentication (SCA)

SCA is a cryptography-based scheme that protects the unencrypted and public spreading code by inserting unpredictable portions (i.e., encrypted chips or watermarking sequences) into the spreading code. Since the power of the GNSS spread spectrum signal is lower than the power of the thermal noise signal (around 20 dB lower), SCA chips are difficult to observe by a spoofer unless the spoofer has the cryptographic information to generate unpredictable chips. However, the spreading code authentication process is a posterior process, which introduces a latency between the ground control segment transmitting unpredictable chips and the receiver receiving unpredictable chips [61]. Kuhn [73] proposed an SCA scheme based on hidden markers. The hidden marker is a rectangular pulse of duration δ, broadcast with direct sequence spread spectrum (DSSS) modulation using a previously unpublished spreading sequence. The receiver can detect complex spoofing attacks by recording the arrival time of the hidden makers. Pozzobon *et al.* [74] proposed an SCA scheme based on signal authentication sequence (SAS) generated by the stream cipher. The proposed method requires a minimum impact on the system design, as only the data subsystem would be affected in a hypothetical update. Pozzobon *et al.* [75] further presented a novel SCA scheme for open GNSS signal authentication using supersonic codes, which provides hybrid authentication. This scheme achieves fast authentication and provides additional bandwidth for GNSS services. In 2021, Wang *et al.* [76] pointed out that the SCA schemes mentioned above change the signal structure, degrade the correlation of the spreading code, and cause performance loss. Then, they proposed a binary phase hopping-based SCA scheme, which can achieve identity authentication without changing the existing signal structure.

B. Signal-Level Authentication

Signal-level authentication is achieved by detecting the differences between a spoofing signal and a real signal. Existing works on signal-level authentication can be classified into signal quality-based and additional hardware-based.

1) Signal Quality-based Schemes

Signal quality-based schemes are designed to detect spoofing attacks by looking for distortion or interference at various stages of signal processing. These approaches differ from cryptographic methods in that they do not require modifications to the existing signal structure but only the update of the device firmware. One approach is called signal power monitoring, which detects spoofing signals by inspecting the carrier-to-noise ratio (C/N_0), absolute signal power value, receiver power variation for receiver movement, or difference between the L1 and L2 signal power levels [77]. Dehghanian *et al.* [78] proposed a signal power monitoring technique that utilizes C/N_0 measurements to detect spoofing attacks. Akos *et al.* [79] also proposed a scheme that monitors the total received power via the automatic gain control (AGC) setpoint. Since the spoofer requires a substantial power advantage to attack, a sudden power jump could indicate the attack. Later, Wesson *et al.* [80] pointed out that the scheme in [79] cannot detect a low-power spoofer and distinguish between spoofing and jamming. Therefore, they proposed a GNSS signal authentication technique called power-distortion detector, which combines the detection of anomalous received power and the detection of correlation profile distortion.

Another approach is signal consistency monitoring, which detects spoofing signals by inspecting the code, carrier, and Doppler consistency. Recently, Li *et al.* [81] proposed a method against single antenna spoofing jamming utilizing the Fréchet distance of Doppler frequency shift difference (DFSD). When the receiver moves randomly, the correlation between two authentic satellite signals is small, while the spoofing signals are with a high correlation. By comparing the DFSD data between two signals using the Fréchet distance method, the spoofing signal and the authentic signal can be detected and recognized. However, signal consistency monitoring may bring a heavy signal processing burden to receivers. There also exist some other kinds of signal processing-based schemes, such as vestigial signal defense (VSD) [82], time of arrival (ToA) monitoring [83], and receiver autonomous integrity monitoring (RAIM) [84].

