IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received July 2, 2021, accepted August 11, 2021, date of publication August 16, 2021, date of current version August 20, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3104875

Effective Methods and Performance Analysis of a Satellite Network Security Mechanism Based on Blockchain Technology

CHENGJIE LI[1,2], (Member, IEEE), XIAOCHAO SUN[3], AND ZHEN ZHANG[4]

[1]Key Laboratory for Computer Systems of State Ethnic Affairs Commission, School of Computer Science and Technology, Southwest Minzu University, Chengdu 610041, China
[2]National Key Laboratory of Science and Technology on Communications, University of Electronic Science and Technology of China, Chengdu 611731, China
[3]Zhejiang Huayun Information Technology Company Ltd., Hangzhou 310000, China
[4]College of Computer Science, Sichuan University, Chengdu 610065, China

Corresponding author: Chengjie Li (junhongabc@126.com)

This work was supported in part by the Natural Science Foundation of China under Grant 61871422, and in part by the Science and Technology Program of Sichuan Province under Grant 2020YFH0071.

ABSTRACT In satellite communication systems, satellite power and processing capacities are limited, which means that storage and security are also constrained. Satellite communication channels are extremely vulnerable to hackers and external interference signals. Protecting satellite networks from illegal information access and use can be extremely challenging. In this paper, an architecture composed of satellite and ground equipment is developed that integrates communication network authentication and privacy protection structures. In the proposed scheme, the communication, registration, authentication, and revocation of information are achieved through stages to improve communication security. The satellite forwards the collected information to a ground base station, which has a strong data processing capacity. The ground base station records all the key parameters in the distributed blockchain, and all malicious node certificates are removed from the system. To further enhance data transmission security, the key is transferred using an asymmetric encryption algorithm. To measure the robustness of using the proposed network architecture, under the same attack condition, an invulnerability analysis is performed. After conducting simulation experiments, the results show that the proposed scheme greatly improves communication security and protection.

INDEX TERMS Satellite communication system, communication network authentication, privacy protection scheme, ground base station.

I. INTRODUCTION

With the rapid development of computer networks and communication technology, satellite communication has become one of the most important and promising transfer information technologies given its intrinsic advantages of long-range mobile communication, cost-effectiveness of multicast and broadcast systems, wide coverage area, and high flexibility. Satellite communications systems enable the sending and receiving of information worldwide, offering internet access, television, telephone, radio, and other civilian and military operations, the satellite network communication framework structure is shown in FIGURE. 1. The advent of HTS (high-throughput satellite) systems has greatly enhanced technical capabilities and offered wideband services at lower costs. Significant improvements are expected on the forthcoming mega-constellations in low Earth orbits that will deploy thousands of satellites, providing full earth coverage to minimize delays in addition to wide bandwidth. The use of satellites, given these characteristics, can increase efficiency in providing large sets of services and applications that are security-sensitive, such as telemedicine, banking, search and rescue, sensor networks, and content delivery network feed, which generate approximately 90% of the total traffic.

However, in many cases, the security of satellite communication has been seriously compromised, resulting in covert dangers [1]. In satellite communications (and even in terrestrial systems), hackers can interfere, intercept, or modify

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

wireless network systems remotely, attack the equipment of flight crews, and control the positioning and transmission of satellite communication antennas. According to satellite communication protocols, the use of space in satellite communications can be developed independently to enhance communication security. Recommendations have been proposed to further increase the unity and compatibility of communication protocols for space. A single security mechanism is insufficient to meet the security requirements for satellite communication services [2]. In this paper, blockchain technology is introduced to analyze the security of satellite communication networks in terms of access control, confidentiality, and security authentication.

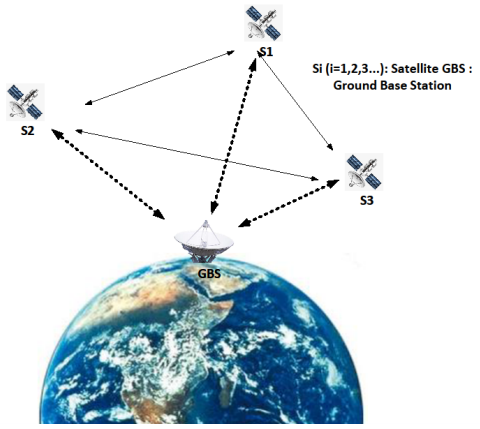

FIGURE 1. Satellite network communication framework structure.

A. ACCESS CONTROL OF THE SATELLITE COMMUNICATION NETWORK

Aside from the Internet, access control represents one of the most important core strategies to ensure the security of the satellite communication network. Concerning access control, the main security risks are unauthorized and illegal access and use of satellite communication resources and data information. In terms of the proportion of hidden dangers in satellite communications, anthropogenic factors are more important than the problems involving the satellite itself.

B. CONFIDENTIALITY OF SATELLITE COMMUNICATION INFORMATION

Satellites employ microwave communication. There are loopholes in the physical layer and the data link layer during the information transmission. Once data are stolen, the consequences could be extremely serious.

