Research on Clustering Management of Power Distribution Internet of Things Based on Trusted Blockchain

Yue Sun*, Wei Chen, Leran Chen, Min Li
State Grid Jibei Electric Power Co. Ltd. Research Institute, North China Electric Power Research Institute Co. Ltd., Beijing, China
*Corresponding author: Yue Sun e-mail: sun.yue.d@jibei.sgcc.com.cn

Abstract. Since the topological structure of power distribution Internet of Things is getting more and more complicated, and the amount of new services, such as remote dynamic monitoring and two-way real-time interaction, has been increasing, it is urgent and necessary to study the clustering management technology of power distribution Internet of Things combined with its running scenarios, security requirements and dynamic access characteristics. In this paper, a clustering security management scheme of power distribution Internet of Things based on trusted blockchain is proposed. The clustering management and data communication of power distribution Internet of Things are conducted based on trusted blockchain, which can improve the security of data interaction.

1. Introduction
With the increasing development of smart grid and Energy Internet, the traditional distribution network has been gradually transformed into the active distribution network based on Internet of things [1]. The interaction of energy and information in distribution network has been extended to the user side, and the communication network is getting opener and more interactive. Due to the wide interconnection, high intelligence and open interaction of power distribution Internet of Things, its network access environment is more complicated and diverse. Since users are in an increasing need of the interaction with power distribution Internet of Things, there exist more and more potential illegal accesses, which also leads to the insecurity of communication. The existing routing mechanisms of distribution network can no longer meet the security requirements, such as dealing with massive information interaction, verifying data integrity, etc.

The clustering management of the nodes of Internet of things has always been a hot issue. The Low Energy Adaptive Clustering Hierarchy (LEACH) protocol proposed in Reference [2] adopts a cyclic random algorithm to select a cluster head node and distributes the energy load equally to each sensor node in order to reduce energy consumption and improve the life cycle of the whole network. What’s mentioned in Reference [3] is the improved LEACH algorithm based on selecting the cluster head node by the node residual energy, which can avoid nodes with low residual energy separating from the network because of too fast energy consumption. What’s mentioned in Reference [4] is a clustering routing protocol based on the improved particle swarm optimization. In this algorithm, the cluster head node is selected based on the energy factor and position factor while the optimal path for data multi-hop transmission is chosen based on the minimum spanning tree algorithm in order to increase lifetime of the network. In the Reference [5], a clustering optimization algorithm based on optimal transmission distance and K-means clustering is proposed. The hierarchical clustering algorithm is used to set up the cluster feature tree to optimize the communication distance within the cluster, and reduce and balance...
the energy consumption of the nodes. The existing clustering routing mechanism of IoT nodes does not fully consider the quality of service communication and the security of data interaction, and is not suitable for the high-speed data interaction of power distribution Internet of Things. It means there’s no suitable clustering control scheme for power distribution Internet of Things; Due to the low security of communication between the nodes of Internet of things, the communication and interaction of data may be easily invaded and attacked, and the data may be stolen or tampered.

In this paper, a clustering security management scheme and system of power distribution Internet of Things based on trusted blockchain is proposed. The trusted blockchain is used to cluster sensing terminals of power distribution Internet of Things so that the security of data transmission between connected devices can be ensured by trust verification. Moreover, the clustering method can improve the efficiency of data interaction in the Internet of Things.

2. Key Technologies

2.1. Trusted Computing Technology
Trusted computing [6] is an active immune computing mode, which can protect the security while computing. When the whole computing process can be measured and controlled, it can improve the traditional and passive network security protection (blocking and killing). The research on trusted computing platform [7], trusted cryptography module [8], trusted dynamic metrics [9], remote proof [10] and trusted chain construction [11] is carried out in various industries. Therefore, embedding trusted computing technology into industrial control systems and the Internet of Things can enhance the endogenous security capability of critical infrastructure.

2.2. Blockchain Technology [12]
As a distributed network data management technology, blockchain technology uses cryptography and distributed consensus algorithm to ensure the security of network data transmission and access control, achieve common maintenance and cross-validation of data, and make data difficult to be tampered with. Blockchain is similar to power distribution Internet of Things in operation mode, topological form, security protection, etc. So the application of blockchain is helpful to improve the security of data management and interaction.

2.3. Merkle Tree
Merkle Tree [13] looks like a binary tree so much, where the value of a leaf node is usually the Hash value of the data block rather than its original value. Merkle Tree first computes the Hash value of a leaf node and then merges the Hash values of the adjacent nodes. When the merge is completed, the Hash value of the current string will be calculated until the one of the root-node is done.

3. Clustering Management Scheme for Power Distribution IoT Based on Trusted Blockchain
In order to realize intelligent fault diagnosis and active isolation of distribution network, and shorten the time of power outage, it is necessary to improve the sense breadth and extend the control range of medium-voltage distribution network. Meanwhile, the enhancement of the perception depth and frequency of distribution stations is also needed to optimize the perception and connection between the grid and users, and realize the excavation of data and customer resource value. In a word, data security and safe operation of power distribution Internet of Things are crucial.

3.1. Equivalent Topology of Power Distribution IoT Based on Blockchain
Each terminal device in power distribution Internet of Things is equivalent to a blockchain node. According to the self-organization characteristics of power distribution Internet of things (IoT), the nodes in the network are clustered. The cluster head nodes are also selected and they’re used to control and manage the communication between the nodes in the cluster. Seen from functions, the gateway is equivalent to the first full node in a blockchain while a cluster head node is equivalent to the second full
node in a blockchain. And the other sensor nodes in the IoT network are equivalent to the light nodes in a blockchain. The first full nodes, second full nodes and light nodes are managed and controlled step by step. The identity authentication of the two nodes that are communicating directly should be conducted. Trusted authentication is used as the way of identity authentication, whose specific diagram can be shown as Fig. 1.