2) Additional Hardware-based Schemes

Additional hardware-based schemes usually require some additional hardware, such as additional receivers, antenna arrays, inertial sensors, and communication infrastructures, to detect spoofing attacks. Psiaki *et al.* [85] and Heng *et al.* [86] proposed two signal authentication schemes that use cross-correlations of encrypted/military GPS signals between two or several receivers to detect spoofing attacks. In their methods, a low cross-correlation indicates the presence of a spoofing attack. This type of detection method is the strongest known defense against sophisticated spoofing attacks if the defended receiver has only one antenna. However, they require receivers to establish secure communication links to perform cross-correlation. Daneshmand *et al.* [87] proposed a low-complexity approach to detect the spoofing signals utilizing an antenna array processing technique based on the assumption that all spoofing signals arriving at the antenna array are all from the same direction. Similarly, Zhao *et al.* [88] presented a spatial-temporal scheme based on the antenna array , which can distinguish not only low-power spoofing from multiple paths but also provides advanced signal processing methods for multi-path phenomenon and spoofing mitigation. The antenna array-based methods are effective against almost all spoofing attacks unless a spoofer can attack with multiple coordinated spoofers. However, these methods require multiple antennas, which might be too expensive to deploy and incurs a heavy computational load on the receivers.

Moreover, many schemes have been proposed using inertial sensors. These methods leverage the fact that GNSS sensors are vulnerable to spoofing, but inertial sensors are less accessible to attacks and thus able to reveal attacks through proper consistency check [89]. Ceccato *et al.* [90] proposed a spoofing detection technique based on the comparison between GNSS and inertial measurement unit (IMU) measurements through a generalized likelihood ratio test (GLRT). Similar to the antenna array-based methods, this method is significantly efficient. However, using inertial sensors increases the size, weight, or cost of the receivers and requires specialized hardware. Recently, some approaches have been introduced utilizing other communication infrastructures, such as cellular networks and IRIDIUM satellite constellation. These methods exploit the location services of other network infrastructure to relocate the receivers and compare this location to that of GPS to detect spoofing. Oligeri *et al.* [91] proposed a scheme that exploits the strength of signals received by the mobile cellular network to estimate the positions of vehicles. Spoofing attacks are then detected by comparing the estimated positions with the vehicles' GPS positions. Later, they proposed another scheme that utilizes unencrypted IRIDIUM Ring Alert (IRA) messages broadcast by IRIDIUM satellites to estimate the receivers' locations [92].

V. Challenges and Future Directions

Although authentication in Satellite Internet has received much attention in recent years, many open issues still require further investigation. In this section, we discuss the opportunities and challenges in satellite authentication and also some promising research directions.

A. Deep Learning-Based PLA

PLA in Satellite Internet is currently a hot research topic. It utilizes the unique characteristics of physical communication links and devices, which are difficult to mimic, to authenticate the entities in the Satellite Internet. PLA has the advantages of low complexity, low processing delay, high compatibility and a high level of security. However, existing Satellite Internet systems always achieve security only via a certain upper-layer authentication scheme, and there is still little literature on PLA in Satellite Internet. With the development of deep learning in wireless communications, more and more researchers are focusing on its application in satellite authentication. In the context of the Satellite Internet, deep learning techniques can be used to identify physical-layer characteristics of signals emitted by satellites and distinguish between authentic signals and spoofing signals. For example, the scheme in [58] utilizes CNN to extract unique fingerprints from signals received from IRIDIUM LEO satellites and authenticate satellite transmitters. Also, the scheme in [95] leverages the potential of deep ensemble methods and the statistical features of path losses between UAVs and base stations to detect GPS spoofing for cellular-connected UAVs. Owing to the benefits of PLA and deep learning, we expect that deep learning-based PLA for satellites is a promising research direction.

B. Cross Layer Authentication

PLA is not intended to replace upper-layer authentication, but rather to serve as a complement, so as to achieve higher security. The cross-layer scheme with both authentication schemes is necessary to defend against increasingly powerful attacks. More specifically, upper-layer authentication is used to authenticate the user's identification, and the PLA is used to authenticate the user's device. However, combining the two authentication mechanisms properly has become an urgent problem to solve. One research direction of this problem is to find a unified authentication metric between upper-layer authentication schemes and PLA schemes. Another research direction is to use physical layer features to generate keys for upper-layer authentication. Although some initial efforts have been devoted to terrestrial networks [93], [94], cross-layer authentication in Satellite Internet still remains unexplored, which is expected to be a significant research direction in the future.

