Author(s): Wang, Biying; Chang, Zheng; Li, Shancang; Hämäläinen, Timo

Title: An Efficient and Privacy-Preserving Blockchain-Based Authentication Scheme for Low Earth Orbit Satellite Assisted Internet of Things

Year: 2022

Version: Accepted version (Final draft)

Please cite the original version:

Wang, B., Chang, Z., Li, S., & Hämäläinen, T. (2022). 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, 58(6), 5153-5164. https://doi.org/10.1109/TAES.2022.3187389

An Efficient and Privacy-Preserving Blockchain-based Authentication Scheme for Low Earth Orbit Satellite assisted Internet of Things

Biying Wang, *Student Member, IEEE,* Zheng Chang, *Senior Member, IEEE,* Shancang Li, *Sebior Member, IEEE*
and Timo Hämäläinen, *Senior Member, IEEE,*

***Abstract*—Recently, integrating satellite networks (e.g. Low-earth-orbit satellite constellation) into the Internet of Things (IoT) ecosystem has emerged as a potential paradigm to provide more reliable, ubiquitous and seamless network services. The LEO satellite networks serves as a key enabler to transform the connectivity across industries and geographical border. Despite the convenience brought from the LEO satellite networks, it arises security concerns, in which the essential one is to secure the communication between the IoT devices and the LEO satellite network. However, some challenges inheriting from the LEO satellite networks need to be considered : 1) the dynamic topology; 2) the resource-constraint satellites; 3) the relative long latency; 4) multiple beams authentication. In particular, the centralized authentication schemes are no longer suitable for the emerging LEO satellite assisted IoT ecosystem. In this paper, we first introduce the architecture of the LEO satellite network assisted IoT ecosystem. Then, we propose an efficient and privacy-preserving blockchain-based authentication scheme. The proposed authentication scheme takes the advantages of certificateless encryption and consortium blockchain to provide lightweight key pair computation without appealing devices' information and efficient signature querying and verification. In addition, a fast authentication mechanism is implemented in the scheme in order to reduce the time complexity from querying a certain record for the authentication within a satellite among multiple beams. With the analysis of the storage and computation complexity, the performance evaluation demonstrates the effectiveness of the proposed scheme.**

***Index Terms*—Blockchain, Authentication Scheme, LEO Satellite Network, Internet of Thing**

I. Introduction

ALTHOUGH the Internet of Things (IoT) seems more than promising to embrace the industrial sectors, such as oil and gas industry, environmental monitoring and food and agriculture systems, it can be easily recognized that fundamental performance limitations related to availability, resilience and cost of terrestrial connectivity, where satellite network plays a complementary role in supporting the development of the IoT applications and in realizing the full potential of the interconnected devices [1, 2]. For some IoT applications, the smart devices can be dispersed over a wide geographical area (e.g. ocean, valley and forest), where the direct terrestrial networks are not available due to the high cost for the deployment and maintenance of the infrastructures, resulting in the lack of the Internet access. In addition, the terrestrial networks rely on the physical infrastructures deployed on the ground to provide wired or wireless connectivity, which are fragile and are easily damaged by nature disasters leading to the severe Internet disruptions. The Gartner, Inc. no single networking technology could satisfy a set of the competing requirements, such as endpoint cost, power consumption, bandwidth, latency, connection density, operating cost, quality of service, and range, where the forthcoming generation of LEO satellite networks will play an irreplaceable role [3]. The Low-Earth-Orbit (LEO) satellite constellation network has been recognized the potential to provide the reliable and dependable connection and has been effectively used as primary fallback for major links to assure resilience to infrastructure failure, which make the LEO satellite network ideal for fulfilling the needs of a meaningful percentage of the IoT applications.

LEO satellite constellation network represents a group of satellites which are arranged in several orbits (normally the altitude is lower than 2000 km according the definition from NASA), moving around the Earth's surface periodically (e.g. Iridium satellites constellation is shown in Fig.1 [4]) in order to provide ubiquitous and seamless Internet access. Due to its desired functionalities, much attention has been paid to integrate LEO satellite constellation networks into IoT applications in both scientific research and industrial practice. Qu et al. [2] summarizes the advantages of employing LEO satellite constellation network in IoT and provided an overview of LEO satellite constellation-based IoT system including constellation design, interference mitigation, constellation network architecture, routing scheme, and united higher layer design. Several emerging IoT applications, which includes mission critical applications, location based services, agriculture, tracking and healthcare, are well discussed in [5] by taking the advantages of the conglomeration of the IoT and the LEO satellite constellation networks. Different satellite operators, such as Vodafone and Inmarsat [6] provide backhaul for IoT devices in smart farms in far corner of the globe, in which Milk Smarts are already planning to leverage satellite backhaul of Low-Power-Wide-Area to new solutions for precision farming in Australian agribusiness.

Despite the great benefit brought by the conglomeration of

B. Wang, Z. Chang and T. Hämäläinen are with Faculty of Information Technology, University of Jyväskylä, P. O. Box 35, FI-40014 Jyväskylä, Finland. Z. Chang is also with School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu 611731, China. Shancang Li is with Department of Computer Science and Creative Technologies, University of the West of England, Bristol BS16 1QY U.K.
This work is partly supported by NSFC (No. 62071105).
E-mail: biyingwang.bing@gmail.com, zheng.chang, timo.hamalainen@jyu.fi, shancang.li@ieee.org

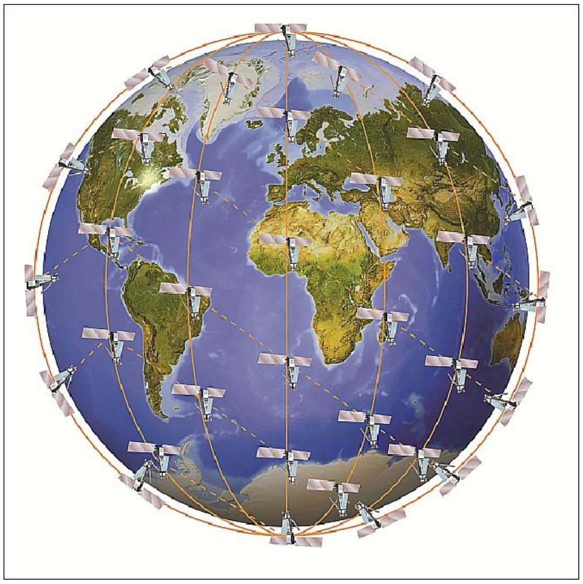


Fig. 1. Iridium NEXT constellation of 66 spacecrafts (image credit: Iridium Satellite)

the LEO satellite constellation network and IoT applications, the communication between the ground and the satellites is vulnerable to non-authorized or malicious attacks due to its openness[7]. To achieve the secure communication in LEO satellite constellation assisted IoT ecosystem, several features inherited from the LEO satellite constellation network have to be taken into consideration, *The dynamic topology* requires the mechanism of the secure communication to be efficient so that the users in the covered area can be served during in passing by period; *Frequent link switching* happens between beam-to-beam and between satellite-to-satellite, the verification process should be lightweight that can be easily performed on the satellite, and possible verification optimization should be considered as well; *The transmission delay* for the uplink/downlink is shorter compared to the other satellite communication system like Geosynchronous Equatorial Orbit (GEO) system, however, it is still unavoidable consumption of time which limit the communication efficiency; *Limited computing capability and storage space* burdens the challenges in designing the secure communication algorithms where those heavy cryptography algorithms are no longer applicable. These intrinsic characteristics make the LEO satellite constellation network more vulnerable to counterfeiting, tampering and other security threats than traditional terrestrial networks. A simplest solution is to develop a lightweight and efficient authentication scheme for such LEO satellite constellation network assisted IoT ecosystem, which is the first and most fundamental step to ensure the network security.

