ISSN: 2664-9640

Research on Data Analysis Model of Nodes Behavior in Industrial IoT Based on Blockchain

Ting Li[1,a],Qiao Zhou[1]

[1]School of Chongqing University of Posts and Telecommunications,
Chong Qin 400065,China.
[a]358530525@qq.com

Abstract

The increasingly widespread use of the Industrial Internet of Things, while bringing industrial production efficiency and intelligent decision-making, is facing severe information security risks, which may cause industrial equipment to malfunction, and even wrong instructions leading to damage to product quality. Blockchain is a distributed database that connects blocks containing data in a chronological order with a chain structure and uses cryptographic algorithms to ensure that it cannot be changed or forged. The industrial Internet of Things system using blockchain technology records the data recognized by most nodes in a distributed database through the participation consensus of multiple nodes, which can effectively prevent the industrial Internet of Things data from being tampered with. The malicious node detection model of the chain provides a new idea for traditional malicious node detection.

Keywords

Blockchain, Industrial Internet of Things, Malicious node detection.

1. Introduction

In recent years, the concept of the Industrial Internet of Things has gradually risen, and it may become one of the backbones of national economic and social development in the future. The Industrial Internet of Things is the continuous integration of nodes with sensing and control capabilities and ubiquitous technology, mobile communications, intelligent analysis and data processing technologies into all aspects of industrial production, which can greatly improve the productivity of industrial processes and change industrial production. Quality is an important step in achieving a smart factory.

As a key part of the Industrial Internet of Things, wireless sensor networks have important research value. Wireless sensor network[1] is a mobile ad hoc network composed of many micro sensor nodes. It has the characteristics of wide coverage area, high-precision monitoring, remote monitoring, rapid deployment, self-organization, and high fault tolerance. Because the environmental conditions of wireless sensor deployment are relatively complex and the number of nodes is large, they are vulnerable to attacks by malicious nodes. Wireless sensor networks currently face two main attacks[2], one is the attack from external attackers on the network, and the other is the attack on internal normal nodes after the internal nodes are controlled by malicious nodes. Therefore, identifying and processing internal malicious nodes in time has important practical significance for the security of the Industrial Internet of Things.

A large number of researches on malicious node detection in wireless sensor networks have been done at home and abroad. Hu Linglong [3] proposed a combined weighted K nearest neighbor method for malicious node detection, which will collect the data set and randomly generate a subset of attributes. Run weighted K-nearest neighbor classifiers on each training subset; combine multiple weighted k-nearest neighbor classifier results by simple voting and output. Song Sanhua [4] proposed a malicious node detection algorithm RDICS based on reliable metrics, which reduces the fusion weight of malicious nodes, thereby weakening their contribution to the final decision. Wang Xin [5] et al. Proposed a wireless sensor network malicious node selection algorithm based on an adaptive metric threshold ruling mechanism. Data collection was performed through ordinary nodes, cluster head nodes, and convergent nodes to obtain the signal sampling sequence of the corresponding nodes. Calculate the adaptive metric threshold of any node according to the sampling sequence, and use this threshold to determine whether a node behaves abnormally. Hu Xiangdong et al. [6] designed a malicious node detection mechanism that combines reputation assessment and inspection mechanisms. By establishing a node reputation assessment model and innovatively proposing an inspection mechanism to randomly detect node communication behavior, it exponentially magnifies the node anomalies. Behavior with higher detection rate.

Blockchain technology, as a new technology, has the characteristics of decentralization, tamper resistance, and traceability. The unique smart contract of the blockchain can be distributed on each node in a distributed manner. Once it meets a certain definition of the smart contract These conditions can automatically execute the code deployed on the contract. These characteristics unique to the blockchain provide a new direction for malicious node detection in wireless sensor networks. Qi Liu et al. [7] proposed a blockchain-based malicious sensor detection model for wireless sensor networks. By integrating reputation evaluation mechanisms and smart contracts, malicious node detection in three dimensions was achieved, and the voting consensus results were recorded in the district. Blockchain. Linghe Kong [8] and others designed a credit-based proof-of-work (POW) proof mechanism based on a directed acyclic graph (DAG) blockchain and implemented the system on the Raspberry Pi and the host. Yinqiu Liu [9] and others based on the power-constrained IIOT scenario, proposed a green consensus mechanism called collaborative multiple proofs to promote cooperation between IIOT devices, and proposed a lightweight block data structure To simplify broadcast content. Wang Shu [10] and others proposed a random block chain-based IoT data integrity protection mechanism. Shared IoT data will be forwarded by a random number and randomly selected cooperative nodes. Blocks are manufactured by IoT edge nodes. Achieved high defense rates in large-scale IoT systems.

