A Heterogeneous IoT Node Authentication Scheme Based on Hybrid Blockchain and Trust Value

Shiqiang Zhang[1], Yang Cao[2*], Zhenhu Ning[1], Fei Xue[2], Dongzhi Cao[1], Yongli Yang[1]
[1] Faculty of Information Technology, Beijing University of Technology
Beijing, Beijing 100124 - China
[sqzhangbjut@163.com, nzh41034@126.com, dzcaocwz@126.com, yyyyll1218@163.com]
[2]School of Information, Beijing Wuzi University
Beijing, Beijing 100149 - China
[caoyangcwz@126.com, xuefei2004@126.com]
*Corresponding author: Yang Cao

Received April 4, 2020; revised June 9, 2020; accepted August 13, 2020; published September 30, 2020

Abstract

Node identity authentication is an essential means to ensure the security of the Internet of Things. Existing blockchain-based IoT node authentication schemes have many problems. A heterogeneous IoT node authentication scheme based on an improved hybrid blockchain is proposed. Firstly, the hybrid blockchain model is designed to make the blockchain and IoT environment more compatible. Then the proxy node selection mechanism is intended to establish a bridge between the ordinary IoT node and the blockchain, building by calculating the trust value between nodes. Finally, based on the improved hybrid blockchain, the node authentication scheme of the model and proxy node selection mechanism establishes a secure connection for communication between nodes. Safety and performance analysis shows proper safety and performance.

Keywords: IoT, Hybrid Blockchain, Proxy node, Trust value, Authentication

1. Introduction

The internet of things (IoT) is the expansion of the current internet, which integrates with the internet in the way of wired and wireless networks [1]. It uses a large number of sensors, intelligent processing terminals, global positioning systems and so on to realize the interconnection between things and people, between things and things, so as to achieve various tasks of the internet of things. IoT has been widely used in smart cities, smart home, smart medical, environmental monitoring and other practical applications [2-8]. Research based on IoT and related computer technology is also widely launched [9,10], such as cloud computing [11], target location [12], and mobile network [13] are also closely connected with IoT. IoT has penetrated every aspect of people's life.

In the environment of IoT, devices need to work with other devices to accomplish specific tasks. In the process of cooperation, devices need to communicate with each other. To ensure the security of the communication process, both sides of the communication need to conduct identity authentication. Due to the characteristics and limitations of IoT, the traditional authentication protocol for the internet is not suitable for the IoT environment. There are PKI based authentication system [14, 15], certificate-based authentication system [16] and certificateless based authentication protocols [17] for IoT. Still, most of them have various problems, such as energy consumption, computing complexity, security, and centralization.

At present, the decentralized characteristics of blockchain technology bring new opportunities to the security research of the IoT [18]. Currently, for the security problems of the internet of things, blockchain-based solutions mainly focus on security architecture and authentication. Bao et al. [19] proposed a security architecture of IoT based on blockchain, which includes authentication layer, blockchain layer and application layer. Add the blockchain layer in the architecture, receive transaction information from the application layer, and provide blockchain services for IoT. However, when the decentralized blockchain layer is added, the scheme does not consider the limitations of the IoT device and still adopts the centralized authentication form. A distributed access control system based on blockchain is proposed in [20], in which the arbitration role and authority system of the internet of things are added. This solution completely separates the devices in IoT from the blockchain network. Although the limitations of IoT equipment are fully considered, when IoT and quarry networks are completely separated, there are security risks in the connection part. In [21], Sharma et al. proposed an IoT architecture, DistBlockNet model, based on the advantages of SDN and blockchain technology. The model uses chain technology to update the process rule table and points out that the security of the system must adapt to the three-tier environment. In [22], Hammi et al. put the authentication process on the cloud blockchain and put forward a decentralized device node authentication method to ensure the security of the authentication process. Even though the scheme meets the basic requirements in terms of security, due to its authentication process needs to be carried out on the cloud blockchain, the authentication delay is high and does not have applicability, which cannot be realized in many WSN scenarios, and the scheme does not consider cross-domain communication. Almadhoun et al. [23] used a group of fog nodes to provide network connection, localized computing, extended storage for IoT devices, and achieve authentication between IoT device nodes and users. In this scheme, fog nodes are deployed near the IoT devices to provide blockchain services for IoT by using fiber optic gyro nodes as a bridge to realize mutual authentication between IoT

users and devices. Although the scheme has excellent security and scalability, it is only suitable for the IoT environment supporting SDN.

To solve these problems, we propose an authentication scheme for heterogeneous IoT nodes based on blockchain and trust value. The contribution of this paper is as follows:

(1) Proposed an improved hybrid blockchain model. In order to adapt to the heterogeneous IoT device nodes, an improved hybrid blockchain model is proposed, which can improve the scalability and authentication efficiency of IoT device nodes by authenticating devices with different capabilities in the local blockchain and the global blockchain in the hybrid blockchain model.

(2) Proposed a proxy node mechanism. By setting the capability device node as the proxy node and calculating the trust degree of the common node to the proxy node, the common node selects the proxy node according to the trust degree, so as to establish the connection between the common node and the blockchain. According to the trust degree of the common nodes, the agent nodes can predict them and speed up the processing efficiency.

(3) A node mutual authentication scheme is proposed. According to the proposed improved hybrid blockchain model, the identity of heterogeneous nodes can be mutually authenticated. In the global blockchain and the local blockchain, the registration of proxy nodes and common nodes is realized respectively. In the local blockchain, the mutual authentication of nodes in the domain is realized. In the global blockchain, the mutual authentication of nodes across the domain is achieved.

The rest of this article is organized as follows. Section 2 introduces the knowledge of blockchain. Section 3 describes the general scheme. In section 4, the mutual authentication scheme of nodes proposed by us is described in detail. Section 5 analyzes the security of the scheme and verifies its effectiveness through simulation experiments. Finally, Section 6 summarizes this paper.

2. Blockchain

In recent years, blockchain technology has been widely concerned by industries such as academia, industry, and the financial community. It originated from the paper " Bitcoin: A peer-to-peer electronic cash system" published by Nakamoto in 2009 and was first presented to the world in the form of bitcoin [24]. The blockchain is actually a distributed ledger that stores funds and transaction records through the P2P network, which has non-tamperable features. This feature determines that it can be widely used in various fields [25-28]. This technology may also be combined with AI in the future [29-31], intelligent algorithm [32-34], data protect [35]. Blockchain enables some technologies [36,37] to execute in an untrusted environment

The blockchain is structurally a chain structure that is connected end to end, as shown in **Fig. 1**. Each block is composed of a block header and a block body. The transaction record in the block (the content that must be stored in the database) is stored in the block body. The block head includes two sets of metadata: (1) information about mining, including timestamp, difficulty target, and Nonce value; (2) information about the block itself, including the field connecting the parent block, the version number, and the Merkle tree root. The transactions are bundled, submitted to the blockchain in chunks, and all blocks are connected using cryptographic techniques in a defined order. In this way, all the modules together form an ordered chain structure. The encryption algorithm and the consensus mechanism serve as the underlying technology to ensure the operation of the blockchain. The encryption algorithm

guarantees the inevitable modification of the data, and the consensus mechanism guarantees the consistency of the distributed ledger.

Blockchains can be divided into public chains, alliance chains, and private chains. The public chain means that any machine can participate in the operation of the blockchain as a peer node. Only when the participant can post the transaction on the chain, and the transaction can be verified by other nodes, the participant can participate in the blockchain. Bitcoin is the most representative public chain. The alliance chain refers to the fact that the consensus process on the chain is completed by predetermined nodes, so the alliance chain is considered to have partial decentralization. Private chains refer to the use of blockchains only for billing operations, but they are not publicly available. The idea of a private chain can be either a company or an individual. The latter must write access to the blockchain separately and implement strict access control.