C. SECURITY CERTIFICATION OF SATELLITE COMMUNICATIONS

Security authentication is one of the primaries means to counteract active attacks on satellite communication. Because the physical locations of satellites are relatively scattered and the numbers of users and equipment are not fixed, satellites adopt the broadcasting method and use a public key as an authentication algorithm. Thus, security authentication can ensure that the source of the message or the message itself is identified in the open satellite communication network [3].

The traditional network security strategy is still effective and feasible for satellite network security. Traditional network security policies include access control, information encryption, authentication exchange, and security audits. Since the satellite communication network and the Internet have the same network security target, the difference is embodied in the physical link, a particular set of adopted resource management techniques [14] and protocols [15], [16], some specific issues arising from the interconnection with terrestrial networks [17]–[19], and the communication infrastructure. The communication protocol is based on the TCP/IP protocol [20], and the traditional network safety strategy of a satellite communication network is still feasible [4].

Additionally, by using satellite communication network transmission of information with encryption and integrity protection to strengthen the access control and communication infrastructure, identifying communication entities can increase security protection through defensive measures based on blockchain technology. Based on the characteristics of the satellite communication system, providing access control, confidentiality, safety certification, and other safety aspects of satellite communication network management can substantially strengthen satellite network security [5].

Given the numerous threats to network security in the satellite communication network, this study assessed security measures from three aspects. First, to achieve better communication effects, channel parameters were estimated from experimental data, providing a better fit for the transmission channel characteristic function. Second, we applied a traditional security strategy to the satellite network. Third, we strengthened the physical security measures and link security measures of the satellite itself. The rest of this paper is organized as follows: In Section II, we discuss the related technologies, including distributed ledgers, asymmetric encryption, and consensus mechanisms. Section III introduces the implementation process, including network data security and privacy protection and the permission of IoT devices and communication management. In Section IV, we present the details of the simulation and implementation and discuss the simulation results, showing the effectiveness and performance of the proposed scheme. Finally, a short conclusion is provided in Section V.

II. PREPARATORY WORK

A. FITTING PROCESS OF THE CHANNEL TRANSFER FUNCTION

Definition 1: A Gaussian process is a set of random variables; any finite number of random variables in this set are subject to a joint normal distribution.

According to this definition, the following conclusions can be drawn:

Lemma 1: If $X = (X_1, X_2, \ldots, X_n)$ is a set of Gaussian random vectors and $T = (1, 2, \ldots, n)$ is an index set, then

the stochastic process $X = \{X_t\}_{t\in T}$ is a Gaussian process; in contrast, if the stochastic process $X = \{X_t\}_{t\in T}$ is a Gaussian process, then $X = (X_1, X_2, \ldots, X_n)$ is a set of Gaussian random vectors.

A Gaussian process is completely determined by the mean and covariance functions, the mapped independent variables, and high-dimensional feature spaces. After mapping, the independent and dependent variables have a linear relationship such that:

$$f(\mathbf{x}) = \phi(\mathbf{x})^{\mathrm{T}}\mathbf{w} \tag{1}$$

where $\phi(\mathbf{x})$ is the M-dimensional basis function in the satellite communication channel and $\mathbf{w} \sim \mathcal{N}(\mathbf{0}, \sum_p)$. The mean function $m(\mathbf{x})$ and covariance function $k(\mathbf{x}, \mathbf{x}')$ are expressed as follows:

$$\begin{aligned} m(\mathbf{x}) &= E[f(\mathbf{x})] = \phi(\mathbf{x})^{\mathrm{T}}E[\mathbf{w}] = 0 \\ k(\mathbf{x}, \mathbf{x}') &= E[(f(\mathbf{x}) - m(\mathbf{x}))(f(\mathbf{x}') - m(\mathbf{x}'))] \\ &= \phi(\mathbf{x})^{\mathrm{T}}E[\mathbf{w}\mathbf{w}^{\mathrm{T}}]\phi(\mathbf{x}') \\ &= \phi(\mathbf{x})^{\mathrm{T}}\sum\nolimits_p \phi(\mathbf{x}') \end{aligned} \tag{2}$$

B. CHANNEL PARAMETER ESTIMATION PROCESS

Suppose there are n samples $X = [x_1, x_2, \ldots, x_n]$; according to Equation (1), the output is

$$f = [b_1(i), b_2(i), \ldots, b_n(i)]^{\mathrm{T}} \tag{3}$$

in which

$$\hat{b_*}(i) = \mathbf{k}_*^{\mathrm{T}}(K + \sigma_n^2 I_n)^{-1}\mathbf{y} \tag{4}$$

and

$$\begin{aligned} \mathbf{k}_* &= K(X, x_*) \\ &= [k(x_1, x_*), k(x_2, x_*), \ldots, k(x_n, x_*)]^{\mathrm{T}} \end{aligned} \tag{5}$$

where x_* is the Gaussian kernel function; therefore,

$$k(\mathbf{x_i}, \mathbf{x_j}) = \theta_1^2 \exp(-\frac{||\mathbf{x_i} - \mathbf{x_j}||^2}{2\theta_2^2}) \tag{6}$$