However, most existing lightweight authentication approaches [8][9][10][11][12] are developed for terrestrial IoT applications which are not appropriate for the LEO satellite constellation assisted IoT applications due to its unique characteristics as the aforementioned. Traditional centralized or decentralized authentication scheme is built under the assumption of the third trustworthy parties, which usually requires the true identity information to issue a certificate, thus compromising the user's privacy. Additionally, the third trustworthy parties are usually deployed at the core network, which may increase the latency since it is far away from the smart devices at the edge of the network. Routing and re-routing is also time-consuming, thus, lower the quality of services. Recently, blockchain technology has received considerable attention for its great potential in addressing the security issues in IoT applications [13, 14]. By leveraging its distributed nature and consensus mechanism, the blockchain technology provides a way to carry out transaction during the dynamic and wide coverage circumstances with other entities without the dependency on the third trust authority. Many blockchain-based authentication approaches have been developed regarding to various IoT applications, such as smart city [15], VANETs[16], 5G networks [17] and etc.. Moreover, the public key infrastructure (PKI) are employed to authenticate a legal entity that introduces a long authentication time together with heavy overhead of certificate storage and management, which could not meet the requirements of the LEO satellite assisted IoT applications. Lightweight authentication scheme such as identity-based encryption or certificateless encryption could be a potential solution.

A. Related works

Since the study of the authentication scheme in the LEO satellite constellation networks assisted IoT ecosystem is a new concern, few research has been developed in this area. As the fundamental of this emerging ecosystem, the traditional satellite networks have been widely studied. Generally, the authentication scheme for the satellite network relies on the technology of the public key cryptosystem, symmetric cryptosystem, hash function, Identity-based certification and blockchain technology.

Regarding the centralized authentication approaches, Cruickshank first presents an authentication protocol [18] for the satellite network by using public key cryptosystem, achieving the mutual authentication between the users and the network control center (NCC). However, the high computation overhead and the complexity of managing the public keys make the system inefficient. In 2005, Chang also introduces a mutual authentication protocols that simply makes use of hash and XOR function [19] in order to provide simple and efficient authentication at low computation cost. Nevertheless, NCC is involved in every authentication procedure, which restricted the performance as a bottleneck and may lead to single point of failure. Moreover, Chang's scheme does not take the user's privacy into consideration so that may suffer from the impersonation attacks. A hybrid authentication scheme which combines the symmetric cryptosystem and the public key cryptosystem is proposed by Chen *et al.* [20] in 2009. This authentication scheme removes the complexity of the PKI and avoids the complex computation from the user's side. Besides, they claims that no sensitive information is stored in the verification table. In 2012, C.C.Chang *et al.* improves Chen's scheme to resists common malicious attacks, in which the security scheme is based on the discrete logarithm problem and one-way hash function [21]. In 2016, Liu.Y *et al.* proposes a lightweight authentication scheme for the satellite network that involves only hash functions, XOR, and string concatenation operations. In 2020, Hu *et al.* [22] introduces a direct percolation routing algorithm based on the satellite grid structure, which achieves low delay and high reliability. Kong *et al.*[23] implements an efficient and secure user access and inter-satellite handover mechanism in an LEO constellation-assisted beyond 5G system, where the control-plane and the user-plane session keys can be successfully established with high efficiency. Liu *et al.*[24] proposes an access authentication protocol with user anonymity and traceability to reduce the communication delay and signaling cost of access authentication. A hierarchical group key distribution scheme is also implemented to avoid the re-authentication.

Inspired by the blockchain technology, many blockchain-based authentication schemes have been introduced into various IoT applications. H. Yang *et al.* [25] introduces an architecture of blockchain on the basis of trust authentication for 5G network and a blockchain-based anonymous access scheme implemented in cloud radio over fibre network. Lee and Kim [26] achieves authentication and data protection in a smart meter system by using blockchain technology and zero-proof technology, which can prevent the data tampering and avoid reveling the user's original data to the third parties. Zhu et al.[27] presents a blockchain-based identity framework for IoT and illustrates how to implement it in smart homes, which enhances the autonomous extraction of the signature and enables the creation of the blockchain-based identity for their owners. Although the blockchain seems a promising solution to achieve the authentication, with respect to the decentralized authentication protocol in satellite networks, related researches are quite insufficient. Wei *et al.* [28] proposes a new distributed authentication protocol with IBE for the key management and with encryption-decryption and blockchain for rapid handover authentication. This scheme provides the logging function with the consideration of the dynamic topology and frequent link switching of LEO satellite network. Zhao.C, Shi.M and Huang.[29] implements a hashchain-based identity authentication and privacy protection scheme in the satellite-terrestrial integrated network, which can support effective data security for the intelligent transportation systems. A token-based access control framework with effective intrusion detection for blockchain-based satellite communication system is proposed by Cao [30], which effectively prevents malicious attacks. Li *et al.* [31] presents an architecture composed of satellite and ground equipment, which improves communication security through all the stages including the communication, registration, authentication, and revocation of information. Deng *et al.* [32] proposes a Blockchain-based Authentication Protocol Using Cryptocurrency Technology (BAPC) including three stages of access authentication, which achieves fast switching authentication and improve the efficiency of generating blocks.

Unfortunately, most of the aforementioned authentication mechanisms are under the assumption that satellites act as the relays between the users and the ground facilities in order to provide the data forwarding services. Therefore, the authentication scheme is implemented between them, which usually causes long access delay. Additionally, most of the current access authentication schemes are commonly using the centralized approaches, in which each procedure of the authentication requires the NCC's participation, leading to the congestion and single point of failure. Moreover, users' privacy is another serious concern for the authentication whereas most above works do not take into consideration (e.g. [18], [19], [20]). Although some authentication schemes utilizes the group signature to protect the user's privacy [33] [34], [35], the group signature requires considerable computation complexity. Furthermore, these techniques demand the update of the signing key when revocation occurs, resulting in unnecessary delay. Thus, these schemes are time-consuming and unsuitable for the LEO satellite networks assisted IoT ecosystem.

B. Contributions

Taking the above challenges into consideration, we develop a blockchain-based authentication scheme (BC-Authen) for the LEO satellite assisted IoT ecosystem by aggregating the lightweight certificateless encryption into the blockchain technology. The main contributions of our work can be summarized as the follows:

- We introduce an emerging architecture for the LEO satellite network assisted IoT ecosystem, in which the LEO satellite network plays a supplementary role in order to provide the seamless and reliable Internet access where are lack of the terrestrial networks. The LEO satellite network as the Internet access provider can cooperate with various consortium as long as they require satellite Internet services.
- The consortium blockchain technology is adopted to record the registration activity and achieve the certificate transparency. All the selected entities in the LEO satellite network assisted IoT ecosystem can monitor the authorities by verifying the signature in each transaction and checking the corresponding updates in the nearby blockchain node.
- Considering the realistic scenario, the consumer who would like to use the Internet services via LEO satellite network may have a branch of smart devices that need to get the access. The novel data structure named the Merkle Patricia Tree (MPT) extended from the conventional blockchain is adopted for the purpose of eliminating the storage and computation intensive certificate revocation list. This distributed certificate management reduces the signal cost and the latency since the satellites do not need to communicate with the ground control center that often.
- We take advantages of the certificateless encryption to compute the key pairs for smart devices, which not only reduce the computation time but also preserve the privacy of the smart devices. The link-ability between the user's real identity and the pseudo identical information is stored in the local semi-control center so that prevent the privacy leakage to the LEO satellite network provider.
- Comparing the authentication scheme with [28], [31] and [32], our scheme requires less storage space on satellites,

as well as shows the better efficiency and the better privacy protection in authentication phase .

C. Organization

The remainder of this paper is organized as follows: Section 2 describes the technologies utilized in the proposed BC-Authen scheme and introduces an overview of the system architecture including each component and their functionalities. Section 3 presents the processes of BC-Authen scheme for the LEO satellite network assisted IoT ecosystem. Some security analysis are discussed in Section 4, while the performance results shows in Section 5. The conclusion and future work is summarized in Section 6.