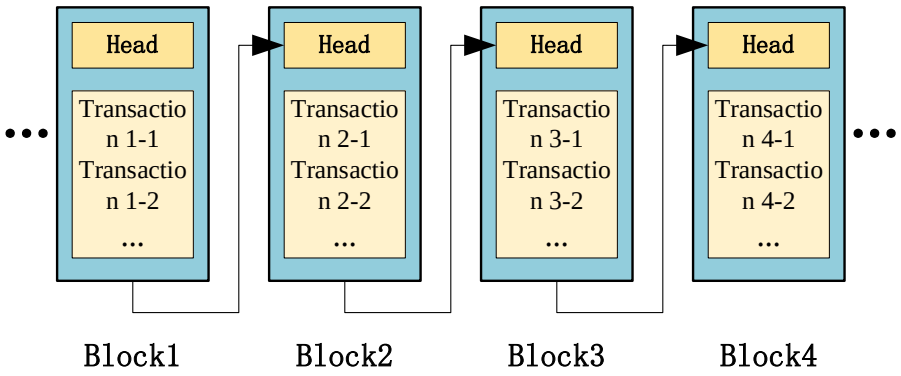


Fig. 1. Blockchain structure

3. General Scheme

3.1 System Model

The IoT contains thousands of heterogeneous devices to sense data and perform related tasks. The devices cooperate to accomplish the tasks. In the whole environment of the IoT, there are many heterogeneous sub-networks, each of which is built according to different needs. The sub-networks together constitute the heterogeneous IoT, as shown in **Fig. 2**. Ordinary IoT sub-networks include smart home networks, wearable devices, wireless sensor networks, wireless radio frequency networks, logistics networks, onboard IoT and so on. In each sub-network, devices with different capabilities are required to perform different functions. According to the capability of the devices, we divide the devices in the IoT into two categories: ordinary device nodes and capability device nodes. In addition to these two types of device nodes, there is also a kind of node responsible for managing the network. They can be the owner of the network or the manager of the network. We call them management nodes.

Ordinary device node. In the IoT environment, most device nodes are ordinary device nodes, which have limited capabilities. In terms of computational capability, only simple operations can be performed, which is not enough to support complex cryptographic algorithm-related calculations; in terms of storage space, because of its simple structure and single function, such devices often do not have ample storage space, but can only store Limited data; in terms of energy, many nodes are deployed in unattended areas, without energy supplement. Consumption is a bottleneck. Ordinary device nodes usually undertake

simple and single tasks in the network, such as sensor nodes in wireless sensor networks, smart cameras in smart home networks, smart refrigerators, and wearable devices such as bracelets, watches, etc. These single-function devices do not support the realization of other functions while completing their own tasks.

Capability device node. In the IoT, there are other devices with robust capabilities, which we call capability device nodes. Capability device nodes are better than ordinary device nodes in computing power, storage capacity, and energy. These nodes generally play a more important role in the network, such as cluster head nodes in wireless sensor networks, personal computers in smart home networks, robots in logistics networks and so on. These devices can accomplish their own tasks in addition to the same. There are spare efforts for other nodes, such as forwarding data, collaborative computing and so on. In this authentication scheme, some capability device nodes are selected as proxy nodes to act as bridges between ordinary device nodes and management nodes.

Manager node. For each sub-network, a manager is needed to coordinate its unified management. Generally, the node is assumed by the owner or manager of the network, and each management node has a public blockchain account. In different IoT networks, the shape of these nodes is different, which can be in the form of gateway nodes, base station nodes and so on.

In the latter description, the capability device nodes selected as the proxy node is called the proxy node. The residual capacity device node and the ordinary device node are unified as the ordinary node, and the management node is still the management node.

In this model, there are two main modes of communication between nodes: communication between two nodes in the same sub-network; communication between nodes in different sub-networks, because the managers of two nodes belonging to different sub-networks are different, they can not directly authenticate.

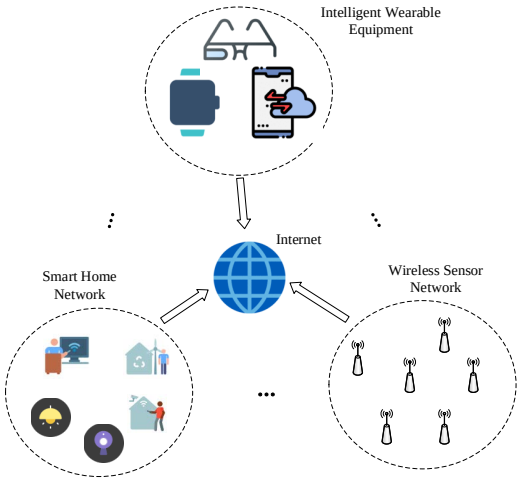


Fig. 2. System model

3.2 Improved Hybrid Blockchain Model

For public blockchain, all nodes join the network in an open form as peers to participate in the consensus process of blockchain, to build a blockchain network. However, in the heterogeneous IoT model mentioned above, because of the large number of nodes, if all nodes join the public blockchain, the time required for the consensus process will be significantly prolonged, which is contrary to the real-time requirements of the IoT. Private chains have the

problem that the devices of the IoT belong to different sub-networks and can not form peer-to-peer nodes, and can not join the same private chain through unified identity authentication. Therefore, based on the hybrid blockchain model proposed in our previous work[38], an improved hybrid blockchain model is proposed for the heterogeneous IoT network model mentioned above, as shown in **Fig. 3**. The improved hybrid blockchain model consists of the following two parts: global blockchain and local blockchain.

Global blockchain. All management nodes in the IoT are connected to the alliance chain as miners to form a global blockchain. The global blockchain can register and authenticate the proxy nodes, store the identity of all nodes in the network, and authenticate the cross-domain communication in the network to construct secure communication. Smart contracts are deployed on the global blockchain, and the agent nodes are registered and stored by contract rules. When nodes in different sub-networks communicate across domains, authentication is also required through intelligent contracts deployed on the global blockchain.

Local blockchain. The local blockchain is composed of proxy nodes in the same region that have passed the global blockchain authentication. Local blockchain realizes the identity registration of nodes in local network and communication authentication between nodes. The smart contract for verifying the local registration and authentication requests submitted by the proxy node is deployed on the local blockchain network. The member nodes in the local blockchain submit the registration identity information for the local device nodes to the global blockchain store. When the local blockchain authenticates the local node, the member nodes in the local blockchain download the related identity information from the global blockchain to authenticate the authentication request. In a local network, there may be one or more IoT sub-networks, which are determined by their region (for example, different IoT sub-networks in a building, different sub-networks in a company). The managers or owners of each subnetwork select the proxy nodes and jointly form a local blockchain network.