The parameter estimation results of the satellite channel can be derived using the formula:

$$\hat{b(i)} = \mathrm{sgn}(\mathbf{k}_*^{\mathrm{T}}(K + \sigma_n^2 I_n)^{-1}\mathbf{y}) \tag{7}$$

C. BLOCKCHAIN TECHNOLOGY

Blockchain is a new application model of distributed data storage, peer-to-peer transmission, consensus mechanisms, encryption algorithms, and other computer technologies. In essence, it is a decentralized database. As the underlying technology for Bitcoin, it is a series of data blocks associated with one another by cryptographic methods. Each data block contains information on a batch of Bitcoin network transactions, which is used to verify the validity of its information (anti-counterfeiting) and generate the next block [6].

D. DISTRIBUTED LEDGER

The distributed ledger refers to the transaction accounting performed by multiple nodes located in different locations. Each node keeps a complete account so that all can participate in monitoring and testifying to the transaction's legality. Different from traditional distributed storage, distributed blockchain storage is unique in two aspects. First, each blockchain node stores complete data according to the blockchain structure. Second, the storage of each blockchain node is independent and has the same status, and the consistency of storage is guaranteed by the consensus mechanism. No single node can record the ledger data separately, thus avoiding the possibility that a single bookkeeper can be controlled or bribed to make false bookkeeping. There are enough accounting nodes so that, in theory, unless all nodes are destroyed, the accounts will not be lost, thus ensuring the security of the accounting data.

E. CONSENSUS MECHANISM

The transaction information stored on the blockchain is public. However, account identification information is highly encrypted and can only be accessed under the authorization of the data owner, thus ensuring the security of the data and the privacy of the individual.

The consensus mechanism determines how consensus is reached among all accounting nodes to determine a record's validity, which is both a means of identification and a means to prevent tampering. The consensus mechanism of blockchain can be characterized as ''the minority is subordinate to the majority'' and ''everyone is equal''. The former does not completely refer to the number of nodes but can also refer to the computing power or other characteristic quantities that computers can use to compare. The latter means that when nodes meet the conditions, all nodes have the right to prioritize the consensus result directly recognized by other nodes, which may eventually become the final consensus outcome. In the case of Bitcoin, which uses proof of work, it is only possible to fake a nonexistent record if more than 51% of the entire network's billing nodes are manipulated. When enough nodes join the blockchain, it is almost impossible to eliminate the possibility of counterfeiting. The establishment of a data management system based on blockchain in satellite communication adopts a decentralized system structure in which an equipment management system is used to set equipment rights and communication control. The management system is under the blockchain records, ensuring the integrity and immutability of the rights and the control records of the device and separating data from data access rights. The blockchain-based system eliminates the security risks of the central authority while all the operations of the application on the data are recorded, ensuring the security of the data.

III. IMPLEMENTATION PROCESS

A. SATELLITE COMMUNICATION CHANNEL ESTIMATION

The satellite communication channel is different not only from the common mobile channel but also from the ground

station channel. The satellite communication channel is the fusion of the satellite channel and the mobile communication channel. From II.(A) and II.(B), the satellite channel waveform is illustrated in FIGURE. 2. In FIGURE. 2, the x-axis is the number of samples, and the y-axis is f in Equation (3).

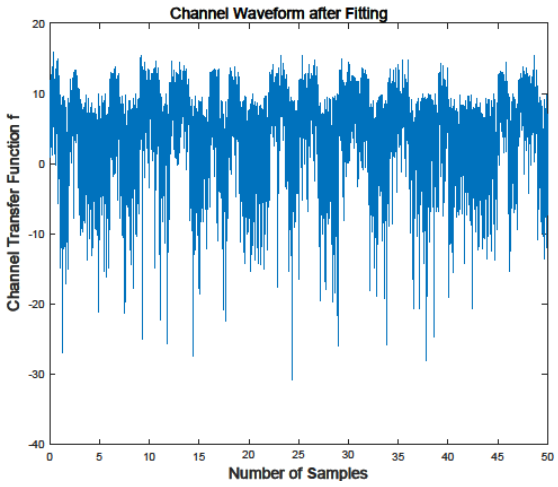

FIGURE 2. Satellite channel waveform.

B. NETWORK DATA SECURITY AND PRIVACY PROTECTION

To manage data and authority, a decentralized personal data management system can be achieved by introducing blockchain technology into the satellite communication network and combining blockchain technology with an off-chain database to separate data and data authority. Before an application can access user data, it would need to obtain access authorization from the user (e.g., user authorization instructions, information storage, query instructions). A distributed database is where user data are encrypted and stored outside the blockchain. When a user wants to change the authorization of certain data by an application, it sets the permissions and the records of granted permissions and data pointers on the blockchain. When an application needs to access certain data, it issues a data access request and records it to the blockchain. The system then checks the signature and blockchain records to confirm whether the application has access to the corresponding data. If the check succeeds, the operation is recorded on the blockchain, and the data are returned to the application by the database. Since blockchain keeps a complete record of the application's behavior, users in the system can change data access rights at any given time.