VI. Conclusion

In this paper, we have provided a comprehensive survey on the authentication schemes for improving the security of the Satellite Internet, for which we introduced the existing authentication schemes from two scenarios respectively, e.g., SATCOM and GNSS. We further divide the works for SATCOM systems into five sub-categories: SMA, AKA, handover authentication, cross-domain authentication and PLA, and those for GNSS into two sub-categories: message-level authentication and signal-level authentication. Finally, we introduced some potential challenges and promising future directions for authentication in Satellite Internet.

VII. Acknowledgements

This work was supported in part by the National Natural Science Foundation of China under Grant 62202354, 62202354, Qin Chuangyuan Innovation and Entrepreneurship Talent Project of Shannxi (Grant No. QCYRCXM-2022-144), the National Natural Science Foundation of China under grant No. 62220106004, the Natural Science Basic Research Program of Shaanxi under Grant No. 2019JC-17, the Key Research and Development Program of Shaanxi under Grant No. 2022KXJ-093, and the Basic and Applied Basic Research Fund of Guangdong Province (Grant No. 2021A1515111017).

References

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

[2] H. Guo, J. Li, J. Liu, N. Tian and N. Kato, "A survey on Space-Air-Ground-Sea integrated network security in 6G," *IEEE Communications Surveys Tutorials*, vol. 24, no. 1, pp. 53-87, Firstquarter 2022.

[3] P. Tedeschi, S. Sciancalepore, and R. D. Pietro, "Satellite-based communications security: A survey of threats, solutions, and research challenges," *Computer Networks*, vol. 216, Oct. 2022.

[4] X. Zhu and C. Jiang, "Integrated Satellite-Terrestrial networks toward 6G: architectures, applications, and challenges," *IEEE Internet of Things Journal*, vol. 9, no. 1, pp. 437-461, 1 Jan. 2022.

[5] J. C. McDowell, "The low earth orbit satellite population and impacts of the SpaceX Starlink constellation," *The Astrophysical Journal Letters*, vol. 892:L36, no. 2, pp. 1-10, Apr. 2020.

[6] Y. Henri, "The OneWeb satellite system," *Handbook of Small Satellites: Technology, Design, Manufacture, Applications, Economics and Regulation*, pp. 1-10, Aug. 2020.

[7] I. del Portillo Barrios, B. Cameron, and E. Crawley, "A technical comparison of three low earth orbit satellite constellation systems to provide global broadband," *Acta Astronautica*, vol. 159, Jun. 2019.

[8] Y. Meng, L. Bian, L. Han, W. Lei, T. Yan, M. He, and X. Li, "A global navigation augmentation system based on LEO communication constellation," in *Proc. Eur. Navig. Conf. (ENC)*, Gothenburg, Sweden, May 2018, pp. 65-71.

[9] H. Cao, L. Wu, Y. Chen, Y. Su, Z. Lei, and C. Zhao, "Analysis on the security of Satellite Internet," in *China Cyber Security Annual Conference*, Springer, Singapore, Aug. 2020, pp. 193-205.

[10] B. Li, Z. Fei, C. Zhou and Y. Zhang, "Physical-layer security in space information networks: a survey," *IEEE Internet of Things Journal*, vol. 7, no. 1, pp. 33-52, Jan. 2020.

[11] Z. Wu, Y. Zhang, Y. Yang, C. Liang and R. Liu, "Spoofing and anti-spoofing technologies of global navigation satellite system: a survey," *IEEE Access*, vol. 8, pp. 165444-165496, Sep. 2020.

[12] J. Zidan, E. I. Adegoke, E. Kampert, S. A. Birrell, C. R. Ford and M. D. Higgins, "GNSS vulnerabilities and existing solutions: a review of the literature," *IEEE Access*, vol. 9, pp. 153960-153976, 2021.