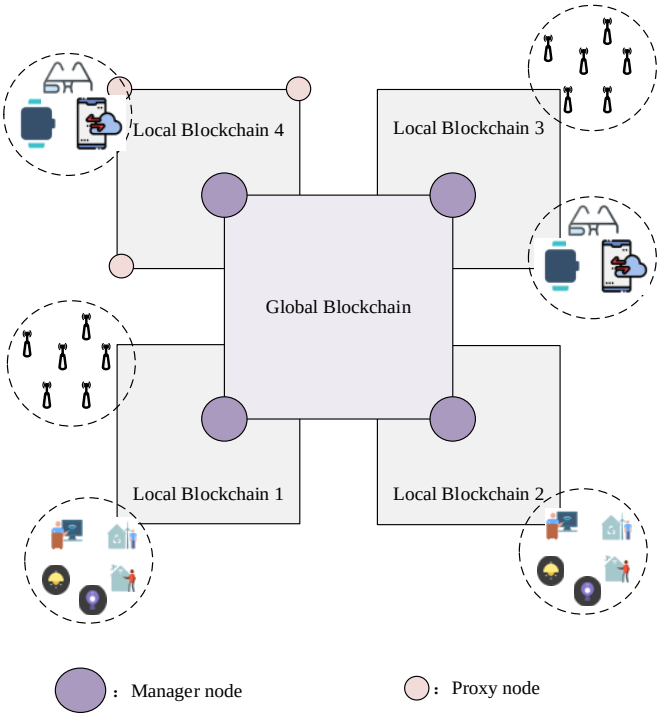


Fig. 3. Improved Hybrid Blockchain Model

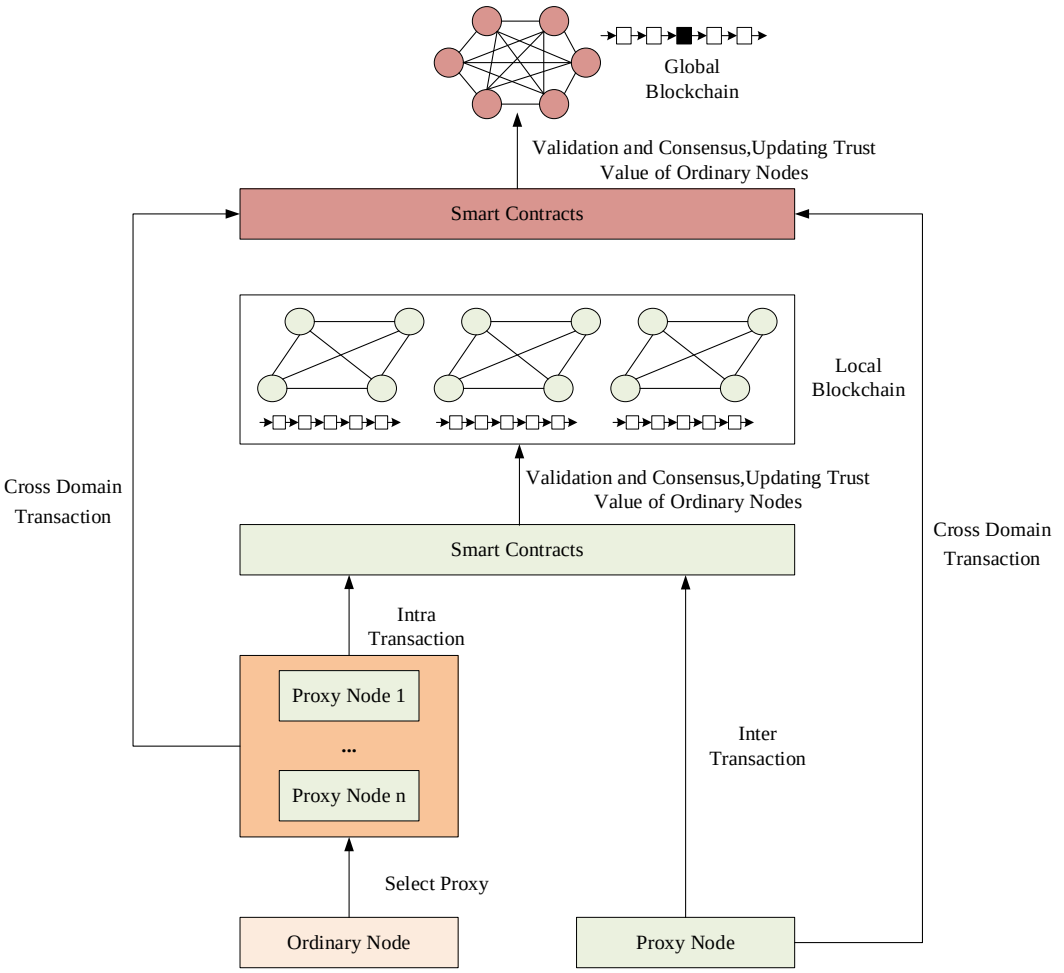


Fig. 4. Overall authentication framework

3.3 Overall Authentication Framework

The overall framework of the authentication scheme proposed in this paper is shown in **Fig. 4**. It mainly includes: (1) the selection of proxy nodes; (2) the submission of authentication transactions; (3) the authentication of device identity information by blockchain, the realization of consensus and the update of trust value of proxy nodes. The proxy node selection mechanism is to divide devices in the IoT into ordinary nodes and capability nodes according to their capabilities. Ordinary nodes select capability nodes as proxy nodes through some mechanism to achieve interaction with blockchain network and complete authentication. Authentication transactions can be divided into local authentication transactions and cross-domain authentication transactions according to the type of communication. Transaction submission will directly affect the delay of authentication. The timeliness of authentication is more reasonable by designing submission rules. In the blockchain validation stage, the authentication transactions are validated and agreed on in the local blockchain network and the global blockchain network respectively according to the internal authentication and

cross-domain authentication, and the trust values of the nodes are updated according to the validation results. This part will be described in more details in this section.

3.3.1 Proxy node selection mechanism

The IoT network model above includes various scenarios of IoT devices. In different situations, IoT devices have different capabilities and functions. However, not all devices have the ability to deploy blockchain software, which is not enough to support the building of a blockchain network. At this time, it is necessary to build a bridge between such devices and the blockchain network. The node with strong capability in local IoT is the right choice. According to the capability of device nodes (including their computing capacity, storage capacity, energy size, etc.), the device nodes of the IoT are divided into ordinary device nodes and capability device nodes.

The network manager (or owner) can select and interact with the blockchain network by setting the capability device node as the proxy node in the local network. Local networks may contain multiple sub-networks (i.e., local devices belong to different managers or owners), so local networks also contain multiple proxy nodes. As a bridge between ordinary device node and blockchain network, the security of the proxy node is more important. How to select a suitable proxy node with high reliability is a problem to be considered? In this paper, we design a method to measure the trust value of proxy nodes. Ordinary device nodes select appropriate proxy nodes according to the trust value of proxy nodes. The proxy node will also make preliminary processing according to the trust value of the ordinary node to improve the efficiency of the blockchain authentication process.

The trust value of an ordinary device node to a proxy node consists of direct trust value and indirect trust value.

Define 1 The trust value of the ordinary node ON_i to the proxy node PN_j $Trust_{ij} = \alpha T\_indirect_{ij} + \beta T\_direct_{ij}$.

Where, T_direct_{ij} denotes the direct trust value of the node ON_i to PN_j, which is directly evaluated by the former; $T\_indirect_{ij}$ denotes the indirect trust value of the node ON_i to PN_j, which is assessed by the neighbour nodes of ON_i; α, β are weight parameters, and $\alpha + \beta = 1$.

The direct trust value of the node ON_i to PN_j is the direct evaluation of the interaction between the node ON_i and the proxy node PN_j, including current authentication results and previous trust values. Calculating as follow:

$$T\_direct_{ij} = \gamma T\_direct_{ij}' + \lambda f(T) \tag{1}$$

Where, T_direct_{ij}' represents the last direct trust value of PN_j, f is the evaluation function, T represents the interactive evaluation value of the proxy nodes. f function can choose weighting function, mean function and so on; γ, λ are weight parameters, and $\gamma + \lambda = 1$.

The indirect trust value of the node ON_i to PN_j is achieved by requesting the trust of the proxy node of other ordinary nodes in the subnet area. When the node ON_i needs to select a proxy node, it first broadcasts the request message to other ordinary nodes in the subnet to

obtain the indirect trust value of all proxy nodes, then calculates and ranks the trust value of all proxy nodes in the current state according to the method defined, and selects the proxy node with the highest trust value as the proxy to submit relevant transaction information.

The trust value of an ordinary device node is determined by its historical authentication record.

Define 2 The trust value of the ordinary node ON_i in the network is defined as $Trust\_O_i^{\tau} = Trust\_O_i^{\tau-1} - Au\_error_i^{\tau}$.

Where, $Trust\_O_i^{\tau}$ denotes the trust value of the node ON_i at τ, and $Trust\_O_i^{\tau-1}$ denotes the trust value in the record. When τ = 1, it is the initial trust value of the ordinary device node. $Au\_error_i^{\tau}$ represents the total number of the authenticate fail times in the current block.

As the owner and manager of the sub-network, it should be able to manage the trust value of the proxy node and the ordinary node to which it belongs. When the trust value of a proxy node is detected to be less than a certain threshold, the management node will revoke the identity of its proxy node; when the trust value of an ordinary node is detected to be lower than a certain threshold, it will revoke the isolation of the node.

3.3.2 Transaction submission and formation block

In the hybrid blockchain model, local blockchains exist in the form of private chains, while global blockchain is an alliance chain. For local authentication, the ordinary node submits the authentication request message to the proxy node, and the proxy node submits to the local blockchain and triggers the smart contract for verification. Block packaging and consensus is one of the critical factors affecting authentication delay. In order to adapt to the high-frequency authentication submission in the IoT environment, this paper designs a corresponding block packaging strategy for different transaction types. There are two types of authentication transactions in this paper. One is the local authentication transaction submitted to the local blockchain. Another is the cross-domain authentication transaction submitted to the global blockchain.