To protect user privacy, digital signature technology can be introduced. A digital signature is a technology used to verify the integrity and source of a file (or data) to ensure that the file (or data) has not been modified and cannot be repudiated. To achieve better protection, the KSI (keyless signature infrastructure) system is introduced in this paper. A KSI system is a keyless signature authentication system based on blockchain technology. As a multi-signature system, multiple files can be signed at once per slot. Within each slot, the system collects the respective hash values of all the files that need to be signed. The system takes the hash value as the leaf node, constructs the Merkle tree, and calculates the root node value. The system makes the root node value calculated by each time slot public, records it on the blockchain, and distributes it on each node. Blockchain ensures the immutability of recorded root node values. After the system publishes the block that records the root node value, the file sender constructs the corresponding root node value and timestamp information into the signature of the corresponding file. The sender needs to transmit the file with the corresponding signature to the file receiver. After the file and the corresponding signature are received, the receiver must verify the file signature. The receiver extracts the node information from the signature, runs the hashing algorithm, builds the Merkle tree, and calculates the root node value. After calculating the root node value, the receiver then compares it with the data stored on the blockchain and verifies the integrity of the file.

C. PERMISSION OF IOT DEVICES AND COMMUNICATION MANAGEMENT

Devices can control or communicate with each other (e.g., data access). Instructions can only be executed if the device has permissions. Blockchain can record communication or control commands and permissions between devices. The initial phase of system operation includes the generation of required keys and initial blocks. After the user has defined the policies required by the system, they are recorded to the initial block. During system operation, devices need to communicate with each other or control each other. The device needs to be authorized by the user before it can obtain the key distributed by the system for communication or control to ensure the security and privacy of communication. Communication between devices and control instructions are chronologically recorded to the blockchain. After the blockchain system releases a block that records the instructions, the device's identity and permissions are confirmed before the instructions can be executed [7].

IV. SIMULATION AND IMPLEMENTATION

In this section, the performance of the proposed architecture is evaluated by various metrics, such as the certification delay, detection accuracy, and throughput. In the following simulation, the system considered for the experiment is an Intel(R) Core^{TM} i3-3240 CPU@3.40 GHz. The various experimental parameters are shown in Table 1.

A. INFORMATION SECURITY AUTHENTICATION AND THROUGHPUT

1) IMPLEMENTATION PROCESS

In the security mechanism framework of satellite network communication (shown in FIGURE. 3), the GBS (ground base station), identified as a trusted body, provides key authentication for sensor nodes and manages all key parameters. GBS performs the tasks of key parameter generation, node registration, parameter allocation, and blockchain generation. These key parameters are securely shared with the

TABLE 1. Simulation parameters.

Parameter	Value	Parameter	Value
Sensor node	200	Satellite attitude altitude	600 km
DPC position	Static random	Hash algorithm	SHA-256
Sensing area	100×100 km^2-400×400 km^2	Antenna	Dual-polarization VHF
Mobility	Random-way point	Packet size	512 bytes

DPC (data processing center), which stores all these parameters in its tamper-proof key mechanism. Therefore, only GBS can obtain the true identity of the registered sensor node. S_i $(i = 1, 2, 3, \ldots)$ collects information about all its members during communication and forwards the collected information to GBS. S_i $(i = 1, 2, 3, \ldots)$ performs the task of sensing from the region of interest, and the detected information is forwarded to the GBS. The architecture implemented with this scheme meets the standards for encryption, nonrepudiation, protection identification, and internal/external attacks.

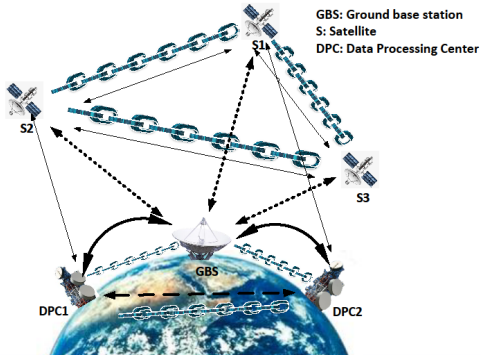

FIGURE 3. Framework of the satellite network communication security mechanism.

a: AUTHENTICATION

Two types of authentication are resolved: information authentication and satellite sensor node authentication. Information authentication verifies that the information acquired during communication is created by a valid satellite sensor node and does not change. The authentication of sensor nodes, also known as mutual authentication, involves the identification of satellites during communication.

b: NONREPUDIATION

This property makes it possible for the receiver to prove to a third party that the sender cannot reject its responsibility to collect the information.

c: PROTECTION IDENTIFICATION

Each satellite sensor node has to broadcast information regarding location, movement speed, and collection frequently.

d: INTERNAL AND EXTERNAL ATTACKS

External and internal attacks can disrupt overall performance and exploit security holes in the network. In-house attacks propagate false information and hide the true identity of the authentication node. These attacks deliberately acquire control over other nodes and force them to act as malicious nodes. An attacker from outside may compromise the system's functionality by modifying routing information and replaying old packets over the network.