ISSN: 2664-9640

2. Blockchain-based malicious node detection and tracking model for the Industrial Internet of Things

2.1 Model structure

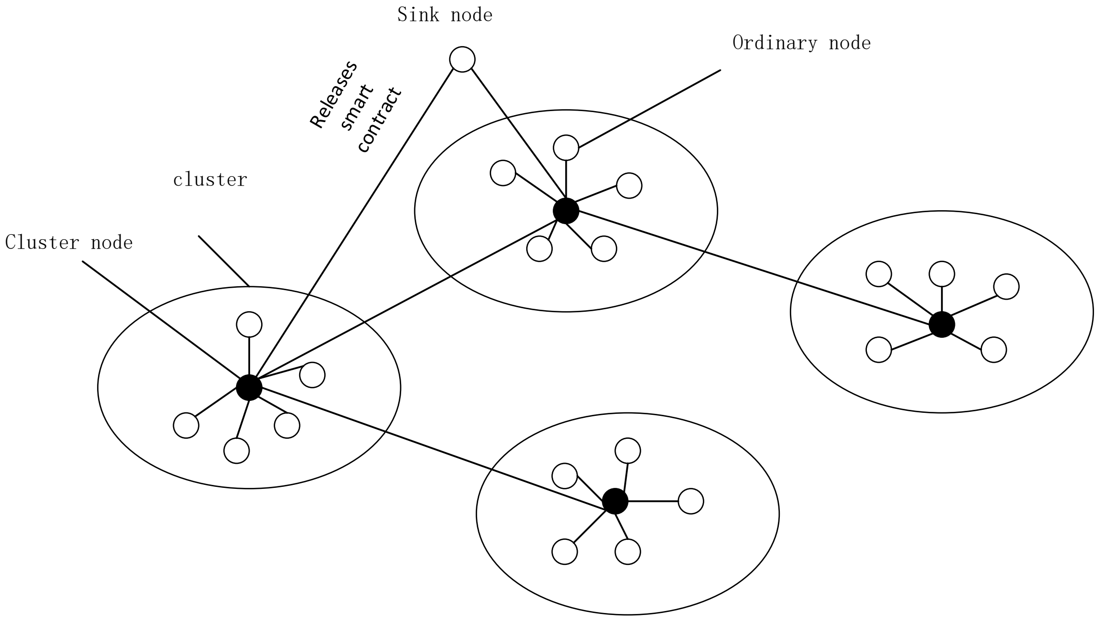

Figure 1: Wireless sensor network and some node functions

Based on the characteristics of the current wireless sensor network layered into clusters, we consider mapping the blockchain model to the wireless sensor network. The aggregation node plays the role of issuing smart contracts. The cluster head node plays the role of maintaining the blockchain, and the ordinary node plays the role. Verify the role of the transaction.

Program steps:

1. The wireless sensor network is layered into clusters through the LEACH protocol, and the node roles are divided into sink nodes, cluster head nodes, and ordinary nodes.

2. Ordinary nodes supervise each other's behavior, and cluster head nodes supervise each other's behavior in both directions. In detail, the three indicators (transmission delay, forwarding rate, and packet loss rate) are monitored to comprehensively judge whether the communication of the node is abnormal, and whether the node is an abnormal node according to the Beta distribution. The network publishes the malicious node ID and publishes the node ID and its credit to the blockchain network as a transaction. All network nodes are prohibited from communicating with it.

If it is determined that the cluster head node is a malicious node, after removing the node from the network, the ordinary node managed by the node selects the nearest cluster head node to join its management domain.

In particular, considering the energy consumption of wireless sensor network nodes in the Industrial Internet of Things, this model takes the residual energy of the cluster head node as an important basis for whether or not it can be selected as a block node. Specifically, the residual energy of the cluster head node is changed from large to large. Sort them, list the remaining energy of the cluster head nodes, and randomly select one of the top three cluster head nodes as the block generating node for the current round. In order to give the cluster head node that has not been selected the accounting node an opportunity to specify the selected accounting The cluster head node of the node cannot be elected as the accounting node in the next three rounds.