II. Preliminaries

In this section, we first describes the technologies employed in the proposed BC-Authen scheme for LEO satellite constellation network assisted IoT ecosystem. After that, an overview of the system architecture for LEO satellite constellation network assisted IoT ecosystem is introduced, following with the functionalities of each component. Finally, a list of symbols used throughout this paper is summarized in TABLE. I.

A. Blockchain Technology

The blockchain (BC), first introduced as the underlying technology of the cryptocurrency Bitcoin [36], is an immutable and distributed ledger that can record the transactions between any untrustworthy parties in a verifiable and permanent way. Some researchers have directly extracted the core technical principle of Bitcoin system, which is blockchain, to build platforms such as Hyperledger[37] and Ethereum [38] for further application developments. For those blockchain-based platforms, there is neither a centralized control nor a centralized storage for maintaining its data, resisting to the denial of service attack and avoiding the privacy disclosure. All participants can be identified by their public keys. Once the transactions are encrypted and verified by the entire network, it will be duplicated maintained at each participants, avoiding the single point of failure. With these attractive features including the universal accessibility, incorruptibility, and the ability to store and transfer the data in a secure manner, blockchain technology has been widely adopted into different areas other than the cryptocurrency [39], one of which is authentication.

1) Blockchain Technology Selection: Generally, the blockchain technology has been categorized into three types: public (permission-less) blockchain, private (permissioned) blockchain and consortium (hybrid) blockchain [40], which mainly differs in the mining and the transaction issuance and validation, as well as the access restriction. In the public blockchain, no one is in charge, and every user with the Internet connection can create a personal address and join the blockchain network by submitting the transactions and adding entries to the ledger. For private blockchain, it belongs to the private property of an individual or an organization as its name suggests. In other words, the in charge looks after of those important things such as mining, granting the access, creating and validating the transactions. The consortium blockchain has more than one in charge compared to the private blockchain, which allows a group of companies or representative individuals making decision together for the best benefit of the whole network. In this type of blockchain, the selected representative nodes are responsible for mining and conducting transaction related computation.

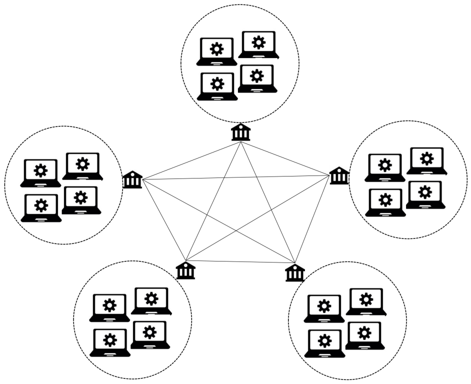


Fig. 2. Consortium Blockchain network structure

The BC-Authen scheme proposed in this paper selects the consortium blockchain technology as shown in Fig. 2 for several reasons. First, the LEO satellite network is only accessible for those parties which has been granted the authority to use the LEO satellite network services. Second, considering the privacy protection, the corporate parties may not be willing to grant the full rights to the LEO satellite network providers, where the consortium blockchain can be utilized to select representatives from different parties and supervised the transactions together. Third, compared to the centralized private blockchain and the public blockchain, the consortium blockchain could provide the distributed supervision with less computation.

2) Merkle Patricia Tree: The Merkle Patricia Tree(MPT) is first proposed in Ethereum [38] that provides a cryptographically authenticated data structure for the Ethereum. Inspired by the Trie, the MPT advances the Merkle tree, in which two features have been added to the common Merkle tree in order to improve the efficiency for data update and lookup. What is more, it forms a persistent data structure, which can provide the proof of membership. The Ethereum introduces three types of nodes in the MPT named as *Leaf node*, *Extension node* and *Branch node* that can be expressed as a key-value pair. The value is the content of an MPT node, while the key is the hash of this node. Importantly, the nibble is the unit to comprise the path to each node in MPT.

- *Leaf node* is a node without a child. In BC-Authen scheme, a leaf node represents a certificate transaction that contains enough information for verifying a legal entity. The $nibbles$ in the leaf node is for accessing the leaf node by the accumulation of keys and branches traversed from the root.
- *Extension node* has a series of nibbles of size greater than one that are shared by at least two distinct keys past the accumulation of nibbles keys and branches as traversed

from the root.

- *Branch node* have up to 16 branches from 0 to f that correspond to each of the sixteen possible nibble values for the keys at this point in their traversal.

The MPT is used to achieve a decentralized Certificate Library that are maintained at those selected representative nodes. The branches can be used to manage different corporate parties efficiently and explicitly.

B. Defination of Verifiable Identity Based Encryption

The certificateless cryptography [41] is developed based on the identity based encryption in order to solve the key escrow problem. It consists of six-tuple of probabilistic polynomial-time algorithms, namely Setup, Extract-Partial-Private-Key, Generate-User-Keys, Set-Private-Key, CLS-Sign and CLS-Verify, which are explained briefly as below.

- **Setup(1^{λ})**: A global set-up algorithm is executed by Key Generation Center (KGC) that takes security parameter 1^{λ} as input and returns KGC's master secret key *MSk* and global system parameters *params*. Only KGC knows the value of *MSk*.
- **Extract-Partial-Secret-Key(*ID$_i$*, *MSk*, *params*)**: After verifying the identity $ID_i \in \{0,1\}^*$ of user i , KGC calculates a partial secret key PSk_i with (*MSk*, *params*, *ID$_i$*) as inputs for user i. The user i can verify PSk_i anytime when it is required.
- **Generate-User-Keys(*ID$_i$*, *params*)**: An algorithm takes the identity ID_i and the global parameters **params** and outputs a public key Pk_i and a Secret-Value x_i. This is run by the user i, who can use the Secret-Value x_i to construct the full private key.
- **Set-Private-Key(*PSk$_i$*, *x$_i$*, *params*)**: The user i runs a deterministic algorithm that takes those parameters to get its full private key Sk_i.
- **CLS-Sign(*m*, *Sk$_i$*, *params*)**: A signature σ is generated with the secret key *Sk$_i$*, message *m* and global parameters *params*, and then transmitted to the receivers.
- **CLS-Verify(*ID$_i$*, *Pk$_i$*, σ_i, *params*, *m*)**: Receivers verify the signature σ_i with given parameters and output VALID if the signature is original, otherwise outputs INVALID.

C. Unified System Architecture for LEO Satellite assisted IoT

Fig. 3 illustrates the architecture of BC-Authen for LEO satellite network assisted IoT ecosystem with partial data stream showing how the system work, in which the LEO satellite network provides the Internet access for the smart devices, the corporate consortium is the potential client who need the satellite network to facilitate the data forwarding, and the data center refers to cloud platform which could provide storage services.

1) LEO Satellite Network: The LEO satellite network, typically consisting of several groups of satellites, several ground gateways (GGW) and the network control center (NCC), acts as an Internet service provider, which aims at providing the seamless and reliable Internet access for the legal smart devices. The NCC deployed at the ground is the core control center for all satellites, which is responsible for initializing the generic block by calculating the system parameters and key pairs for each satellite. On each orbit, one satellite is selected as the satellite gateway (SGW), which stores and maintains the blockchain, as well as verifies the user's identity. The other satellites on the same orbit follows the result of verification from the satellite gateway to process the forwarding data and cache a copy of the certificate in order to faster the verification scenario when the user change to other beams within the satellite. The ground gateways are distributed at different locations so that ensure the feeder link could be received globally and easily.