In the proposed scheme, the communication channel is assumed to be unsecured, meaning that an adversary can steal, eavesdrop, and receive the information exchanged. An attacker can also attack conventional satellite sensors and DPCs and extract as much information from them as possible.

The performance of the proposed architecture is impacted by the authentication mechanism, nonrepudiation, and internal and external attacks. Network performance is measured by certification delay. From FIGURE. 4, as the number of nodes increases, the certification delay time of the network also increases. In the proposed scheme, the network architecture performs better than the TRBR [12] and the AAKA [13].

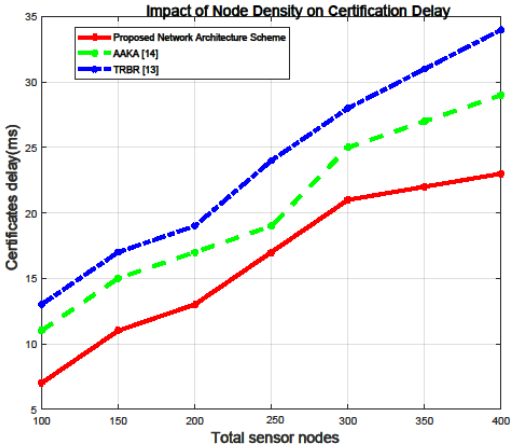

FIGURE 4. Impact of node density on the certification delay.

2) NETWORK THROUGHPUT

The proposed scheme is developed to solve the security problem of using a centralized database in satellite communication. In this scheme, two types of sensor nodes are used: conventional (S) and data processing center (DPC). S has limited resources in terms of energy, storage, and processing capacity. These sensor nodes sense what is happening around them and forward the information gathered to the DPC. The DPC is responsible for collecting information from S and forwarding it to the base station GBS, which, being the trusted body, is responsible for the authentication of all sensor nodes S. Initially, the legitimacy of node S is granted by the GBS before it is able to join the network. Node S obtains the authentication information and parameters from the base station GBS. The S sensor forwards the sensed information to the DPC. The DPC then forwards the information to the base station via a wireless medium, allowing attackers to steal and falsify data (e.g., location, speed, identity, and perception

information) during transmission. Therefore, a privacy protection scheme based on blockchain is proposed to mitigate these risks.

The scheme is divided into initialization, registration, sensor node authentication, message signature, verification, key update and retraction, and tracking phases. Initially, all parameters required for all phases are calculated by the GBS. All conventional sensor nodes can initialize the process by providing their information to the DPC, which then transmits all information to the GBS. Once the information is collected, the GBS uses this information to build an immutable key mechanism (UKM), which is then distributed to the entire DPC. The DPC stores the UKM, and further keys are distributed among the conventional sensor nodes.

Throughput is the amount of data passed over a network (channel or interface) per unit time and is often used to measure network performance. We tested the simulation time using throughput for the proposed network architecture. The test results are shown in FIGURE. 5. As shown in FIGURE. 5, the proposed network architecture scheme performed better than the TRBR [12] and the AAKA [13].

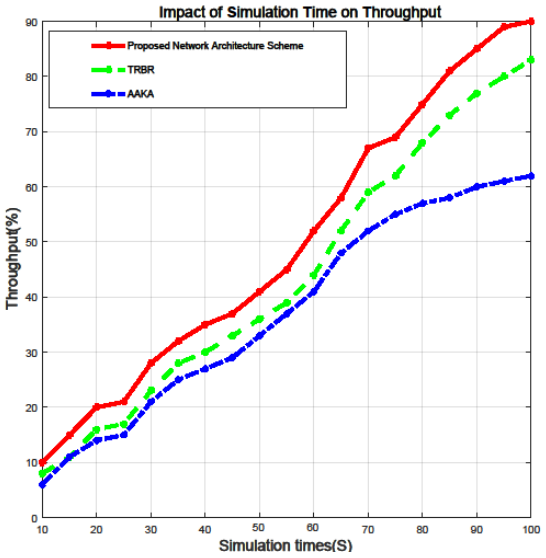

FIGURE 5. Impact of simulation time on throughput.

For different types of attacks, a differential fault attack model was used to analyze the satellite network [8]. The performance in satellite network attacks [9] is discussed in the following section.

The impact value of network throughput is calculated using the formula:

$$\Delta T = \begin{cases} 1, & T_1 < T_2 \\ -\log_2^{(\frac{T_2}{T_1})}, & T_1 > T_2 \\ 0, & T_1 = T_2 \end{cases} \tag{8}$$

where T_1 and T_2 are the throughputs of the network before and after the attack. ΔT is the throughput decline value after the network is attacked; the higher the value of ΔT, the greater the throughput decreases [6], [10], [11].