2.2. Define malicious node evaluation indicators

Wireless sensor networks are usually deployed on a large scale, and there are many evaluation indicators for each sensor node. Here we choose the following indicators:
(1) Forwarding rate

$$R_f = {}^{P_f}\!/\!_{P_t} \tag{1}$$

In formula (1), R_f is the forwarding rate of the node, P_f is the number of data packets successfully forwarded by the current node, and P_t is the total number of data packets received by the current node. In wormhole and black hole attacks, malicious nodes deliberately do not forward or discard received packets.
(2) Transmission delay

$$DT = {}^{T_{sensor}}\!/\!_{T} \tag{2}$$

In formula (2), DT represents the processing delay of the node, T_{sensor} is the time it takes for the data packet to be received from the time it is transmitted, and T is a certain time interval.
(3) Packet loss rate

$$R_s = 1 - {}^{P_s}\!/\!_{P_a} \tag{3}$$

In formula (3), R_s represents the packet loss rate of the node, P_s represents the sum of the data packets successfully received by the node, and P_a represents the data packets sent by the neighboring node to the node.
definition:

$$Q = \alpha * R_f + \beta * DT + \delta * R_s \tag{4}$$

In formula (4), Q is the communication quality, α 、 β 、 δ are the weights of related indicators, which can be set according to the specific scenario of the Industrial Internet of Things. Set a threshold ω , if $\eta < \omega$, Then the current node communication is considered successful and the number of successful actions C_s plus one, Otherwise, the current node communication is considered abnormal C_f plus one, Finally, calculate the node's credit based on the Beta distribution $\eta = \frac{C_s}{C_s + C_f + 1}$, Setting a credit threshold ∂ ,if $\eta \leq \partial$, The node is considered a malicious node.