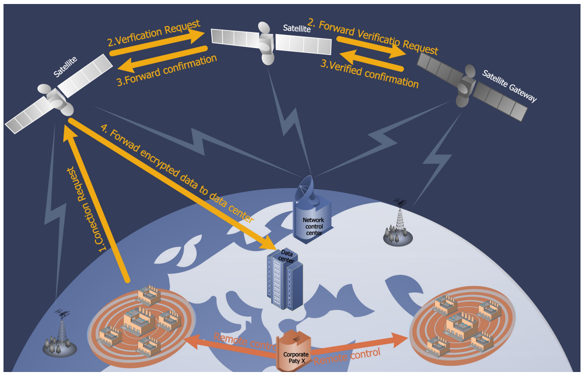


Fig. 3. An overview of the BC-Authen system model

2) Corporate Parties: As showing in Fig. 3, the corporate parties are those industrial sectors, who need the LEO satellite network services to assist the data forwarding. For these industrial companies, the sensors and the actuators are usually distributed at wide geographically places with a Semi-Control Center(SCC) assisting all the events. The involved companies will be responsible for reaching the agreement of the services with LEO satellite network provider, as well as for calculating all the key-pairs for each entity owned by the company. The headquarter of the corporate party and the SCC of the companies act as the miner of the BC-Authen scheme, which not only keeps a copy of the transactions but also issue and verify the transactions. Once the smart devices request a connection to a satellite, it can directly send the encrypted data together with its signature to the satellite.

3) Data Center in the Cloud: The cloud center can be a part of the whole system, which is employed by the corporate parties to store the forwarded data from the smart devices. The cloud center calculates its key-pairs and register the related signature information on the blockchain. At the same time, the cloud center also maintains a copy of the blockchain in order to verify whether the forwarded data is coming from the legal users. Thus, the integrity and the confidentiality of the sensing data is protected.

The authentication procedures in the the proposed BC-Authen scheme are: 1) The smart devices (such as sensors) first check whether they have registered for the LEO satellite network service. 2) If yes, the smart devices collect the data, encrypted it and send it to the satellite that serves covered region at this moment together with its signature. 3) If no, the smart devices can send a registration request to the SCC, who

TABLE I
NOTATIONS AND DEFINITIONS

Symbols	Meaning
params	The security parameters of the system
MSk	The public master key of the NCC
ID_i^X	The identity of smart device i owned by party X
x_i^X	A secret value of the smart device i
Pk_i^X	The public key of the smart device i
Sk_i^X	The private key of the smart device i
σ_i	The signature of device the smart device i
SGW^m	The identity of the satellite gateway of group m
S_n^m	The identity of satellite n in the group of m
$Enc(m, k)$	Encryption algorithm that encrypt m with key k
$Dec(m, k)$	Decryption algorithm that decrypt m with key k

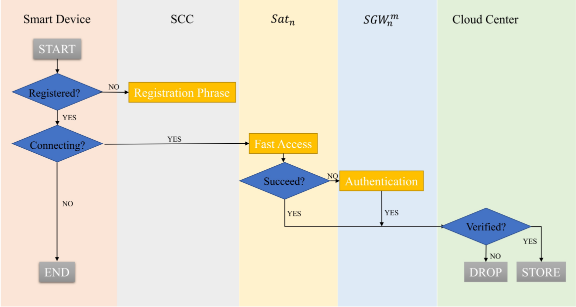


Fig. 4. The complete authentication procedures

can conduct the registration for those smart devices in charge. 4) Upon receiving the message from the sensors, the satellite first search its cache for a fast authentication. 5) Otherwise, the satellite sends the verification request to its SGW and follows the command from the SGW. 6) The satellite will forward the data to the cloud center if the sensor is authenticated together with its signature; otherwise, drop the message. 7) When the encrypted data arrives at the cloud center, it queries on its local blockchain and verifies the signature of the satellite. The data will be stored once it keeps the authenticity.

At the end, a list of notations and definitions in the proposed model are given in TABLE. I.

III. BLOCKCHAIN-BASED AUTHENTICATION SCHEME FOR LEO SATELLITE NETWORK ASSISTED IOT ECOSYSTEM

In this section, we propose an efficient and privacy-preserving authentication scheme based on the extended blockchain for the LEO satellite network assisted IoT ecosystem. Following the four phrases *System Initialization Phase*, *Registration Phrase*, *Access Authentication Phrase* and *Fast-access Authentication Phrase*, the BC-Authen scheme could be realized.

A. Procedures for Authentication Scheme

Fig. 4 illustrates the complete procedures of the proposed BC-Authen scheme for LEO satellite network assisted IoT ecosystem. The BC-Authen scheme is triggered when the smart device requests the connection to the LEO satellite network. It first checks whether the smart device has registered in the platform or not. If yes, the smart device could use its public key to encrypt the data and send it to the satellite with its signature. Upon receiving the signature and the encrypted data, the satellite first run the fast access authentication algorithm to validate whether the data is sent by the genius smart device. The authentication phase will be carried out by the satellite gateway when the fast authentication phase failed. Once the authenticity is valid, the satellite will provide data forwarding services. In this BC-Authen scheme, the smart devices can be verified by its own public key registered in the blockchain, where the certificate is no long needed.

1) System Initialization Phrase: NCC as the control center of the LEO satellite network is responsible for initializing the BC-Authen scheme. NCC takes security parameter λ as input and calculates the master secret key MSk and the global system parameters $params$. Before deploying the satellites, the NCC takes global system parameters $params$ to compute the key pairs for each satellite and each GGW. This step does not need to use the certificateless calculation since the NCC and the satellites are owned to the same company. While for those corporate parties, the certificateless algorithm can be conducted to create key pairs for all involved entities as introduced in Section 2. After that, NCC initialize the first block by registering all the involved entities. The certificate transaction of an entity contains the public key, entities' authority, certificate start time, certificate end time and a signature from its owner, note that $TA(ID||Pk||Authority||StartTime||EndTime||Owner_{sign})$. Note that all entities are genius with this process.

2) Registration Phrase: In the registration phrase, NCC plays as an semi-trust authority, which is responsible for calculating the public key, partial secret key and a certificate for the legal smart devices using certificateless encryption algorithm. If the owner of the smart devices has already reached the agreement with the LEO satellite network service provider, the smart device will be registered into the blockchain. During the certificate's valid period, the smart device is allowed to access the LEO satellite network at any time. Otherwise, a new coming smart device need to register first.

The SCC who is in charge of the new coming smart device need to submit the partial unique identity related information with its signature to NCC in order to obtain the public key and private key together with a certificate signed by NCC. Suppose that the corporate party X deploy a new smart device ID_A^X, which need to access the LEO satellite network. The calculation procedures are as follows:

1) The SCC provides the unique identical information (such as a series code) ID_A^X to NCC, which can be differentiated from the other smart devices belong to the same corporate party. In this way, the linkability between the real smart device and its identity information is protected.
2) The NCC calculates the partial secret key PSk_A^X for smart device ID_A^X .
3) The NCC encrypts the partial secret key PSk_A^X and transmits it to the SCC together with its signature.
4) Upon receiving the message from the NCC, the SCC first validate if the message is from the NCC by comparing

the signature stored in local blockchain.

5) Once verified, the SCC randomly select a secret value x_A^X and computes the public key Pk_A^X and full private key Sk_A^X.
6) The SCC updates a certificate record of

$$\begin{aligned} & ID_A^X || StartTime || StopTime || PK_A^X || \sigma_A^X \\ & Sign_{SCC}\{ID_A || StartTime || StopTime\} \end{aligned} \tag{1}$$

in its local blockchain and broadcast it to the other nodes with its signature.