[13] L. Meng, L. Yang, W. Yang, and L. Zhang, "A survey of GNSS spoofing and anti-spoofing technology," *Remote Sensing*, vol. 14, no. 19, p. 4826, Sep. 2022.

[14] L. Jianwei, L. Weiran, W. Qianhong, L. Dawei and C. Shigang, "Survey on key security technologies for space information networks," *Journal of Communications and Information Networks*, vol. 1, no. 1, pp. 72-85, June 2016.

[15] S. Sanders, GEO, MEO, and LEO: How orbital altitude impacts network performance in satellite datea services, Via Satellite, May. 2020. [Online]. Available: https://www.satellitetoday.com/content-collection/ses-hub-geo-meo-and-leo

[16] J. Bailey, LEO, GEO, MEO Satellites-What's the difference?, Simple Flying, Mar. 2020. [Online]. Available: https://simpleflying.com/leo-geo-meo-satellites-whats-the-difference

[17] B. Shang, Y. Yi, and L. Liu, "Computing over space-air-ground integrated networks: Challenges and opportunities," *IEEE Network*, vol. 35, no. 4, pp. 302-309, July/August 2021.

[18] A. Sharma, P. Vanjani, N. Paliwal, "Communication and networking technologies for UAVs: A survey," *Journal of Network and Computer Applications*, vol. 168, Oct. 2020, Art. no. 102739.

[19] M. Conti and S. Giordano, "Mobile ad hoc networking: milestones, challenges, and new research directions," *IEEE Communications Magazine*, vol. 52, no. 1, pp. 85-96, Jan. 2014.

[20] S.-L. Tsao and C.-H. Huang, "A survey of energy efficient MAC protocols for IEEE 802.11 WLAN," *Computer Communications*, vol. 31, pp. 54-67, Jan. 2011.

[21] I. Papapanagiotou, D. Toumpakaris, J. Lee, and M. Devetsikiotis, "A survey on next generation mobile WiMAX networks: objectives, features and technical challenges," *IEEE Communications Surveys Tutorials*, vol. 11, no. 4, pp. 3-18, , Dec. 2009.

[22] A. Roy-Chowdhury and J. S. Baras, "A lightweight certificate-based source authentication protocol for group communications in hybrid wireless/satellite networks," in *Proceedings of Global Telecommunications Conference, 2008. IEEE GLOBECOM 2008. IEEE*, Dec. 2008, pp. 1-6.

[23] A. Roy-Chowdhury and J. S. Baras, "A certificate-based light-weight authentication algorithm for resource-constrained devices," Center for Satellite and Hybrid Communication Networks, University of Maryland College Park, Tech. Rep. CSHCN TR 2005-4, 2005.

[24] A. Roy-Chowdhury and J. S. Baras, "Energy-efficient source authentication for secure group communication with low-powered smart devices in hybrid wireless/satellite networks," *EURASIP Journal on Wireless Communications and Networking*, Dec. 2011.

[25] T.-H. Chen, W.-B. Lee, and H.-B. Chen, "A self-verification authentication mechanism for mobile satellite communication systems," *Computers Electrical Engineering*, vol. 35, no. 1, pp. 42-48, Jan. 2009.

[26] I. Lasc, R. Dojen, and T. Coffey, "Countering jamming attacks against an authentication and key agreement protocol for mobile satellite communications," *Computers Electrical Engineering*, vol. 37, no. 2, pp. 160-168, Mar. 2011.

[27] C.-C. Chang, T.-F. Cheng, and H.-L. Wu, "An authentication and key agreement protocol for satellite communications," *International Journal of Communication Systems*, vol. 27, no. 10, pp. 1994-2006, Oct. 2014.

[28] C.-C. Lee, C.-T. Li, and R.-X. Chang, "A simple and efficient authentication scheme for mobile satellite communication systems," *International Journal of Satellite Communications and Networking*, vol. 30, no. 1, pp. 29-38, Jan. 2012.