2.3. Block Design Based on Industrial Internet of Things

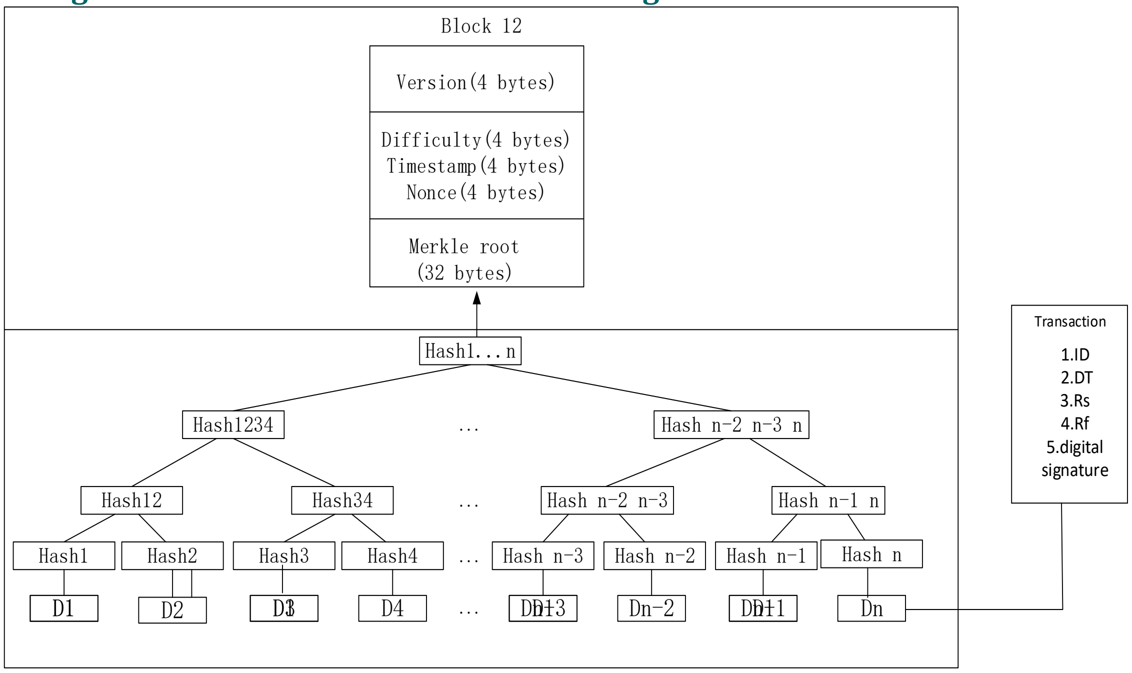

Figure 2: Block design diagram based on Industrial Internet of Things

Figure 2 is a block design diagram based on the Industrial Internet of Things. By collecting data packets issued by ordinary nodes and cluster head nodes, and storing the data packets in the block body, the Merkel tree formed by the data packets can guarantee the data packets. Real and immutable, Merkel root is stored in the block header, ensuring the security of the entire blockchain data. In addition, the block header also contains the version of the block, the difficulty value of the block, the block timestamp, and a random number. The difficulty value and random number can ensure the validity and legality of the block and protect the rights and interests of the miners. The time stamp within the block generation interval guarantees the continuous time of the blockchain.

The verification of the block includes the following steps:

1) Check whether the block ID is legal, that is, the block IDs are arranged in order from the beginning to the end;

2) Check whether the hash summary of the previous block in the block header is the same as the hash value of the previous block;

3) Check whether the timestamp is valid, that is, the current UNIX timestamp of the blockchain must be strictly greater than the median of the first n timestamps.

2.4. Confidential design of data communication

The RSA algorithm is an algorithm based on the large integer factorization problem. With the improvement of computer performance, the RSA algorithm must use a key with a large key length, which leads to an increase in the complexity of the algorithm, which greatly increases Algorithm runtime. Ecc is based on the discrete logarithm problem on the elliptic curve. It is generally believed that the difficulty of solving this problem is much greater than the difficulty of large integer factorization, so that under the same conditions, the ECC key length is shorter. Based on this feature, this model selects Ecc (Elliptic Curve Cryptography) as the data transmission encryption algorithm and signature algorithm, which can better ensure the security and belonging of data during transmission.

3.Conclusion

1) Model security analysis

This model adopts the distributed communication method of the blockchain, and uses the non-tamperable characteristics of the blockchain to ensure that the industrial Internet of Things data cannot be tampered with. The elliptic curve encryption algorithm is added to the node communication process to ensure the security of the node communication. The smart contract is used. Can automatically analyze node data and determine malicious nodes, and remove malicious nodes from the network.

2) Traceability analysis

Due to the unique chain structure of the blockchain and the data stored in the block cannot be tampered with, the malicious time and malicious information of the malicious node can be queried transparently, real-time update of the data record is realized, and the traditional WSN detects malicious Defects that are difficult to reproduce in the node process better protect the security of the Industrial Internet of Things.

References

[1] Pakzad S N, Fenves G L,Kim S,et al: Design and implementation of scalable wireless sensor network for structural monitoring,Journal of Infrastructure Systems,14(2008) No.1, p.89.

[2] Akkaya K, Younis M: A survey on routing protocols for wireless sensor networks,Ad Hoc Networks,3(2005) No.3, p.325.

[3] Hu Linglong, Pan Julong, Cui Hui: Reputation-based malicious node detection in wireless sensor networks,Journal of China Jiliang University,23(2012) No.01, p.41.

[4] Song Sanhua: Malicious node detection algorithm for wireless sensor networks based on reliability measurement,China Test,44(2018) No.07, p.148.

[5] Wang Xin, Hu Ping, Jing Bo: WSN Malicious Node Selection Algorithm Based on Metric Threshold Decision,Computer Engineering and Design,38(2017) No.05, p.1142.

[6] Hu Xiangdong, Xing Quanquan, He Wenxiang: Energy-efficient and secure clustering algorithm for WSN integrating reputation evaluation and inspection mechanism,Telecommunication Engineering,59(2019) No.02, p.125.

[7] Liu Qi: Blockchain Trust Model for Malicious Node Detection in Wireless Sensor Networks, IEEE Access,7(2019) No.5, p.2169.

[8] Junqin Huang: Towards Secure Industrial IoT: Blockchain System With Credit-Based Consensus Mechanism,IEEE Transactions on Industrial Informatics,15(2019), No.6, p.3680.

[9] Sujit Biswas: PoBT: A Light Weight Consensus Algorithm for Scalable IoT Business Blockchain,IEEE Internet of Things Journal,18(2019) No.8, p.2561.

[10] Yu-Jia Chen: Stochastic Blockchain for IoT Data Integrity,IEEE Transactions on Network Science and Engineering,21(2019) No.2, p.3620.