7) Other selected miner nodes in the proposed BC-Authen scheme appends the new transaction into their blockchain after verifying the authenticity of the transaction and the previous root hash of the sender's branch.

```
Algorithm 1 Key Generation for Smart Device
Input: $ID_A^X$
Output: $Pk_A^X, Sk_A^X$
SCC sends registration request $ID_A^X || \sigma_{SCC}$
if $\sigma_{SCC}$ = valid then
    $PSk_A^X \leftarrow (ID_A^X, MSk, params)$
    NCC sends the $PSk_A^X || \sigma_{NCC}$ to SCC
    if $\sigma_{NCC}$ is valid then
        $(Pk_A^X, Sk_A^X) \leftarrow (PSk_A^X, x_A^X, params)$
    end if
end if
```

Algorithm 1 illustrates the key generation operators for a smart device in the *Registration Phrase*. After that, the SCC will register the smart device in the blockchain, while each selected representative follows the Algorithm 2 to verify the transaction, the flag F_{T_j} will be set to 1 once successfully verified. Once completing the verification, the selected representatives append the transaction by running the Algorithm 3, in which the $value$ is the certificate obtained from the algorithm 1 and the key is the hash value of the $value$. Since the the sender's identity has been verified in the algorithm 2, Algorithm 3 will only focus on how to register the verified transaction in the blockchain.

```
Algorithm 2 Verify the Transaction
Input: $T_j, \sigma$
Output: $true, false$
    Procedure VerTrans $(T_j, \sigma)$
$F_{T_j} \leftarrow 0$
$(ID, Pk) \leftarrow QueryAuthority(\sigma)$
$V_{T_j} \leftarrow Ver(T_j, \sigma, ID, Pk)$
if $V_{T_j}$ = valid then
    $F_{T_j} \leftarrow 1$
else
    $Abort$
end if
```

At this point, the smart device ID_A^X has completed all the procedures of registration and is allowed to access the LEO satellite network services.

```
Algorithm 3 Register the Node in MPT
Input: The current MPT $T, key, value$
Output: The update MPT $T'$
SCC broadcasts the $ID_{scc} || Sign(T, key, value, T')$
Procedure InsertNode($key, value$)
$Pk_{scc} \leftarrow QueryBC(ID_{scc})$
$(T, key, value, T') \leftarrow Dec(Sign(T, key, value, T'), Pk_{scc})$
if $T$ holds then
    Calculate $T'$ with $(key, value)$
    if $T'$ holds then
        Append the $(key, value)$ and update $T'$
    else
        $Abort$
    end if
else
    $Abort$
end if
```

3) Access Authentication phrase: The access authentication phrase describes the scenario when a smart device wants to get access to a satellite, which is shown in Fig. 5 The following processes give an overview of how this phrase is realized:

1) When the smart device ID_A^X wants to connect to LEO satellite network, it directly encrypts the data using public key Pk_A^X, sign it with its private key Sk_A^X, and send message (1) to the served satellite S_n^m.

$$m1 = ID_A^X || Enc(Enc(data, Pk_A^X) || \sigma_A^X, Sk_A^X) \tag{2}$$

2) When the satellite S_n^m confirms that there is no fast access authentication information available (see the details in the fast access phrase). The satellite S_n^m sends the smart device identity and signature (ID_A^X, σ_A^X) to the satellite gateway SGW^m who is in charge of the group m of the satellites and maintaining the local blockchain.
3) After receiving the request from the satellite S_n^m, the satellite gateway SGW^m retrieves the block and find the corresponding public key of the smart device. If found, then the satellite gateway SGW^m uses its public key Pk_A^X decrypts the message (2) and compares the σ_A^X. If the signature is the same, the satellite gateway replies *VALID_USER*, otherwise, the satellite gateway replies *INVALID_USER*.
4) The satellite S_n^m follows the commands returned by the satellite gateway SGW^m, and serves the smart device ID_A^X if get *VALID_USER*. Then, the satellite S_n^m forwards the message (3) to data center with its own signature. Otherwise, the satellite S_n^m rejects the request from the smart device ID_A^X if get *INVALID_USER*.

$$m2 = ID_n^m || Enc(Enc(data, Pk_A^X) || \sigma_n^m, Sk_n^m) \tag{3}$$

5) The data center queries its local blockchain, and authenticate the satellite S_n^m with its public key, saves the encrypted data if the signature is valid, otherwise, drops the encrypted data.

By completing all the steps mentioned above without any mistakes, the satellite S_n^m will allocate the resources based on

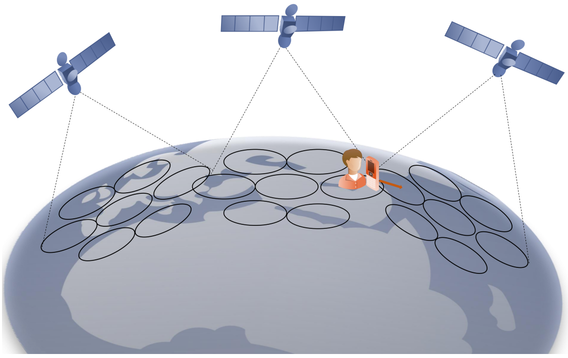


Fig. 5. Authentication handover when changing satellites

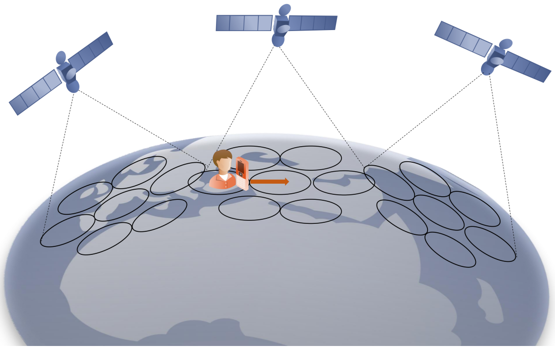


Fig. 6. Authentication handover when changing beams

the service type to establish a secure connection with the smart device ID_A^X. When receiving the message from the satellite S_n^m, smart device ID_A^X verifies with its Sk_A^X. Once succeed, a secure channel between the satellite S_n^m and smart device ID_A is maintained. The smart device doesn't need to obtain the public key of the satellite in advance, since the message comes from the satellite is encrypted with the public key of the smart device that is known by the legal parties. Thus, the mutual authentication between the satellite and the smart device is accomplished with the proposed BC-Authen scheme.

The access authentication algorithm conducted by the satellites is as follows:

Algorithm 4 Access Authentication Algorithm

```
Input: $ID_{A^X}||Enc(Enc(data, Pk_{A^X})||\sigma_{A^X}, Sk_{A^X})$
Output: $true, false$
    Satellite $ID_{n^m}$
$(Pk_{A^X}, \sigma'_{A^X}) \leftarrow QueryBC(ID_{A^X})$
$\sigma_{A^X} \leftarrow Dec(Enc(Enc(data, Pk_{A^X})||\sigma_{A^X}, Sk_{A^X}), Pk_{A^X})$
if $\sigma_{A^X} = \sigma'_{A^X}$ then
    Sends $ID_{n^m}||Enc(Enc(data, Pk_{A^X})||\sigma_{n^m}, Sk_{n^m})$ to data center
end if
    Data center
$(Pk_{n^m}, \sigma'_{n^m}) \leftarrow QueryBC(ID_{n^m})$
$\sigma_{n^m} \leftarrow Dec(Enc(Enc(data, Pk_{n^m})||\sigma_{n^m}, Sk_{n^m}), Pk_{n^m})$
if $\sigma_{n^m} = \sigma'_{n^m}$ then
    Stores encrypted data $Enc(data, Pk_{A^X})$
end if
```

4) *Fast-Access Authentication phrase:* Considering the handover between beams within the same satellite as shown in Fig. 6, a fast access authentication mechanism is provided to reduce the time of querying the public key and transmitting the validation result from satellite gateway to the access satellites. When the smart device once get authenticated by a satellite, the access satellite will cache the related information about the smart device. Taking the dynamic topology of the LEO satellite constellation network and the limited storage and computation resources into the consideration, the cache information will be set valid for a given short time $ValidTime$. Suppose $ValidTime$ represents the period that the satellite could serve a given point on the earth. The access satellite cache information about smart device ID_A^X, which note as $(ID_A^X,\ Pk_A^X,\ \sigma_A^X,\ ValidTime)$. Once the $ValidTime$ has been passed, the satellite will remove the record from its cache.