[29] A. D. Jurcut, J. Chen, A. Kalla, M. Liyanage and J. Murphy, "A novel authentication mechanism for mobile satellite communication systems," in *IEEE Wireless Communications and Networking Conference Workshop (WCNCW)*, 2019, pp. 1-7.

[30] I. Altaf, M. A. Saleem, K. Mahmood, S. Kumari, P. Chaudhary and C.-M. Chen, "A lightweight key agreement and authentication scheme for Satellite-Communication systems," *IEEE Access*, vol. 8, pp. 46278-46287, Mar. 2020.

[31] S. Xu, X. Liu, M. Ma and J. Chen, "An improved mutual authentication protocol based on perfect forward secrecy for satellite communications," *International Journal of Satellite Communications and Networking*, vol. 31, no. 1, pp. 62-73, Jan. 2020.

[32] H. Huang, X. Miao, Z. Wu, and Q. Wei, "An efficient ECC-based authentication scheme against clock asynchronous for spatial information network," *Mathematical Problems in Engineering*, vol. 2021, Feb. 2021, Art. no. 8811970.

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

[34] U. Kumar, and M. Garg, "Learning with error-based key agreement and authentication scheme for satellite communication," *International Journal of Satellite Communications and Networking*, vol. 40, no. 2, pp. 83-95, Mar. 2022.

[35] D. Dharminder, P. K. Dadsena, P. Gupta, and S. Sankaran, "A post quantum secure construction of an authentication protocol for satellite communication," *Proceedings of International Journal of Satellite Communications and Networking*, Jul. 2022.

[36] W. Meng, K. Xue, J. Xu, J. Hong, and N. Yu, "Low-latency authentication against satellite compromising for space information network," in *IEEE 15th International Conference on Mobile Ad Hoc and Sensor Systems (MASS)*, 2018, pp. 237-244.

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

[38] Z. Yi, X. Du, Y. Liao and X. Lu, "An access authentication algorithm based on a hierarchical identity-based signature over lattice for the space-ground integrated network," in *Proceedings of International Conference on Advanced Communication Technologies and Networking (CommNet)*, Apr. 2019, pp. 1-9.

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

[40] S. Yao, J. Guan, Y. Wu, K. Xu and M. Xu, "Toward secure and lightweight access authentication in SAGINs," *IEEE Wireless Communications*, vol. 27, no. 6, pp. 75-81, Dec. 2020.

[41] J. Guan, Y. Wu, S. Yao, T. Zhang, X. Su, and C. Li, "BSLA: blockchain-assisted secure and lightweight authentication for SGIN," *Computer Communications*, vol. 176, p. 46-55, Aug. 2021.

[42] C. Huang, Z. Zhang, M. Li, L. Zhu, Z. Zhu, and X. Yang, "A mutual authentication and key update protocol in satellite communication network," *Automatika*, vol. 61, no. 3, pp. 334-344, Jul. 2020.

[43] T. Xiong, R. Zhang, J. Liu, T. Huang, Y. Liu, and F. R. Yu, "A blockchain-based and privacy-preserved authentication scheme for inter-constellation collaboration in Space-Ground Integrated Networks," *Computer Networks*, vol. 206, Apr. 2022.

[44] Y. Y, J. Cao, X. Ren, B. Niu, Y. Zhang, and H. Li, "LK-AKA: A lightweight location key-based authentication and key agreement protocol for S2S communication," *Computer Communications*, Nov. 2022.

[45] G. Maral, J. Restrepo, E. del Re, R. Fantacci and G. Giambene, "Performance analysis for a guaranteed handover service in an LEO constellation with a "satellite-fixed cell" system," *IEEE Transactions on Vehicular Technology*, vol. 47, no. 4, pp. 1200-1214, Nov. 1998.

[46] K. Xue, W. Meng, H. Zhou, D. S. L. Wei and M. Guizani, "A lightweight and secure group key based handover authentication protocol for the software-defined Space Information Network," *IEEE Transactions on Wireless Communications*, vol. 19, no. 6, pp. 3673-3684, Jun. 2020.