For local authentication transactions, it's submitted to the proxy node. And then the smart contract is triggered to verify the authentication and the verification results are placed in the proxy node transaction pool. When the authentication transactions in the transaction pool meet certain conditions, the proxy node packs the transactions in the pool into blocks and achieves block consensus with other nodes in the local blockchain through the consensus mechanism. After receiving the authentication message sent by the ordinary node, the proxy node checks the number of transactions in the transaction pool, and according to the real-time requirements of the current transaction message submitted (given by the network manager, it can be divided into emergency, general, etc.). The number of transactions in the transaction pool is recorded as sum_trans, the real-time requirements of transactions are recorded as req_rt, the time from the last receipt of emergency authentication transactions is recorded as $time\_last$. When any of the following conditions are met, the proxy node packages the transactions in the transaction pool and submits them to the local blockchain for consensus:

$$time\_last = T\_TH \;\&\&\; sum\_trans \le S\_TH \tag{2}$$

$$sum\_trans = S\_TH \tag{3}$$

Formula (2) denotes that when a proxy node receives an authentication request with high real-time requirement and reaches a certain time threshold, it can pack the transaction in the transaction pool into blocks to submit; formula (3) denotes that when the proxy node has not received authentication transaction with high real-time requirement, it packages blocks and submits them when the transaction number in the pool reaches the threshold.

For cross-domain authentication transactions, the proxy node submits the authentication request to the global blockchain, and the network administrator pays the authentication cost to the global blockchain for verification and consensus.

3.3.3 Smart Contract and Consensus Mechanism

According to different functional requirements, including registration requests and authentication requests of different types of nodes, different verification rules need to be formulated, and the corresponding smart contracts are deployed on the corresponding global blockchain and local blockchain. The specific process will be given below.

Consensus mechanisms are different in alliance chains and private chains. The global blockchain in this paper is a kind of alliance chain, which needs to use the consensus mechanism of the alliance chain. In contrast, the local blockchain belongs to a private chain, which needs to use an efficient consensus mechanism. Users can choose the appropriate consensus mechanism according to their own needs.

4. Authentication Process

According to the above network model and hybrid blockchain model, the corresponding node authentication scheme is designed in this section, and its overall flow is shown in the **Fig. 5**, mainly including four parts:

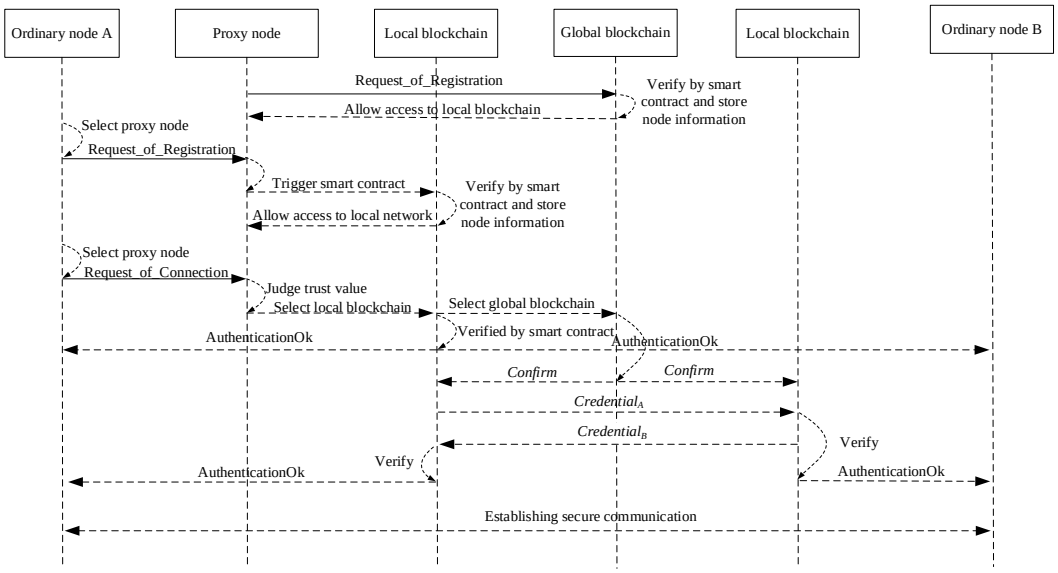


Fig. 5. Authentication flow chart

(1) **Initialization**: Each management node will distribute the required safety materials to its own nodes.
(2) **Registration stage**: The management node forms a global blockchain network, publishes its own information, completes the selection and registration of proxy nodes, and the proxy nodes form a local blockchain. The local blockchain completes the registration of ordinary device nodes in the local network and uploads its information to the global blockchain for storage.
(3) **Authentication stage**: The nodes in the local network are directly authenticated by the local blockchain, and the nodes in different networks are authenticated by the global blockchain.
(4) **Node logout**: When the number of authentication failures reaches a certain number, or the node is attacked, or the energy of the node is exhausted, the node needs to log out.

4.1 Initialization

First, the management node calculates the identity ID_i of the node i according to the Ethernet address EA_i of the node i (including the management node, the proxy node, and the ordinary node) as $ID_i = hash(EA_i)$. And send ID_i to node i for storage. Among them, the management node's identity is marked as *ManagerID* (*MID*), the proxy node's identity is marked as *ProxyID* (*PID*), and the ordinary node's identity is marked as *OrdinaryID* (*OID*). Then, the management nodes generate a *public-private* key pair $publickey_u$ / $privatekey_u$ (puk_u / prk_u) for each node it owns. The *public-private* key pair is used to verify the integrity of the message passing during the execution of the scheme to ensure that the message is not tampered with. Since the focus of this paper is not here, the process will not be described in detail later. Finally, the management node generates *IDcard* to prove its unique legal identity for all the nodes and sends it to the node to save. For node i, its identity card $IDcard_i$ has the following structure:

MID	// Identification of the management node to which node *i* belongs
OID/PID	// Identification of node *i*
$sig_{prk_{MID}}(keccak(XX \| YY))$	// The sequence obtained by the management node signing with the private key, where *XX* and *YY* represent the identity of the management node and node *i*, respectively.

4.2 Registration

IoT devices need to be deployed in the corresponding location after initialization and then self-organize into a network through the corresponding mechanism to accomplish some tasks in coordination. Prior to that, the management node was validated by certificates issued by the manufacturer or the corresponding organization to form a global blockchain. In the process of registration, the device needs to register on the blockchain. Only the device node with legal identity can be allowed to join the network, and the identity information of the legal node can be stored in the blockchain to provide credentials for subsequent node communication authentication. To this end, the corresponding data structure is designed to store the relevant information of nodes in the blockchain more effectively. The structure of the data is shown in **Table 1**.

Table 1. The structure of the data

Attribute	Value
Manager ID	*XX*
Ordinary ID / Proxy ID	*YY*
$publickey_{MID}$	P_1
$publickey_{OID/PID}$	P_2
Tag	*-1/0/1*
Trust value	*TT*

The structure includes the identity and public key of the management node to which the node *i* belongs, the node identity and its public key of the node itself, and the node status label *Tag*, whose value is -1/0/1. The *Tag* default value is 0, indicating that the proxy node is inactive; *Tag* value is - 1 indicating that the node is revoked; *Tag* value is 1 indicating that the node is active. *TT* is the trust value of the node, the value is empty when the node is a proxy node, and the node can be updated dynamically when it is an ordinary node.

4.2.1 Registration of Proxy Node

The proxy node is selected by the management node in the capability device node. The management node chooses the proxy node according to the performance of the equipment node, and publishes the information of the proxy node to the global blockchain, and sets its state information to the inactive state. When a capability device node submits a registration request to the global blockchain as a proxy node, the global blockchain verifies it.

The proxy node sends a registration request message $reg\_req\_p(EA_{PID}, PID, MID, IDcard_{PID}, Time)$ to the global blockchain. The global blockchain receives the registration request message and validates the request message through the smart contract. The validation steps are as follows:

(1) Verify the validity of the timestamp *Time*, if it is valid, continue; otherwise, registration fails;
(2) Verify whether the Ethernet address of the proxy node is legitimate according to the composition structure of the Ethernet address, and then proceed to the next step; otherwise, registration fails;
(3) According to the management node in the global blockchain, judge whether the *MID* in the registration request message is legitimate or not, and then proceed to the next step; otherwise, the registration will fail;
(4) Query whether the proxy node *PID* has been published in the global blockchain. If it has been published and its state is not activated, then continue the next step; otherwise, registration fails;
(5) According to the public key of the management node and the relevant node information in the request message, verify the validity of the $IDcard_{PID}$. If the authentication is

passed, the registration is successful, and the status of the proxy node *PID* is set to the active state; otherwise, the registration will fail.