Upon receiving the message (1) from the same smart device ID_A^X, the satellite ID_n^m can validate the identity of the smart device in a similar way as it is in the access authentication phase. The detailed procedures of the fast access authentication can be realized by Algorithm 5. In this way, the satellite does not need to send the verification request to the satellite gateway, thus reducing the searching time in the blockchain $O(n)$. Note that the fast access authentication is only used on the condition of 1) the smart device gets authenticated by the satellite successfully and 2) the smart device is still under the coverage of the same satellite but served by an another beam. While another satellite takes charge the area where the smart devices located, the fast access is not applicable for that there is no related verification information cached in the satellite, instead, the access authentication phase will be performed.

Algorithm 5 Fast Access Authentication Algorithm

```
Input: $ID_{A^X}||Enc(Enc(data, Pk_{A^X})||\sigma_{A^X}, Sk_{A^X})$
Output: $true, false$
$\sigma'_{A^X} \leftarrow QueryCache(ID_{A^X})$
if find then
    $\sigma_{A^X} \leftarrow Dec(Enc(Enc(data, Pk_{A^X})||\sigma_{A^X}, Sk_{A^X}), Pk_{A^X})$
    if $\sigma_{A^X} = \sigma'_{A^X}$ then
        Respond to the request
    else
        Reject the request
    end if
else
    Conduct the access authentication phrase
end if
```

IV. Security Analysis

In this section, we address the security analysis of the proposed BC-Authen Scheme with the respect to authentication security and the conditional privacy.

A. Security

The BC-Authen scheme is a secure authentication scheme since it is developed under the certificateless cryptography. In such scheme, the adversary has a negligible advantage that the probability to distinguish two distinct plaintexts from a ciphertext is $1/2 + \varepsilon(k)$, where the ε is a negligible function with the security parameter k [41]. In other words, the adversary is not to guess the secret key of a smart device from the large amount of the ciphertext in the LEO satellite network assisted IoT ecosystem. Therefore, an adversary has no chance to forge a digital signature σ for any transactions published in the system. Additionally, we employed the consortium blockchain in BC-Authen scheme, which only grant the authority to those corporate parties. Only selected representatives have the authority to create and validate the transactions.

For some malicious attacks, the BC-Authen is resisted. The detailed analysis can be found as follows:

- **Data Tampering:** Since the sensed data is encrypted with the public key before transmitting to the satellite, even the access satellite has no knowledge of what are the content of the sensed data. If the adversary wants to tamper the encrypted data, he needs to get the secret key first which is impossible.
- **Eavesdropping:** The adversary can eavesdrop the communication between the smart device and the satellite and obtain the ciphertexts. However, he can't get the plaintexts unless he gets the secret keys from involved entities, which is quite hard.
- **Man-in-the-middle:** It is impossible for the man in the middle to register with the role that is already existed in the system. Besides, the secret keys of any entities in this ecosystem is hard to obtain. Thus, the adversary couldn't disguise himself as any role of the system to conduct man-in-the-middle attack.

By taking the advantage of the blockchain, our BC-Authen scheme are unforgeable and immutable as long as more than half of selected representatives in the network have not been compromised. The proof of authentication is provided by the selected representatives to guarantee that each transaction is coming from the legal entities.

B. Privacy

Considering each party of the LEO satellite network assisted IoT ecosystem, the proposed BC-Authen scheme preserve the privacy of the smart device' identity and the sensed data. In the registration phrase, it is the SCC who registers the smart devices to the blockchain. The SCC acts as the intermediate that maintains the linkability of the real identical information of the smart device and the pseudonymous identity which is unique among the same party. The NCC can generate the partial secret key for the smart device without knowing its true identity, thus, protecting the privacy of the smart devices. Besides, the LEO satellite network provider can gain no knowledge of the sensing data, because the sensing data is encrypted with public key of the smart device in the BC-Authen scheme which is hard to decrypt without the smart device's secret key. However, as discussed in the security, it is not possible to get the smart device's secret key. Therefore, the genius identity information and sensitive data is protected under the BC-Authen scheme.

TABLE II
SECURITY PROPERTIES.

	IBE-Auth	SatSec	BAPC	Our Scheme
Type of Cryptography	IBE	Public	Public	IBE-variant
Key Agreement	✓	✓	✓	✓
Mutual Authentication	×	✓	×	✓
User Anonymity	Partially	Partially	Partially	✓

TABLE III
PERFORMANCE COMPARISON

	SAT storage	Query Time	Transmission
IBE-Auth	n*m*blocks	$O(2log(size_b))$	$4T_u$
SatSec	0	$O(log(size_b))$	$2T_u$+$2T_g$
BAPC	n*m*blocks	$O(log(size_c))$	$2T_u$
Our scheme	m*blocks	$O(log(size_c))$	$2T_u$+$2T_s$

n: The number of the satellites on the same orbit.
m: The number of orbits in a LEO satellite constellation.
$\mathbf{Size_b}$: The size of the blockchain ledger.
$\mathbf{Size_c}$: The cache size on satellite.
$\mathbf{T_u}$: The transmission time between the user and the satellite.
$\mathbf{T_s}$: The transmission time between the satellites in the same orbit.
$\mathbf{T_g}$: The transmission time between the ground station and the satellite.

V. PERFORMANCE ANALYSIS

In this section, we analyze the performance of our scheme with three other authentication schemes, IBE-Auth [28], SatSec [31] and BAPC [32] from the perspective of security features, the storage consumption on LEO Satellite Constellation, query time consumption and transmission time consumption.

A. Security Features

The comparison of the security features is concluded in TABLE. II. For the type of cryptography system, BAPC and SatSec adopt public key cryptography system, IBE-Auth adopts the Identity-based system, and our scheme uses a variant of Identity-based system. As for mutual authentication, both our scheme and SatSec provide mutual authentication while the other related work does not have the authentication at user device side, which is a security risk. In terms of user anonymity, the identity of a userâĂŹs device cannot be extracted without secret credentials in BAPC, SatSec and IBE-Auth, limiting traceability but ensuring user anonymity to some level. In our scheme, all the real identity of the owned smart devices are maintained by themselves, which is more secure from the corporate parties' view. The NCC who is responsible for the key generation does not need the genius identity of the smart devices but a unique identical information provided by the trust corporate party, thus, achieving the non-traceability.

B. Storage Overhead

TABLE. III shows the comparison of the total storage consumption of blockchain in the LEO satellite constellation. In IBE-Auth scheme, each satellite maintains a ledger copy, which takes up $n * m * blocks$. SatSec scheme only keeps the blockchain ledgers in data processing center and ground base station, thus, no storage consumption on satellite side. BAPC scheme employs the consortium blockchain but keeps the ledger copy in every satellite, which also requires $n{*}m{*}blocks$

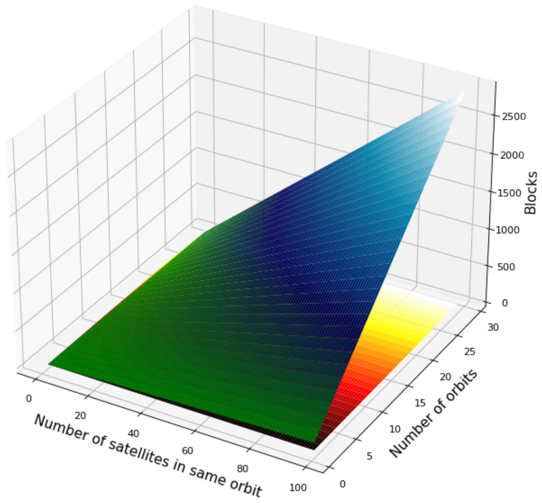


Fig. 7. Storage Consumption on LEO Satellite Constellation

storage space. Our scheme preserves the ledger only in the satellite gateway, which demands storage $m * blocks$. As can be seen from the Fig. 7, our scheme requires much less storage space than IBE-Auth and BAPC.