[47] J. Guo, Y. Zhang, and M. Li, "A provably secure ECC-based access and handover authentication protocol for space information networks," *Journal of Network and Computer Applications*, vol. 193, Nov. 2021.

[48] B. Wang, Z. Chang, S. Li and T. Hämäläinen, "An efficient and privacy-preserving blockchain-based authentication scheme for low earth orbit satellite assisted Internet of Things," *IEEE Transactions on Aerospace and Electronic Systems*, Jun. 2022.

[49] Q. Cui, Z. Zhu, W. Ni, X. Tao and P. Zhang, "Edge-intelligence-empowered, unified authentication and trust evaluation for heterogeneous beyond 5G systems," *IEEE Wireless Communications*, vol. 28, no. 2, pp. 78-85, Apr. 2021.

[50] Y. Wang, W. Zhang and X. Wang, "A lightweight and secure authentication protocol for Space-Ground Integrated Network of railway," in *International Conference on Communications, Information System and Computer Engineering (CISCE)*, May. 2021, pp. 30-35.

[51] Y. Liu, L. Ni and M. Peng,"A Secure and Efficient Authentication Protocol for Satellite-Terrestrial Networks," *IEEE Internet of Things Journal*, Feb. 2022.

[52] Q. Yang, K. Xue, J. Xu, J. Wang, F. Li and N. Yu, "AnFRA: Anonymous and Fast Roaming Authentication for Space Information Network," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 2, pp. 486-497, Feb. 2019.

[53] J. Guo, and Y. Du, "A secure three-factor anonymous roaming authentication protocol using ECC for space information networks," *Peer-to-Peer Networking and Applications*, vol. 14, no. 2, pp. 898-916, Mar. 2021.

[54] X. Liu, A. Yang, C. Huang, Y. Li, T. Li and M. Li, "Decentralized anonymous authentication with fair billing for Space-Ground Integrated Networks," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 8, pp. 7764-7777, Aug. 2021.

[55] X. Wang, P. Hao and L. Hanzo, "Physical-layer authentication for wireless security enhancement: current challenges and future developments," *IEEE Communications Magazine*, vol. 54, no. 6, pp. 152-158, Jun. 2016.

[56] N. Xie, Z. Li and H. Tan, "A survey of physical-layer authentication in wireless communications," *IEEE Communications Surveys Tutorials*, vol. 23, no. 1, pp. 282-310, 1st Quart., 2021.

[57] N. Xie, J. Chen and L. Huang, "Physical-layer authentication using multiple channel-based features," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 2356-2366, Jan. 2021.

[58] G. Oligeri, S. Sciancalepore, S. Raponi and R. Di Pietro, "PAST-AI: Physical-layer authentication of satellite transmitters via deep learning," *IEEE Transactions on Information Forensics and Security*, Nov. 2022.

[59] Q.-Y. Fu, Y.-H. Feng, H.-M. Wang and P. Liu, "Initial satellite access authentication based on Doppler Frequency shift," in IEEE Wireless Communications Letters, vol. 10, no. 3, pp. 498-502, March 2021.

[60] O. A. Topal and G. Karabulut Kurt, "Physical layer authentication for LEO satellite constellations," *Proceedings of IEEE Wireless Communications and Networking Conference (WCNC)*, Apr. 2022, pp. 1952-1957.

[61] D. Margaria, B. Motella, M. Anghileri, J.-J. Floch, I. Fernandez-Hernandez and M. Paonni, "Signal structure-based authentication for civil GNSSs: recent solutions and perspectives," *IEEE Signal Processing Magazine*, vol. 34, no. 5, pp. 27-37, Sep. 2017.

[62] K. Wesson, M. Rothlisberger, and T. Humphreys, "Practical cryptographic civil GPS signal authentication," *NAVIGATION: Journal of the Institute of Navigation*, vol. 59, no. 3, pp. 177-193, Sep. 2012.