If anyone of the above steps fails to validate, the node registration will fail, and the global blockchain returns the failure message. Only when all the steps are validated successfully, the global blockchain will send the successful registration message to the local blockchain, allowing the registered node to join the local blockchain network.

4.2.2 Registration of Ordinary Node

The registration process of ordinary nodes is completed on the local blockchain network where they are located. In the registration phase, because the trust value of the ordinary node to the proxy node is in the initial state, it randomly selects a proxy node to submit the registration request message $reg\_req\_o(EA_{OID}, OID, MID, IDcard_{OID}, Time)$.

After receiving the registration request message, the proxy node triggers the smart contract on the local blockchain to verify. The specific steps are as follows:

(1) Verify the validity of the timestamp *Time*, if it is valid, continue; otherwise, registration fails;
(2) Verify whether the Ethernet address of the proxy node is legitimate according to the composition structure of the Ethernet address, and then proceed to the next step; otherwise, registration fails;
(3) According to the management node in the global blockchain, judge whether the *MID* in the registration request message is legitimate or not, and then proceed to the next step; otherwise, the registration will fail;
(4) Query whether the ordinary node *OID* has existed in the local blockchain. If it does not exist, continue to the next step; otherwise, the registration fails;
(5) According to the public key of the management node and the relevant node information in the request message, verify the validity of the $IDcard_{OID}$. If the verification succeeds, the registration is successful, and the state of the ordinary node *OID* is set to the active state, and the node information is uploaded to the local blockchain and the global blockchain storage, otherwise, the registration fails.

If anyone of the above steps fails to validate, the node registration will fail, and the local blockchain returns the failure message. Only when all the steps are validated successfully, the local blockchain will send a successful registration message to the ordinary node, allowing the node to join the local network.

4.3 Node Authentication

When the ordinary node OID_A needs to cooperate with another ordinary node OIDB, it needs to establish secure communication between them firstly, which is realized by mutual authentication of nodes. When the node OID_A and the OID_B establish a secure connection, first, the former needs to calculate the trust value of all the proxy nodes in the local network according to the above formula (1), select the appropriate proxy node according to the trust value, and submit the authentication request message $con\_req\_A(OID_A, MID_A, IDcard_{OID_A}, OID_B, Time)$ to the proxy node. When the proxy node receives the request message, it judges its credibility according to the trust value of node OID_A in the global blockchain. If it is lower than the threshold value, the authentication fails. Otherwise, it continues to operate. It constructs transaction information according to the submitted request message and judges whether the target node is in the same local network as the request node

according to the node information stored in the local block. If it is in the same local network in the network, trigger the smart contract verification of the local blockchain, otherwise submit to the global blockchain and trigger the smart contract to verify the transaction information; in the local blockchain, after the verification is passed, the proxy node judges whether to pack the transaction information according to the above formula (2) (3) according to the transaction situation in its own transaction pool and if the conditions are met, pack the block and submit the local block. The global blockchain smart contract is directly submitted to the network for consensus after passing the verification. The global blockchain is similar to the smart contract process on the local blockchain, and the verification process is as follows:

(1) Verify the validity of the timestamp *Time*, if it is valid, continue, otherwise, registration fails;
(2) Query the identity and public key of the management node to which the node belongs, and verify the correctness of the identity card $IDcard_{OID_A}$ in combination with the relevant identity information. If it is correct, continue, otherwise return *error*;
(3) verify whether node OID_A and OID_B already exist. If they exist, continue; otherwise, *error* will be returned;
(4) verify the status of node OID_A and OID_B. If both of them survive, continue; otherwise, *error* will be returned;
(5) the smart contracts on the local blockchain are in accordance with (5), and the global blockchain is in accordance with (6);
(6) the local blockchain returns the authentication result, and sends the result to the nodes OID_A and OID_B, which establish secure communication;
(7) according to the node information stored on the blockchain, the global blockchain will send confirmation messages $confirm(Voucher\_of\_Transation, Timestamp, OID_A, OID_B)$ to the local blockchain where the OID_A and OID_B are located. $Voucher\_of\_Transation = keccak(OID_A, OID_B, global\_timestamp)$ is the transaction voucher of the global blockchain. The local blockchain $local_A$ where the OID_A is located sends the authentication certificate message $Credential_A = (Voucher\_of\_Transation, local\_timestamp, OID_A)$ and the signature of the message to the local blockchain network $local_B$ where the OID_B is located (which can be obtained by the joint signature of the verification node of the blockchain network $local_A$). The $local_B$ sends the authentication credential $Credential_B = (Voucher\_of\_Transation, local\_timestamp - 1, OID_B)$ and the signature of the message to $local_A$. When both $local_A$ and $local_B$ have passed the authentication certificate of the other party, they will respectively notify OID_A and OID_B of the success of authentication, and establish secure communication between them.

4.4 Node logout

When the energy of the node is exhausted, the proxy node can be selected according to the rules to submit the cancellation request. The proxy node constructs transaction information triggering the smart contract and changes the status of the node to cancel. When the node is attacked or frequently fails to authenticate, and the trust value is lower than the critical value, the blockchain automatically cancels it. As the manager of the node it owns, the management node can directly go to the block. The chain submits the cancellation application and changes the status of the proxy node and ordinary node to be cancelled.

5. Secure Performance and Efficiency Analysis

5.1 Secure Performance Analysis

The authentication scheme proposed in this paper is to establish a secure communication channel for communication between IoT devices in heterogeneous environments. Unlike the traditional internet, the security mechanism in the IoT environment needs to meet certain security mechanisms. In this section, we will analyze the security of this solution against the common security attacks in the IoT.

In general, the security requirements of IoT security mechanisms include integrity, validity, scalability, and non-repudiation.

Integrity. Integrity typically includes message integrity and data integrity. Message integrity refers to the message passing process, or can not be tampered with during the interaction process. The message of the message authentication process in this document is signed by the public key, which can guarantee its integrity. Data integrity means that data stored in the Internet of Things cannot be accessed or tampered with by unauthorized or illegal users. The authentication scheme of this paper is designed for this purpose. Illegal devices and users cannot interact with other devices through authentication or access to their data.

Validity. It means that legitimate devices and users can effectively access and interact with IoT devices. Validity is usually affected by a denial of service attack, and the ability to prevent denial of service attacks will be described later.

Scalability. The IoT contains thousands of devices, with different types and shapes, and frequent device updates. This series of features has led to the scalability of the IoT has always been a difficult problem to solve. In this paper, the IoT devices are hierarchically managed by designing a hybrid blockchain. The blockchain in this region cooperates with the local IoT devices and then connects all the local networks through the global blockchain. In addition, through the smart contract, the legitimate device is authenticated and deregistered, which greatly enhances its scalability.

Non-repudiation. Non-repudiation refers to the fact that a device or user cannot refute a message or action made by itself. This article is based on the blockchain design of the authentication scheme, and all operations are stored on the blockchain, naturally non-repudiation.

In order to meet the above security requirements, the security mechanism for the IoT environment needs to be able to withstand certain network attacks. The attacks on the IoT are also different from those on the internet. Common attacks against the IoT include Sybil attack, Spoofing attack, message substitution attack, message replay attack, man-in-the-middle attack, and denial of service attack. In response to the above attacks, this section makes a corresponding analysis.

Sybil Attack. In the solution proposed in this paper, each device node has a unique Ethereum address EA_i and an identity OID/PID, and each node corresponds to the corresponding management node and is stored on the blockchain. For an attacking node, it is not possible to have multiple node identities at the same time to launch a Sybil attack.

Spoofing Attack. In the solution proposed in this paper, mutual authentication is required before the node communication. The authentication is done on the blockchain, and each time the identity card owned by each node is verified to verify the validity of its identity. A malicious node cannot impersonate a legitimate node in the network to attack.

Message Substitution Attack. In this scenario, the registration request and authentication request of the ordinary node is sent to the blockchain through the proxy node. The message replacement attack can only occur in these two phases. If the attack occurs during the

registration phase, even if the submitted registration message is replaced by an illegal node, it is impossible to complete the registration; if the attack occurs in the authentication phase, the message can be replaced only when the authentication request is submitted, because the other operations are performed by the blockchain. Completed, and the authentication request message is replaced and cannot be authenticated.