C. Query Time

In TABLE. III, the query time shows the average time complexity case to find a record in the blockchian ledger. The search space for both IBE-Auth scheme and SatSec scheme is the blockchain ledger size $\mathbf{Size_b}$, the query time is $O(log(size_b))$. However, IBE-Auth scheme requires two queries during the authentication phase, thus, the query time will be $O(2log(size_b))$. Since a fast authentication is implemented for both BAPC scheme and our scheme, the query time under the search space of local cache size $Size_c$ is $O(log(size_c))$.

D. Transmission time

The total transmission time of the authentication phase is summarized in TABLE .III. The IBE-Auth scheme takes $4T_u$, two Round-Trip Time (RTT) of user-satellite, to complete an authentication phase. The SatSec scheme requires one RTT of user-satellite $2T_u$ and another RTT of ground-satellite $2T_g$. The BAPC scheme only needs one RTT of user-satellite $2T_u$, and our scheme demands one RTT of user-satellite $2T_u$ and one RTT of satellite-satellite $2T_s$. Since the transmission time of inter satellites within the same orbit is negligible since they are connected by optical links [4], and the T_g should be smaller than T_u since the ground station always keeps connections to the satellite. Thus, we assume that T_s is $0.1T_u$ and T_g is $0.9T_u$. As shown in Fig. 8, our authentication scheme is much faster than IBE-Auth and SatSec, and slightly slower than scheme BAPC.

VI. Conclusion

The emergence of integrating the LEO satellite constellation into the IoT has attracted lots of attentions for its global coverage and seamless Internet access services. Due to its dynamic topology and frequent link switching of the LEO satellite network, the traditional centralized secure mechanism is no longer applicable. In this paper, we first proposed an blockchain-based authentication architecture for the emerging LEO satellite network assisted IoT. Then, a distributed authentication scheme BC-Authen has been proposed by seamlessly integrating the blockchain technology and the certificateless encryption. By comparing the BC-Authen to IBE-Auth from the storage overhead, the time complexity and the security, the results show the proposed BC-Authen scheme needs less storage space for resource restrained LEO satellite network. Moreover, we employed the certificateless encryption in the BC-Authen scheme, which does not need the genius identity of the smart devices but a pseudonym provided by its owner. The owner of the smart devices maintain the relation between the real identity of the smart devices and the pseudonym. In this way, the NCC could serve the smart devices without knowing its real identity, therefore, the privacy of the smart devices have been preserved. Regarding the sensed data, they are encrypted by the public key of the smart device before transmitting through the satellite, preventing the data leakage to the access satellite.

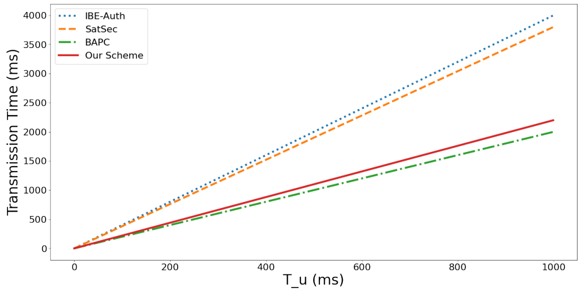


Fig. 8. Transmission Time Consumption of Authentication Phase

The future work will focus on implementing the BC-Authen scheme based on the Hyperledger Fabric, and together with the limited resources sensors, and running the simulation with taking the topology movement from Satellite Tool Kits (STK) and network simulation tool (OMNeT++).

References

[1] Mauro De Sanctis, Ernestina Cianca, Giuseppe Araniti, Igor Bisio, and Ramjee Prasad. Satellite communications supporting internet of remote things. *IEEE Internet of Things Journal*, 3(1):113–123, 2015.

[2] Zhicheng Qu, Gengxin Zhang, Haotong Cao, and Jidong Xie. Leo satellite constellation for internet of things. *IEEE Access*, 5:18391–18401, 2017.

[3] Gartner Report:. Top strategic iot trends and technologies through 2023.

[4] Iridium Satellite LLC. Iridium next (hosting payloads on a communications constellation).

[5] Sudhir K Routray and Habib Mohammed Hussein. Satellite based iot networks for emerging applications. *arXiv preprint arXiv:1904.00520*, 2019.

[6] IOT UK. Satellite technologies for iot applications, 2017.

[7] Baokang Zhao, Puguang Liu, Xiaofeng Wang, and Ilsun You. Toward efficient authentication for space-air-ground integrated internet of things. *International Journal of Distributed Sensor Networks*, 15(7), 2019.

[8] Pandi Vijayakumar, Maria Azees, and L Jegatha Deborah. Cpav: Computationally efficient privacy preserving anonymous authentication scheme for vehicular ad hoc networks. In *2015 IEEE 2nd international conference on cyber security and cloud computing*, pages 62–67. IEEE, 2015.

[9] Maria Azees, Pandi Vijayakumar, and Lazarus Jegatha Deboarh. Eaap: Efficient anonymous authentication with conditional privacy-preserving scheme for vehicular ad hoc networks. *IEEE Transactions on Intelligent Transportation Systems*, 18(9):2467–2476, 2017.

[10] Pandi Vijayakumar, Maria Azees, Victor Chang, Jegatha Deborah, and Balamurugan Balusamy. Computationally efficient privacy preserving authentication and key distribution techniques for vehicular ad hoc networks. *cluster computing*, 20(3):2439–2450, 2017.

[11] Pandi Vijayakumar, Victor Chang, L Jegatha Deborah, Balamurugan Balusamy, and PG Shynu. Computationally efficient privacy preserving anonymous mutual and batch authentication schemes for vehicular ad hoc networks. *Future generation computer systems*, 78:943–955, 2018.

[12] Subramani Jegadeesan, Mohammad S Obaidat, Pandi Vijayakumar, Maria Azees, and Marimuthu Karuppiah. Efficient privacy-preserving anonymous authentication scheme for human predictive online education system. *Cluster Computing*, pages 1–15, 2021.

[13] S. S. Kanhere A. Dorri, M. Steger and R. Jurdak. BlockChain: A Distributed Solution to Automotive Security and Privacy. *IEEE Communications Magazine*, 55(12):119–125, Dec 2017.

[14] Tiago M Fernández-Caramés and Paula Fraga-Lamas. A review on the use of blockchain for the internet of things. *IEEE Access*, 6:32979–33001, 2018.

[15] Pradip Kumar Sharma and Jong Hyuk Park. Blockchain based hybrid network architecture for the smart city. *Future Generation Computer Systems*, 86:650 – 655, 2018.

[16] Z. Lu, Q. Wang, G. Qu, H. Zhang, and Z. Liu. A blockchain-based privacy-preserving authentication scheme for vanets. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, pages 1–10, 2019.

[17] Abbas Yazdinejad, Reza M. Parizi, Ali Dehghantanha, and Kim-Kwang Raymond Choo. Blockchain-enabled authentication handover with efficient privacy protection in sdn-based 5g networks. *CoRR*, abs/1905.03193, 2019.

[18] H. S. Cruickshank. A security system for satellite networks. In *Fifth International Conference on Satellite Systems for Mobile Communications and Navigation, 1996.*, pages 187–190, May 1996.

[19] Ya-Fen Chang and Chin-Chen Chang. An efficient authentication protocol for mobile satellite communication systems. *SIGOPS Oper. Syst. Rev.*, 39(1):70–84, January 2005.

[20] Tzung-Her Chen, Wei-Bin Lee, and Hsing-Bai Chen. A self-verification authentication mechanism for mobile satellite communication systems. *Computers & Electrical Engineering*, 35(1):41 – 48, 2009.