[63] K. Chino, D. Manandhar and R. Shibasaki, "Authentication technology using QZSS," in *Proceedings of IEEE/ION Position, Location and Navigation Symposium (PLANS)*, May. 2014, pp. 367-372.

[64] Z. Wu, R. Liu and H. Cao, "ECDSA-based message suthentication dcheme for BeiDou-II navigation satellite system," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 55, no. 4, pp. 1666-1682, Aug. 2019.

[65] Z. Wu, and Y. Yang, "BD-D1Sec: Protocol of security authentication for BeiDou D1 civil navigation message based on certificateless signature," *Computers Security*, vol. 105, Jun. 2021.

[66] A. Perrig, R. Canetti, J. D. Tygar, D. Song, "The TESLA broadcast authentication protocol," *RSA CryptoBytes*, vol. 5, no. 2, pp. 2–13, 2002.

[67] I. Fernández-Hernández, V. Rijmen, G. Seco-Granados, J. Simon, I. Rodríguez, and J. D. Calle, "A navigation message authentication proposal for the galileo open service," *Navigation: Journal of the Institute of Navigation*, vol. 63, no. 1, pp. 85-102, Mar. 2016.

[68] K. Ghorbani, N. Orouji, and M. R. Mosavi, "Navigation message authentication based on one-way hash chain to mitigate spoofing attacks for GPS L1," *Wireless Personal Communications*, vol. 113, no. 4, pp. 1743-1754, Aug. 2020.

[69] Z. Wu, Y. Zhang, L. Liu and M. Yue, "TESLA-based authentication for BeiDou civil navigation message," *China Communications*, vol. 17, no. 11, pp. 194-218, Nov. 2020.

[70] I. Fernández-Hernández, T. Ashur and V. Rijmen, "Analysis and recommendations for MAC and key lengths in delayed disclosure GNSS authentication protocols," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 57, no. 3, pp. 1827-1839, Jun. 2021.

[71] A. J. Kerns, K. D. Wesson and T. E. Humphreys, "A blueprint for civil GPS navigation message authentication," in *Proceedings of IEEE/ION Position, Location and Navigation Symposium (PLANS)*, May. 2014, pp. 262-269.

[72] M. Yuan, Z. Lv, H. Chen, J. Li, and G. Ou, "An implementation of navigation message authentication with reserved bits for civil BDS anti-spoofing," in *China Satellite Navigation Conference (CSNC)*, vol. 2, May. 2017, pp. 69-80.

[73] M. G. Kuhn, "An asymmetric security mechanism for navigation signals," in *International workshop on information hiding*, May. 2004, pp. 239-252.

[74] O. Pozzobon, L. Canzian, M. Danieletto and A. D. Chiara, "Anti-spoofing and open GNSS signal authentication with signal authentication sequences," *Proceedings of ESA Workshop on Satellite Navigation Technologies and European Workshop on GNSS Signals and Signal Processing (NAVITEC)*, 2010, pp. 1-6.

[75] O. Pozzobon, G. Gamba, and M. Canale, "From data schemes to supersonic codes. GNSS authentication for modernized signals," *Inside GNSS*, vol. 10, no. 1, pp. 55-64, Jan. 2015.

[76] S. Wang, H. Liu, Z. Tang, and B. Ye, "Binary phase hopping based spreading code authentication technique," *Satellite Navigation*, vol. 2, no. 1, pp. 1-9, Dec. 2021.

[77] S. Jeong, M. Kim, and J. Lee, "CUSUM-based GNSS spoofing detection method for users of GNSS augmentation system," *International Journal of Aeronautical and Space Sciences*, vol. 21, no. 2, pp. 512-535, Jun. 2020.

[78] V. Dehghanian, J. Nielsen, and G. Lachapelle, "GNSS spoofing detection based on receiver C/No estimates," in *Proceedings of International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS)*, Sep. 2012, pp. 2878-2884.

[79] D. M. Akos, "Who's afraid of the spoofer? GPS/GNSS spoofing detection via automatic gain control (AGC)," *Journal of the Institute of Navigation*, vol. 59, no. 4, pp. 281-290, Dec. 2012.