The results are shown in Table 2. Compared with the existing TRBR [12] and AAKA [13] schemes, the proposed scheme has superior performance.

TABLE 2. Throughput decline value after the network is attacked.

Algorithm	Throughput of the network before the attack (Gbit/s)	Throughput of the network after the attack (Gbit/s)	ΔT
TRBR [12]	0.1844	0.1545	0.2552
AAKA [13]	0.1403	0.1047	0.4223
Proposed Scheme	0.1691	0.1656	0.0302

B. BLOCKCHAIN GENERATION AND DATA SHARING

1) COMPONENTS OF THE PROPOSED BLOCKCHAIN SOLUTION

a: GROUND BASE STATION (GBS)

The GBS is an important component of the blockchain system that supports wireless sensor networks. The GBS generates the validation information, and the mining process of block generation is performed. The verified block is then added to the blockchain and broadcast over the network. When the certificate of any satellite sensor node is revoked, new key parameters are updated to the blockchain. The GBS ensures authentication between sensor nodes and provides them with authentication within their communication range.

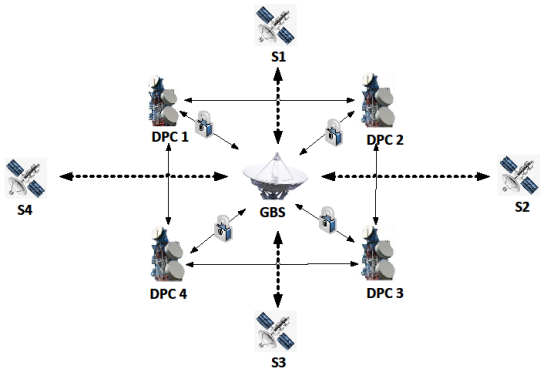

FIGURE 6. Framework structure of data transmission and encryption in blockchain technology.

b: DATA PROCESSING CENTER (DPC)

The DPC is also a major component in the blockchain. The key parameters stored in the blockchain are provided by the GBS to the DPC during the authentication process. The DPC stores all these parameters to UKM. These nodes are responsible for passing the collected information to the GBS.

c: MESSAGE

In this framework, three messages are essential: registration messages, authentication messages, and revocation messages. The framework structure for data transmission and encryption in blockchain technology is shown in FIGURE. 6 [7].

2) ASYMMETRIC ENCRYPTION

In this paper, the ECC (elliptic curve encryption algorithm) was used. The algorithm flow chart is shown in FIGURE. 7.

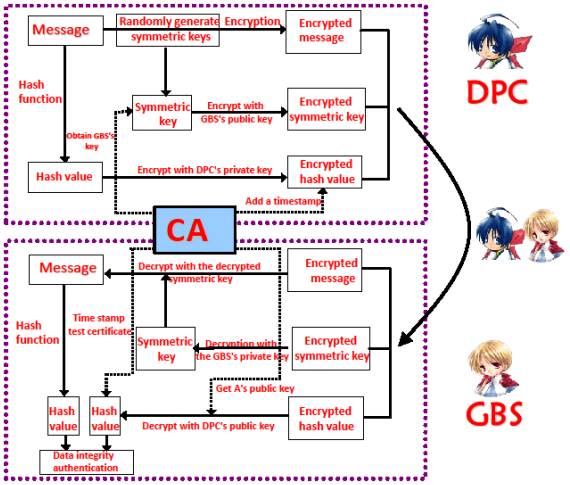

FIGURE 7. Flow chart of the asymmetric encryption algorithm.

3) IMPLEMENTATION PROCESS

The system used in the experiment is an Intel(R) Core™ i3-3240 CPU@3.40 GHz.

Once the GBS successfully performs the certification process, the legitimacy of all satellite sensor nodes S_i ($i = 1, 2, 3 \ldots$) is verified. Information about key parameters is shared with all of its DPCs, as shown in FIGURE. 2, and a blockchain is generated. Key parameters stored in a centralized database are more likely to attract the attention of hackers, thereby compromising their security. Once an attacker performs malicious activities on the central data storage, all stored information can potentially be accessed. To avoid this, blockchain-based information storage is used. The legitimate satellite sensor node S_i ($i = 1, 2, 3, \ldots$) is encrypted with asymmetric cryptography, and the storage is distributed in a certain way. All key information of the satellite sensor node S_i ($i = 1, 2, 3 \ldots$) is stored on the blockchain, making it difficult for attackers to crack. Some of the features of blockchain are as follows [21], [22]:

a: AUTONOMY

Autonomy is one of the most important blockchain features, allowing the blockchain to operate without any central control. Any node can publish a transaction if it is validated by the rest of the network. The information stored on the blockchain is public, and any node can join the network at any time.

b: DISTRIBUTED

A blockchain works in a distributed manner over a peer-to-peer network, where each signed transaction is broadcast over the network, avoiding the single failure point problem. Adjacent nodes check the validity of upcoming transactions and transmit each verified transaction. Invalid transactions are discarded by the node, and the network synchronizes with newly updated transactions.

c: IMMUTABILITY

A valid blockchain recorded in the global ledger is virtually immutable due to the validation required by other nodes in the network. All transactions in the global ledger are synchronized according to a conformance mechanism to ensure the authenticity and accuracy of the data in the ledger.

d: CONSENSUS

The blockchain has a consensual mechanism dependent on the state of relevant information. The consensus-building process is achieved by enforcing a set of rules without central control. These rules are executed successfully and correctly without human involvement.