[21] Chin-Chen Chang, Ting-Fang Cheng, and Hsiao-Ling Wu. An authentication and key agreement protocol for satellite communications. *International Journal of Communication Systems*, 27(10):1994–2006, 2014.

[22] Junhao Hu, Lin Cai, Chengcheng Zhao, and Jianping Pan. Directed percolation routing for ultra-reliable and low-latency services in low earth orbit (leo) satellite networks. In *2020 IEEE 92nd Vehicular Technology Conference (VTC2020-Fall)*, pages 1–6. IEEE, 2020.

[23] Qinglei Kong, Rongxing Lu, and Feng Yin. Achieving efficient and secure handover in leo constellation-assisted beyond 5g networks. *IEEE Open Journal of the Communications Society*, 3:641–653, 2022.

[24] Yang Liu, Leiqing Ni, and Mugen Peng. A secure and efficient authentication protocol for satellite-terrestrial networks. *IEEE Internet of Things Journal*, 2022.

[25] H. Yang, H. Zheng, J. Zhang, Y. Wu, Y. Lee, and Y. Ji. Blockchain-based trusted authentication in cloud radio over fiber network for 5g. In *2017 16th International Conference on Optical Communications and Networks (ICOCN)*, pages 1–3, Aug 2017.

[26] C. H. Lee and K. Kim. Implementation of iot system using block chain with authentication and data protection. In *2018 International Conference on Information Networking (ICOIN)*, pages 936–940, Jan 2018.

[27] J. Pacheco X. Zhu, Y. Badr and S. Hariri. Autonomic Identity Framework for the Internet of Things. *2017 International Conference on Cloud and Autonomic Computing (ICCAC), Tucson, AZ*, pages 69–79, 2017.

[28] Shuai Li, Meilin Liu, and Songjie Wei. *A Distributed Authentication Protocol Using Identity-Based Encryption and Blockchain for LEO Network*, pages 446–460. 12 2017.

[29] Caidan Zhao, Mingxian Shi, Minmin Huang, and Xiaojiang Du. Authentication scheme based on hashchain for space-air-ground integrated network. *CoRR*, abs/1902.03683, 2019.

[30] Sheng Cao, Sixuan Dang, Yuan Zhang, Wei Wang, and Nan Cheng. A blockchain-based access control and intrusion detection framework for satellite communication systems. *Computer Communications*, 172:216–225, 2021.

[31] Chengjie Li, Xiaochao Sun, and Zhen Zhang. Effective methods and performance analysis of a satellite network security mechanism based on blockchain technology. *IEEE Access*, 9:113558–113565, 2021.

[32] Xia Deng, Junbin Shao, Le Chang, and Junbin Liang. A blockchain-based authentication protocol using cryptocurrency technology in leo satellite networks. *Electronics*, 10(24):3151, 2021.

[33] X. Lin, X. Sun, P. Ho, and X. Shen. Gsis: A secure and privacy-preserving protocol for vehicular communications. *IEEE Transactions on Vehicular Technology*, 56(6):3442–3456, Nov 2007.

[34] J. K. Liu, C. Chu, S. S. M. Chow, X. Huang, M. H. Au,

and J. Zhou. Time-bound anonymous authentication for roaming networks. *IEEE Transactions on Information Forensics and Security*, 10(1):178–189, Jan 2015.

[35] 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*, 14(2):486–497, Feb 2019.

[36] S. Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System, 2008.

[37] Christian Cachin. Architecture of the hyperledger blockchain fabric. In *Workshop on distributed cryptocurrencies and consensus ledgers*, volume 310, page 4, 2016.

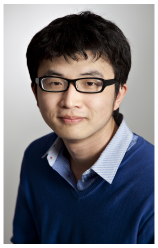
[38] GAVIN WOOD. Ethereum: A secure decentralised generalised transaction ledger. *Ethereum Project Yellow Paper*, 151:1–32, April 2014.

[39] AH Mohsin, AA Zaidan, BB Zaidan, OS Albahri, AS Albahri, MA Alsalem, and KI Mohammed. Blockchain authentication of network applications: Taxonomy, classification, capabilities, open challenges, motivations, recommendations and future directions. *Computer Standards & Interfaces*, 2018.

[40] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang. An overview of blockchain technology: Architecture, consensus, and future trends. In *2017 IEEE International Congress on Big Data (BigData Congress)*, pages 557–564, June 2017.

[41] Joseph K. Liu, Man Ho Au, and Willy Susilo. Self-generated-certificate public key cryptography and certificateless signature/encryption scheme in the standard model: Extended abstract. In *Proceedings of the 2Nd ACM Symposium on Information, Computer and Communications Security*, ASIACCS '07, pages 273–283, New York, NY, USA, 2007. ACM.

Biying Wang received B.Sc and M.Sc degree from Donghua University, Shanghai, China in 2014, and received M.Sc. (Tech.) degree form Mid Sweden University, Sundsvall, Sweden in 2017. She has been granted the right for doctoral level study at the Faculty of Information Technology, University of Jyväskylä, Jyväskylä, Finland since 2017. Her research interests include the security and privacy in IoT, machine learning algorithms.



Zheng Chang (S'10-M'13-SM'17) received the B.Eng. degree from Jilin University, Changchun, China in 2007, M.Sc. (Tech.) degree from Helsinki University of Technology (Now Aalto University), Espoo, Finland in 2009 and Ph.D degree from the University of Jyväskylä, Jyväskylä, Finland in 2013. Since 2008, he has held various research positions at Helsinki University of Technology, University of Jyväskylä and Magister Solutions Ltd in Finland. He has been awarded by the Ulla Tuominen Foundation, the Nokia Foundation and the Riitta and Jorma J. Takanen Foundation for his research excellence. He has been awarded as 2018 IEEE Communications Society best young research professional for Europe, Middle East and Africa Region and 2021 IEEE Communications Society Multimedia Communications Technical Committee Outstanding Young Researcher.

He has published over 140 papers in Journals and Conferences, and received received best paper awards from IEEE TCGCC and APCC in 2017. He serves as an editor of IEEE Wireless Communications Letters, Springer Wireless Networks and International Journal of Distributed Sensor Networks, and a guest editor for IEEE Network, IEEE Wireless Communications, IEEE Communications Magazine, IEEE Internet of Things Journal, IEEE Transactions on Industrial Informatics, etc. He was the exemplary reviewer of IEEE Wireless Communication Letters in 2018. He has participated in organizing workshops and special sessions in Globecom'19, WCNC'18-22, SPAWC'19 and ISWCS'18. He also serves as Symposium Chair for ICC'20 and Publicity Chair for INFOCOM'22. His research interests include IoT, cloud/edge computing, security and privacy, vehicular networks, and green communications.

Shancang Li (Member, IEEE) received the B.Sc. and M.Sc. degrees in mechanics engineering and the Ph.D. degree in computer science from XiâĂŹan Jiaotong University, Xi' an, China, in 2001, 2004, and 2008, respectively. He is currently a Senior Lecturer in Cyber Security with the Department of Computer Science and Creative Technologies, University of the West of England, U.K. His current research interests include digital forensics for emerging technologies, network security, cyber attacks, wireless sensor networks, the Internet of Things, and the lightweight cryptography in resource constrained devices.

Timo Hämäläinen received the PhD degree in telecommunication from the University of Jyväskylä, Finland, in 2002. He joined the University of Jyväskylä, in 1997, where he is currently a professor of computer networks. He has more than 25 years' research and teaching experience of computer networks. He has led many external funded network management related projects. He has launched and leads master programs with the University of Jyväskylä (SW & Comm. Eng.), and teaches network management related courses. He has more than 200 internationally peer reviewed publications and he has supervised almost 40 PhD theses. His research interests include network resource management, IoT, and networking security.