Message Replay Attack. Message records in the blockchain are timestamped, and message replay attacks cannot occur on the blockchain. The attack may only occur when an ordinary node submits a registration request and an authentication request to the proxy node, and both of them are timestamped at the time of submission, and a message replay attack cannot occur.

Man-in-the-middle Attack. Assumes that the third-party attack node conducts a man-in-the-middle attack by intercepting the message in the execution process, and in this process, the message is signed for an integrity check, and the attacker cannot intercept the message between the ordinary node and the proxy node. Tampering with the message to achieve the purpose of the attack.

Denial of Service Attack. Because the global blockchain and the local blockchain in the hybrid blockchain model proposed in this paper are alliance chains, illegal nodes cannot join the blockchain, and this part cannot launch denial of service attacks. After the ordinary node submits the registration and authentication request to the proxy node, the first thing the proxy node does is to judge its trust value. The node with low trust value is untrusted and is shielded, which greatly reduces the possibility of denial of service attack.

Compared with the existing node management and authentication methods for the IoT, it can defend against several common attack methods and has higher security than other solutions.

5.2 Efficiency Analysis

5.2.1 Experiment setup

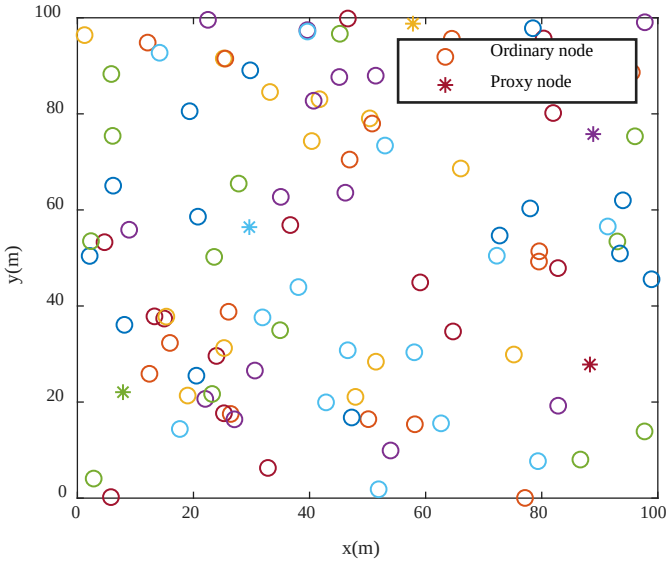


Fig. 6. Node distribution

In this section, simulation experiments are carried out to verify the effectiveness of the proposed method. The simulation experiment is carried out on the MATLAB simulation platform. As shown in **Fig. 6**, the experiment assumes that 100 ordinary nodes and 5 proxy

nodes are randomly deployed in the monitoring area of 100m x 100m, including 10 malicious ordinary nodes and 1 malicious proxy node. Other parameters related to the experiment are set as **Table 2**.

Table 2. Parameter setting

Simulation parameters	Values
α (The weight of indirect trust)	0.3
β (The weight of direct trust)	0.7
γ (The weight of history trust)	0.3
λ (The weight of current trust)	0.7

5.2.2 The validity of proxy node selection mechanism

During the experiment, the ordinary nodes are randomly selected, and the proxy nodes are selected according to the above scheme to submit the authentication request, and the relevant evaluation values are calculated every 100 times for verification.

(1) The trust value of the proxy node

In this section, to verify the validity of the scheme, the trust evaluation function described above is simplified, and the current trust value is calculated as follows:

$$f(T)=\begin{cases}1 & \text{if Authentication successful}\\ 0 & \text{if Authentication failed}\end{cases} \tag{4}$$

In fact, a complete trust calculation function can better reflect the trust level of normal and malicious nodes. This section only needs to verify the validity of the selection mechanism, so it simplifies the function. The average trust values of all normal nodes to the five selected proxy nodes are compared experimentally, and the results are shown in the following **Fig. 7**. From the diagram, it can be seen that the trust values of all proxy nodes tend to converge after a certain number of authentication times, and the trust values of four normal proxy nodes are significantly higher than those of malicious proxy nodes, indicating that malicious proxy nodes can be effectively identified by trust calculation.

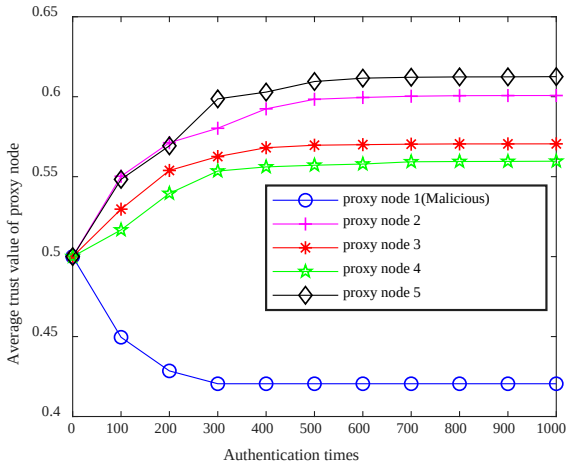


Fig. 7. The trust value of the proxy node

(2) The successful submission rate

The proxy node selection mechanism can effectively avoid submitting authentication requests to malicious proxy nodes. To verify the effectiveness of this method, the successful submission rate under this mechanism and without this mechanism is calculated as follows:

$$successful\_rate = \frac{sub\_time - failed\_time}{sub\_time} \tag{5}$$

Where sub_time is the total number of authentication submissions and $failed\_time$ is the number of requests submitted to malicious nodes that were not correctly submitted to the blockchain for authentication.

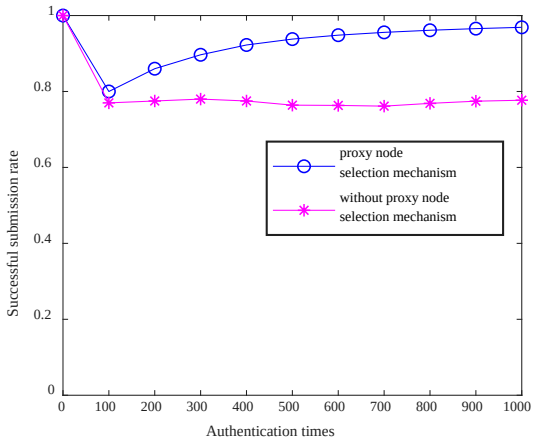


Fig. 8. The successful submission rate

The experiment compared the successful submission rate when using the proxy node selection mechanism with that when not using it. The experimental results in **Fig. 8.** It shows that, when using proxy node selection mechanism, the successful submission rate gradually increases to 100% after 100 authentications, which is due to the mechanism used by ordinary nodes to shield malicious proxy nodes in the network; when not using this mechanism, the successful submission rate is stable at 80%. This is consistent with the proportion of normal proxy nodes in all proxy nodes. The comparison shows that the proxy node selection mechanism can effectively improve the probability of ordinary nodes submitting authentication requests to normal proxy nodes, and proves the effectiveness of the mechanism.

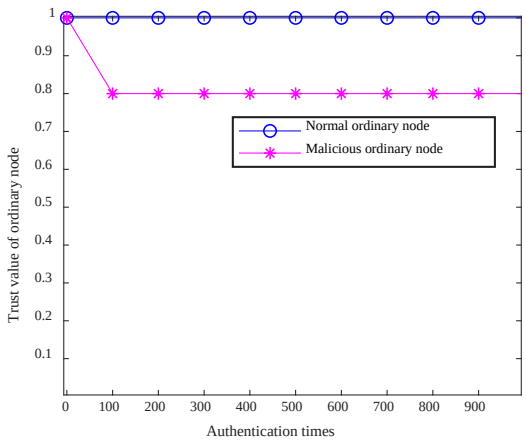


Fig. 9. The trust value of the ordinary node

(3) The trust value of the ordinary node

In order to identify malicious ordinary nodes in the network, we calculate the trust value of ordinary nodes. We set the initial trust value of the normal node to 1 and adjust the trust value through the authentication results. In the simulation experiment, a normal node and a malicious normal node are selected, and their trust values are compared. The results are shown in **Fig. 9**. It can be seen that the trust values of the normal ordinary node is maintained at 1. This indicates that no malicious behaviour occurs in the normal node during the authentication process, and the malicious ordinary node will converge after a certain number of times. This is related to the threshold value set when the proxy node filters the authentication request of the ordinary node. In this paper, 0.8 is selected, so the trust value of malicious ordinary nodes will not change around 0.8.