TABLE 3. Average detection accuracy.

Algorithm	Average Detection Accuracy
TRBR [12]	63.505
AAKA [13]	55.238
Proposed Scheme	72.026

As shown by the results in Table 3, the proposed scheme performed considerably better than the existing TRBR [12] and AAKA [13] schemes.

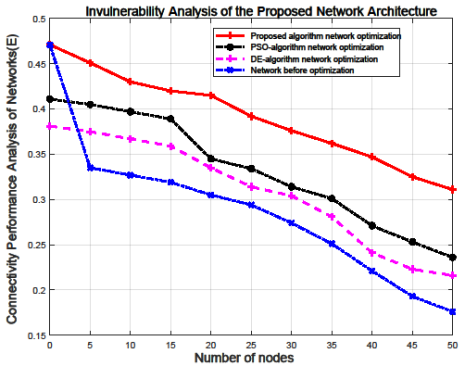

FIGURE 8. Invulnerability analysis of the proposed network architecture.

C. INVULNERABILITY ANALYSIS OF THE PROPOSED NETWORK ARCHITECTURE

To better verify the security of the proposed architecture, its invulnerability under random attack is analyzed. The various experimental parameters are shown in Table 1, and the cost function is given in formula (9),

$$E = \frac{1}{N(N-1)} \sum_{i \neq j} \frac{1}{l_{ij}} \tag{9}$$

where l_{ij} is the distance of node i and node j, and the formula measures the connectivity of a network under random attack. The test results are shown in FIGURE. 8. The connectivity performance of the proposed network architecture under random attack is significantly improved compared with that before optimization, which indicates that the invulnerability of the optimized network is significantly improved, and the connectivity performance is significantly better than the DE

(differential evolution) algorithm network optimization and PSO (particle swarm optimization) network optimization. With an increase in the number of nodes, the connectivity of the network decreases, and the network architecture proposed in this paper decreases more slowly than any of them.

V. CONCLUSION

The privacy protection authentication scheme based on blockchain data storage can effectively provide a security protection mechanism for satellite communications. Initially, the registration and certification processes for all satellite sensor nodes are carried out by the base station, ensuring the authenticity of the sensor nodes. After completing the authentication process, all key parameter information is stored in the DPC's immutable key mechanism (UKM). The GBS transmits key parameter information to the satellite sensor nodes, which then record the key parameters on intersatellite blockchain technology to improve the invariance and transparency of the acquired data. The simulation results show that the proposed method was able to significantly improve security and protection for satellite communications.

REFERENCES

[1] F. Feng and M. Kowalski, "Underdetermined reverberant blind source separation: Sparse approaches for multiplicative and convolutive narrowband approximation," *IEEE/ACM Trans. Audio, Speech, Lang. Process.*, vol. 27, no. 2, pp. 442–456, Feb. 2019.

[2] S. Rathore, Y. Pan, and J. H. Park, "BlockDeepNet: A blockchain-based secure deep learning for IoT network," *Sustainability*, vol. 11, no. 14, p. 3974, Jul. 2019.

[3] C. Li, L. Zhu, Z. Luo, and Z. Zhang, "Solutions to data reception with improve blind source separation in satellite communications," in *Proc. IEEE Int. Symp. Netw., Comput. Commun. (ISNCC)*, Montreal, QC, Canada, Oct. 2020, pp. 1–5.

[4] Y. Chen, W. Wang, Z. Wang, and B. Xia, "A source counting method using acoustic vector sensor based on sparse modeling of DOA histogram," *IEEE Signal Process. Lett.*, vol. 26, no. 1, pp. 69–73, Jan. 2019.

[5] M. E. Sudip, A. Mukherjee, A. Roy, N. Saurabh, Y. Rahulamathavan, and M. Rajarajan, "Blockchain at the edge: Performance of resource-constrained IoT networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 32, no. 1, pp. 174–183, Jan. 2021.

[6] S. Fu, J. Gao, and L. Zhao, "Integrated resource management for terrestrial-satellite systems," *IEEE Trans. Veh. Technol.*, vol. 69, no. 3, pp. 3256–3266, Mar. 2020.

[7] R. Goyat, G. Kumar, R. Saha, M. Conti, M. K. Rai, R. Thomas, M. Alazab, and T. Hoon-Kim, "'Blockchain-based data storage with privacy and authentication in Internet-of-Things," *IEEE Internet Things J.*, early access, Aug. 24, 2020, doi: 10.1109/JIOT.2020.3019074.