[80] K. D. Wesson, J. N. Gross, T. E. Humphreys and B. L. Evans, "GNSS signal authentication via power and distortion monitoring," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 54, no. 2, pp. 739-754, Apr. 2018.

[81] J. Li, X. Zhu, M. Ouyang, D. Shen, Z. Chen, and Z. Dai, "GNSS spoofing detection technology based on Doppler frequency shift difference correlation," *Measurement Science and Technology*, vol. 33, no. 9, Jun. 2022.

[82] K. D. Wesson, D. P. Shepard, J. A. Bhatti, and T. E. Humphreys, "An evaluation of the vestigial signal defense for civil GPS anti-spoofing," in *Proceedings of International Technical Meeting of the Satellite Division of The institute of navigation (ION GNSS)*, Sep. 2011, pp. 2646-2656.

[83] Q. Zeng, H. Li and L. Qian, "GPS spoofing attack on time synchronization in wireless networks and detection scheme design," in *IEEE Military Communications Conference (MILCOM)*, 2012, pp. 1-5.

[84] J. Li, H. Li, and M. Lu, "One-dimensional traversal receiver autonomous integrity monitoring method based on maximum likelihood estimation for GNSS anti-spoofing applications," *IET Radar Sonar Navigation*, vol. 14, no. 12, pp. 1888-1896, Dec. 2020.

[85] M. Psiaki, B. O'Hanlon, J. Bhatti, D. Shepard, and T. Humphreys, "Civilian GPS spoofing detection based on dual-receiver correlation of military signals," in *Proceedings of International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS)*, Sep. 2011, pp. 2619-2645.

[86] L. Heng, D. B. Work and G. X. Gao, "GPS signal authentication from cooperative peers," *IEEE Transactions on Intelligent Transportation Systems*, vol. 16, no. 4, pp. 1794-1805, Aug. 2015.

[87] S. Daneshmand, A. Jafarnia-Jahromi, A. Broumandon, and G. Lachapelle, "A low-complexity GPS anti-spoofing method using a multi-antenna array," in *Proceedings of International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS)*, Sep. 2012, pp. 1233-1243.

[88] Y. Zhao, F. Shen, G. Xu, and G. Wang, "A spatial-temporal approach based on antenna array for GNSS anti-spoofing," *Sensors*, vol. 21, no. 3, p. 929, Jan. 2021.

[89] J. T. Curran and A. Broumendan, "On the use of low-cost IMUs for GNSS spoofing detection in vehicular applications," in *International Technical Symposium on Navigation and Timing (ITSNT)*, Toulouse, France, Nov. 2017.

[90] M. Ceccato, F. Formaggio, N. Laurenti and S. Tomasin, "Generalized likelihood ratio test for GNSS spoofing detection in devices with IMU," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 3496-3509, 2021.

[91] G. Oligeri, S. Sciancalepore, O. A. Ibrahim, and R. Di Pietro, "Drive me not: GPS spoofing detection via cellular network: (architectures, models, and experiments)," in *Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks*, May. 2019, pp. 12-22.

[92] G. Oligeri, S. Sciancalepore, and R. Di Pietro, "GNSS spoofing detection via opportunistic IRIDIUM signals," in *Proceedings of the 13th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, Jul. 2020, pp.42-52.

[93] Y. Lee, J. Yoon, J. Choi and E. Hwang, "A novel cross-layer authentication protocol for the Internet of Things," *IEEE Access*, vol. 8, pp. 196135-196150, Oct. 2020.

[94] D. Xu, K. Yu and J. A. Ritcey, "Cross-layer device authentication with quantum encryption for 5G enabled IIoT in industry 4.0," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 9, pp. 6368-6378, Sep. 2022.

[95] Y. Dang, C. Benzaïd, B. Yang, T. Taleb and Y. Shen, "Deep ensemble learning based GPS dpoofing detection for cellular-connected UAVs," *IEEE Internet of Things Journal*, Aug. 2022.