(4) The successful intercept rate

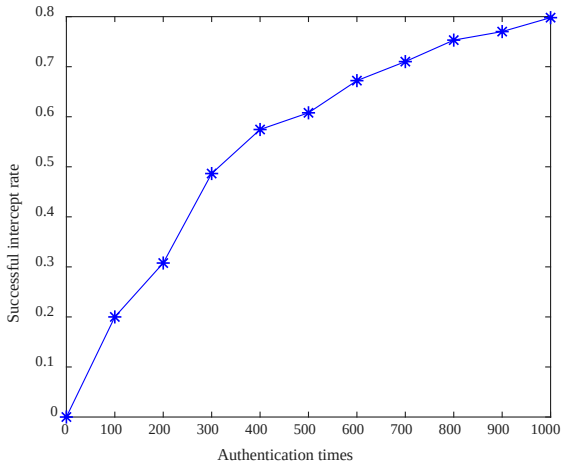


Fig. 10. The successful intercept rate

It can improve the efficiency of node authentication to identify the malicious ordinary nodes in the network and effectively intercept the malicious requests submitted by them. To verify the efficiency of this scheme, we calculate the interception rate of malicious requests, which is calculated as follows:

$$intercpt\_rate = \frac{intercept\_time}{malice\_time} \tag{6}$$

Where $malice\_time$ is the total number of authentication requests submitted by malicious ordinary nodes and $intercept\_time$ is the number of malicious authentication requests effectively intercepted by proxy nodes.

The malicious request interception rate obtained in the simulation experiment is as shown in **Fig. 10**. From the experimental results, it can be seen that with the increase of authentication times, the malicious request interception rate is gradually increasing, which shows that the proxy node selection mechanism in this paper can effectively identify the malicious ordinary nodes in the network and intercept them in time to improve the efficiency of node authentication.

5.2.3 Energy consumption analysis

In this paper, the nodes are divided according to the capacity, so the stable proxy nodes are not considered. In this section, only the energy consumption of common nodes is discussed. In the registration stage, since the energy consumption of the registration application only needs to be submitted once, compared with the whole life cycle of the node, this section only considers the energy consumption of ordinary nodes in the authentication process. The energy consumption of nodes mainly occurs in communication consumption. In this scheme, the ordinary nodes only request the trust value more than when they do not use the proxy node selection mechanism in the authentication process. Compared with the authentication request message, the trust value request message is concise, and the energy consumption is also less. So the energy consumption of common nodes will not increase too much.

5.2.4 Storage consumption analysis

In this scheme, after adding the proxy node selection mechanism, the common node only needs to store the trust value of the proxy node in the local network in this node, which is negligible compared with other required storage information.

6. Conclusions

This paper combines the security mechanism based on trust management and the security mechanism based on cryptography in the IoT and uses the blockchain technology to propose the authentication scheme of heterogeneous nodes. Firstly, a hybrid blockchain model is proposed for the IoT model to make the integration more reasonable; secondly, based on the trust model, a selection mechanism of proxy node and ordinary device node is proposed to improve the reliability of nodes in the early stage of authentication and reduce unnecessary consumption; Then, a corresponding block packaging mechanism is proposed for request messages with different delay requirements, Finally, based on the former three, the authentication scheme between nodes is proposed. The analysis of security and performance shows that the scheme proposed in this paper has better security performance and efficiency.

Acknowledgement

This paper is supported by Beijing Intelligent Logistics System Collaborative Innovation Center open topic (No. BILSCIC-2019KF-21), Youth Fund Project of Beijing Wuzi University (No. 2018XJQN03, 2020XJQN02), Major Project of Beijing Wuzi University (No. 2019XJZD11), General Program of Science and Technology Development Project of Beijing Municipal Education Commission of China (No. KM202110037001), Grass-roots Academic Team Building Project of Beijing Wuzi University (No. 2019XJJCTD04), Beijing Youth Top-notch Talent Plan of High-Creation Plan (No. 2017000026833ZK25), Canal Plan-Leading Talent Project of Beijing Tongzhou District (No. YHLB2017038), National Natural Science Foundation of China (No. 61803035, 71831001).

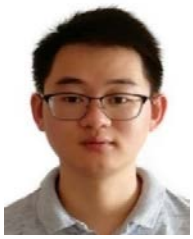
References

[1] J. Gubbi, R. Buyya, S. Marusic and M. Palaniswami, “Internet of Things (IoT): A vision, architectural elements, and future directions,” *Future Generation Computer Systems*, vol. 29, no. 7, pp. 1645-1660, 2013. Article (CrossRef Link)

[2] P. Gope, T. Hwang, "A Realistic Lightweight Anonymous Authentication Protocol for Securing Real-time Application Data Access in Wireless Sensor Networks," *IEEE Transactions on Industrial Electronics*, vol. 63, no. 11, pp. 7124-7132, 2016. Article (CrossRef Link)
[3] M. G. Masciotta, A. Barontini, L. I. S. F. Ramos, P. A. Mendes and P. B. L. C. O, "An overview on structural health monitoring: from the current state-of-the-art to new bio-inspired sensing paradigms," *International Journal of Bio-Inspired Computation*, vol. 14, no. 1, pp. 1-26, 2019. Article (CrossRef Link)
[4] S. Kumari, H. Om, "Authentication Protocol for Wireless Sensor Networks Applications like Safety Monitoring in Coal Mines," *Computer Networks*, vol. 104, pp. 137-154, 2016. Article (CrossRef Link)
[5] Y. Jeong, J. H. Park, "IoT and Smart City Technology: Challenges, Opportunities, and Solutions," *Journal of Information Processing Systems*, vol. 15, no. 2, pp. 233-238, 2019. Article (CrossRef Link)
[6] M. Tao, J. Zuo, Z. Liu, A. Castiglione and F. Palmieri, "Multi-layer cloud architectural model and ontology-based security service framework for IoT-based smart homes," *Future Generation Computer Systems*, vol. 78, pp. 1040-1051, 2018. Article (CrossRef Link)
[7] T. Mekki, I. Jabri, A. Rachedi and M. B. Jemaa, "Vehicular cloud networking: evolutionary game with reinforcement learning-based access approach," *Int. J. Bio-Inspired Computation*,13, 45-58, 2019. Article (CrossRef Link)
[8] E. P. K. Gilbert, B. Kaliaperumal, E. B. Rajsingh, M. Lydia and A. I. Selvakumar, "Trust aware nature inspired optimized routing in clustered wireless sensor networks," *International Journal of Bio-Inspired Computation*, vol. 14, no. 2, pp. 103-113, 2019. Article (CrossRef Link)
[9] X. Cai, P. Wang, L. Du, Z. Cui, W. Zhang and J. Chen, "Multi-Objective Three-Dimensional DV-Hop Localization Algorithm With NSGA-II," *IEEE Sensors Journal*, vol. 19, no. 21, pp. 10003-100015, 2019. Article (CrossRef Link)
[10] Z. Cui, X. Xu, F. Xue, X. Cai and J. Chen, "Personalized Recommendation System based on Collaborative Filtering for IoT Scenarios," *IEEE Transactions on Services Computing*, vol. 13, no. 4, pp. 685-695, 2020. Article (CrossRef Link)
[11] S. Asghari, N. J. Navimipour, "Cloud service composition using an inverted ant colony optimization algorithm," *International Journal of Bio-Inspired Computation*, vol. 13, no. 4, pp. 257-268, 2019. Article (CrossRef Link)
[12] P. Wang, J. Huang, Z. Cui, L. Xie and J. Chen, "A Gaussian error correction multi-objective positioning model with NSGA-II," *Concurrency and Computation: Practice and Experience*, vol. 32, no. 5, pp. e5464, 2020. Article (CrossRef Link)
[13] S. Hati, D. De and A. Mukherjee, "Bio-inspired innovative green fault recovery modelling for macro-femtocell mobile network," *International Journal of Bio-Inspired Computation*, vol. 14, no. 3, pp. 181-189, 2019. Article (CrossRef Link)
[14] O. Alfandi, A. Bochem, A. Kellner and D. Hogrefe, "Improving energy efficiency of data communication in a hybrid PKI-based approach for WSNs," in *Proc. of 2013 IEEE 10th Consumer Communications and Networking Conference (CCNC)*, 2013. Article (CrossRef Link)
[15] B. Kadri, M. Feham and A. M Hamed, "Lightweight PKI for WSN µPKI," *The Journal of Security and Communication Networks*, vol. 10, no. 2, pp. 135-141, 2010. Article (CrossRef Link)
[16] M. Prasad, R. Manoharan, "A secure certificate based authentication to reduce overhead for heterogeneous wireless network," in *Proc. of International Conference on Advanced Computing & Communication Systems*, 2017. Article (CrossRef Link)
[17] Q. Nong, "Practical Secure Certificateless Cryptographic Protocol with Batch Verification for Intelligent Robot Authentication," in *Proc. of International Conference on Mechatronics and Intelligent Robotics*, pp. 483-488, 2018. Article (CrossRef Link)
[18] M. A. Khan, K. Salah, "IoT security: Review, blockchain solutions, and open challenges," *Future Generation Computer Systems*, vol. 82, pp. 395-411, 2018. Article (CrossRef Link)
[19] Z. Bao, W. Shi, D. He and K. R. Chood, "Iotchain: A three-tier blockchain-based iot security architecture," *arXiv preprint arXiv:1806.02008*, 2018. Article (CrossRef Link)