[8] Y.-H. Zhao, Z.-L. Wang, J.-Z. Xu, and X.-J. Guo, "Realization algorithm of satellite network attack graph based on performance state space," *J. Shenyang Univ. Technol.*, vol. 33, no. 2, pp. 202–207, Apr. 2011.

[9] Y. Wu, W.-C. Jiao, Y.-H. Pan, and H. Li, "Analysis of cipher security and cipher attack modeling in satellite network," *Comput. Technol. Develop.*, vol. 21, no. 6, pp. 140–144, Jun. 2011.

[10] H. Yang, Y. Liang, Q. Yao, S. Guo, A. Yu, and J. Zhang, "Blockchain-based secure distributed control for software defined optical networking," *China Commun.*, vol. 16, no. 6, pp. 42–54, Jun. 2019.

[11] L. Xu and F. Wu, "A lightweight authentication scheme for multi-gateway wireless sensor networks under IoT conception," *Arabian J. Sci. Eng.*, vol. 44, no. 4, pp. 3977–3993, Apr. 2019.

[12] J. Yang, S. He, Y. Xu, L. Chen, and J. Ren, "A trusted routing scheme using blockchain and reinforcement learning for wireless sensor networks," *Sensors*, vol. 19, no. 4, pp. 1–19, 2019.

[13] W.-L. Tai, Y.-F. Chang, and W.-H. Li, "An IoT notion–based authentication and key agreement scheme ensuring user anonymity for heterogeneous ad hoc wireless sensor networks," *J. Inf. Secur. Appl.*, vol. 34, pp. 133–141, Jun. 2017.

[14] C. Roseti, M. Luglio, and F. Zampognaro, "Analysis and performance evaluation of a burst-based TCP for satellite DVB RCS links," *IEEE/ACM Trans. Netw.*, vol. 18, no. 3, pp. 911–921, Jun. 2010.

[15] A. Abdelsalam, M. Luglio, C. Roseti, and F. Zampognaro, "TCP wave resilience to link changes—A new transport layer approach towards dynamic communication environments," in *Proc. 7th Int. Conf. Data Commun. Netw.*, Lisbon, Portugal, 2016, pp. 1–5.

[16] M. Luglio, C. Roseti, G. Savone, and F. Zampognaro, "TCP Noordwijk for high-speed trains," in *Proc. 1st Int. Conf. Adv. Satell. Space Commun. (SPACOMM)*, Colmar, France, Jul. 2009, pp. 102–106.

[17] M. Luglio, C. Roseti, G. Savone, and F. Zampognaro, "Cross-layer architecture for a satellite–Wi-Fi efficient handover," *IEEE Trans. Veh. Technol.*, vol. 58, no. 6, pp. 2990–3001, Jul. 2009.

[18] O. S. Badarneh, P. C. Sofotasios, S. Muhaidat, S. L. Cotton, K. M. Rabie, and N. Aldhahir, "Achievable physical-layer security over composite fading channels," *IEEE Access*, vol. 8, pp. 195772–195787, 2020.

[19] M. Luglio, C. Monti, C. Roseti, A. Saitto, and M. Segal, "Interworking between MANET and satellite systems for emergency applications," *Int. J. Satell. Commun. Netw.*, vol. 25, no. 5, pp. 551–558, Sep. 2007.

[20] F. Belli, M. Luglio, C. Roseti, and F. Zampognaro, "Evaluation of TCP performance over emulated DVB-RCS scenario with multiple RCSTs," in *Proc. Int. Workshop Satell. Space Commun. (IWSSC)*, Siena, Italy, Sep. 2009, pp. 424–428.

[21] H.-N. Nguyen, N.-L. Nguyen, N.-T. Nguyen, A.-T. Le, N.-D. X. Ha, D.-T. Do, and M. Voznak, "Reliable and secure transmission in multiple antennas hybrid satellite-terrestrial cognitive networks relying on NOMA," *IEEE Access*, vol. 8, pp. 215044–215056, 2020.

[22] K. Li, H. Zhou, Z. Tu, W. Wang, and H. Zhang, "Distributed network intrusion detection system in satellite-terrestrial integrated networks using federated learning," *IEEE Access*, vol. 8, pp. 214852–214865, 2020.

CHENGJIE LI (Member, IEEE) received the B.Sc. degree from Qufu Normal University, Qufu (Confucius's hometown), China, in 2004, the M.Sc. degree in applied mathematics from Xihua University, Chengdu, China, in 2010, and the Ph.D. degree in communication and information system from the University of Electronic Science and Technology of China (UESTC), in 2017. His research interests include blind source separation, satellite communications, and intelligent information processing.

XIAOCHAO SUN graduated from Shandong University of Finance and Economics, in 2005. He is currently with Zhejiang Huayun Information Technology Company Ltd., as a Senior Engineer. His research interests include power network informatization, digital supply chain, and intelligent energy.

ZHEN ZHANG received the B.Sc. degree from Sichuan University, in 2005, and the M.Sc. degree from Xihua University, in 2010. She is currently pursuing the Ph.D. degree with Sichuan University. Her research interests include channel code, signal processing, and intelligent information processing.