[20] Novo, Oscar, "Blockchain Meets IoT: an Architecture for Scalable Access Management in IoT," *IEEE Internet of Things Journal*, vol. 5, no. 2, pp. 1184-1195, 2018. Article (CrossRef Link)
[21] P. K. Sharma, S. Singh, Y. Jeong and J. H. Park, "Distblocknet: A distributed blockchains-based secure sdn architecture for iot networks," *IEEE Communications Magazine*, vol. 55, no. 9, pp. 78-85, 2017. Article (CrossRef Link)
[22] M. T. Hammi, B. Hammi, P. Bellot and A. Serhrouchni, "Bubbles of Trust: A decentralized blockchain-based authentication system for IoT," *Computers & Security*, vol. 78, pp. 126-142, 2018. Article (CrossRef Link)
[23] R. Almadhoun, M. Kadadha, M. Alhemeiri, M. Alshehhi and K. Salah, "A user authentication scheme of iot devices using blockchain-enabled fog nodes," in *Proc. of 2018 IEEE/ACS 15th International Conference on Computer Systems and Applications (AICCSA)*, 2018. Article (CrossRef Link)
[24] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008. Article (CrossRef Link)
[25] M. El Ghazouani, M. A. El Kiram and L. Er-Rajy, "Blockchain & Multi-Agent System: A New Promising Approach for Cloud Data Integrity Auditing with Deduplication," *International Journal of Communication Networks and Information Security*, vol. 11, no. 1, pp. 175-184, 2019. Article (CrossRef Link)
[26] X. Yue, H. Wang, D. Jin, M. Li and W. Jiang, "Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control," *Journal of medical systems*, vol. 40, no. 10, pp. 218, 2016. Article (CrossRef Link)
[27] M. U. Hassan, M. H. Rehmani and J. Chen, "Privacy preservation in blockchain based IoT systems: Integration issues, prospects, challenges, and future research directions," *Future Generation Computer Systems*, vol. 97, pp. 512-529, 2019. Article (CrossRef Link)
[28] W. Dai, C. Dai, K. R. Choo, C. Cui, D. Zou and H. Jin, "SDTE: A secure blockchain-based data trading ecosystem," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 725-737, 2019.
[29] M. Polina, O. Lucy, Y. Yury, O. Alex, B. Alex, P. Pavel, I. Eugene, A. Alexander, R. Konstantin and Z. Alexander, "Converging blockchain and next-generation artificial intelligence technologies to decentralize and accelerate biomedical research and healthcare," *Oncotarget*, vol. 9, no. 5, pp. 5665-5690, 2018. Article (CrossRef Link)
[30] J. Shi, S. Chengchao, H. Lei and X. Mengxi, "Smart grid short-term load estimation model based on BP neural network," *International Journal of Computing Science and Mathematics*, vol. 11, no. 2, pp. 123-136, 2020. Article (CrossRef Link)
[31] Z. Shen, Y. Niu, Y. Zuo, Q. Xie and Z. Chen, "Power control of wind energy conversion system under multiple operating regimes with deep residual recurrent neural network: theory and experiment," *International Journal of Computing Science and Mathematics*, vol. 10, no. 4, pp. 413-428, 2019. Article (CrossRef Link)
[32] X. Cai, Y. Niu, S. Geng, J. Zhang, Z. Cui, J. Li and J. Chen, "An under-sampled software defect prediction method based on hybrid multi-objective cuckoo search," *Concurrency and Computation: Practice and Experience*, vol. 32, no. 5, pp. e5478, 2020. Article (CrossRef Link)
[33] W. H. Bangyal, J. Ahmed and H. T. Rauf, "A modified bat algorithm with torus walk for solving global optimization problems," *International Journal of Bio-Inspired Computation*, vol. 15, no. 1, pp. 1-13, 2020. Article (CrossRef Link)
[34] K. G. Dhal, S. Das, "Local search-based dynamically adapted bat algorithm in image enhancement domain," *International Journal of Computing Science and Mathematics*, vol. 11, no. 1, pp. 1-28, 2020. Article (CrossRef Link)
[35] S. Sharma, "Respondents view of novel framework for data protection in social networking sites: an analysis," *International Journal of Computing Science and Mathematics*, vol. 10, no. 1, pp. 22-31, 2019. Article (CrossRef Link)
[36] Y. Lu, X. Huang, Y. Dai, S. Maharjan and Y. Zhang, "Blockchain and Federated Learning for Privacy-Preserved Data Sharing in Industrial IoT," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 6, pp. 4177-4186, 2020. Article (CrossRef Link)

[37] Z. Cui, L. Du, P. Wang, X. Cai and W. Zhang, "Malicious code detection based on CNNs and multi-objective algorithm," *Journal of Parallel and Distributed Computing*, vol. 129, pp. 50-58, 2019. Article (CrossRef Link)
[38] Z. Cui, F. Xue, S. Zhang, X. Cai and J. Chen, "A Hybrid BlockChain-Based Identity Authentication Scheme for Multi-WSN," *IEEE Transactions on Services Computing*, vol. 13, no. 2, pp. 241-251, 2020. Article (CrossRef Link)



Shiqiang Zhang is a Ph.D. candidate of Faculty of Information Technology, Beijing University of Technology, China. He received his B.S. degree in Computer Science and Technology from Beijing University of Chemical Technology, China, in 2012. His current research interests include trusted computing, Internet of Things security, blockchain.

Yang Cao is a Lecturer at the School of Information, Beijing Wuzi University. He received the Ph.D. degree in Computer Science and Technology from Beijing University of Technology, China, in 2019. His current research interests are in the field of Internet of Things security, machine learning and big data analysis.

Zhenhu Ning is a Lecturer at the Faculty of Information Technology, Beijing University of Technology. He received the Ph.D. degree in Computer Science and Technology from Beijing University of Technology, China, in 2016. His current research interests include IOT security, cloud security, malicious code detection, machine learning, system optimization and control, and practical partial differential equations.

Fei Xue is a Lecturer at the School of Information, Beijing Wuzi University. He received the Ph.D. degree in Computer Science and Technology from Beijing University of Technology, China, in 2016. His current research interests are in the field of swarm intelligence optimization, deep learning and network security.

Dongzhi Cao is a Ph.D. candidate of Faculty of Information Technology, Beijing University of Technology, China. She received her M.S. degree in Computer Technology from Beijing University of Technology, China, in 2020. Her current research interests include trusted computing, malicious code detection, neural networks.

Yongli Yang is a Ph.D. candidate of Faculty of Information Technology, Beijing University of Technology, China. She received her M.S. degree in Computer Technology from Beijing University of Technology, China, in 2018. Her research interests include recommendation systems, machine learning, swarm intelligence, and quantum encryption.