3.2. Scheme of the Switching of Cluster Head Nodes in PD-IoT (power distribution Internet of Things)  
To ensure the operation and management of autonomous and self-healing weak center of each node in the PD-IoT network, the consensus mechanism of blockchain is used to regularly replace a cluster head node in the cluster. It can also ensure that the performance of a cluster head node won’t be affected due to the overheating of the equipment, excessive energy consumption, etc.

It is agreed that: a cluster head node will be switched after working continuously for a fixed period of time $\Delta T$, which forms the consensus mechanism in blockchain. If the node failure rate of a cluster head node exceeds the set threshold (node failure rate = the number of times that a node fails to transmit information/the total number of the times a node has transmitted information) during the running process, the one will be replaced immediately and the running time will be recalculated. The flowchart is shown in Fig. 2:
Cluster head node works smoothly

Whether a cluster head node fails to work

NO

YES

Switch the cluster head node immediately

A cluster head node is switched after working continuously for a fixed period of time $\Delta T$

A new cluster head node sends a message to notice the gateway node

A new cluster head node notices other nodes in the cluster

Fig. 2 Flow Chart of the Switching of a Cluster Head Node

The total amount of data sent and received by each node, the Quality of Service (QoS) and the hash value of the sent data are all recorded in a blockchain. Among them, a cluster head node is selected according to the following indicators:

(1) Distance (expressed by $r$): when selecting a cluster head node, the distance between a cluster head node and the other nodes in the cluster should be considered so that the quality of communication won’t be affected due to communication delay, etc.

When there are $n$ nodes in a cluster, $r_k$ represents the distance factor of the $k$ node in the cluster while $r_{ik}$ represents the distance between Node $i$ node and the Node $k$.

$$r_k = \sum_{i=1,i\neq k}^{n} r_{ik}$$

(2) The total amount of data sent and received (expressed by $b$) : The total amount of data sent and received by each node within the time interval $\Delta T$ when one cluster head node is switched by another node is taken as an indicator for selecting a cluster head node. A node that receives and sends relatively less data in this time interval will be selected as a cluster head node.

(3) QoS (expressed by $q$): The key indicators of QoS mainly include: availability, throughput, delay, delay variation (including jitter and drift) and loss. A suitable cluster head node is selected based on the QoS data recorded in a blockchain.

$$p_k = f \left( r_k, b_k, \frac{q_k}{a} \right) \quad (a \text{ is constant})$$
\[ p_k = \frac{p_k}{\sum_{i=1}^{n} p_i} \]

\( p_k \) represents the probability that \( k \) is chosen as a cluster head node. Among them, \( r_k \), \( b_k \), and \( q_k \) represent the values of the node \( k \) in the cluster during the interval when a cluster head node is switched, which will also be recorded in a blockchain. \( p_k \) is negatively correlated with \( r_k \) and \( b_k \) but positively correlated with \( q_k \).

When a cluster head node is switched, the new cluster head node will send a message to notice the gateway node, and then it will notice the other nodes in the cluster through the blockchain. Moreover, it will also conduct trusted authentication with other cluster head nodes. After that, nodes in clusters can send data to their cluster head nodes and the information interaction can be done among cluster head nodes. The information transmitted by cluster head nodes will be transmitted to the gateway node after Hash calculation.

3.3. Trusted Transmission of Data Based on Blockchain

As one of the basic supporting technologies of blockchain, Hash algorithm maps strings of arbitrary length to fixed length ones. As shown in Fig.3, when Node A wants to send information to Cluster Head Node C: Step1: When Node A sends Data A and Hash A to Relay Node B, Relay Node B will compare the received Data A which has been calculated by Hash algorithm with the received Hash A. If the two values are the same, the data transmission is successful. Otherwise, the data transmission will be considered as a failure and Node A will be informed to send the data again. Step 2: When Relay Node B sends Data B to Cluster Head Node C simultaneously, a Merkle Tree containing Data B and the received Data A will be generated. And then, Data A, Data B and Hash AB of the Merkle Tree will be sent to Cluster Head Node C and it will conduct the same verification process mentioned in Step 1.

![Fig. 3 Secure Data Interaction between Nodes and Cluster Heads](image)

4. Conclusion

In this paper, clustering management and control technology of power distribution Internet of Things is studied to improve the efficiency and security of distribution network. When the mapping between nodes in power distribution Internet of Things and the blockchain topology is constructed, a clustering-head selection method suitable for weak centralization of power distribution Internet of Things is proposed. It can improve the efficiency and reliability of data transmission between nodes and totally ensure the efficient running of the whole system.
Acknowledgments
This project is supported by the Science and Technology Project of State Grid Jibei Electric Power Co. Ltd. (52018K190024).

References
[1] Zhang Yajian, Yang Ting, et al. Review and Prospect of Ubiquitous Power Internet of Things in Smart Distribution System [J]. Electric Power Construction, 2019, 40 (06): 1-12 (in Chinese).
[2] Heinzelman, W., Chandrakasan, A., et al. Energy Efficient Communication Protocol for Wireless Microsensor Networks. Proceedings of the 33rd Annual Hawaii International Conference on System Sciences, 2000:3005-3014.
[3] Heinzelman, W., Chandrakasan, A., et al. An Application-specific protocol architecture for wireless microsensor networks. IEEE Trans. Wirel. Commun 2002, 1, 660–670.
[4] Wu Xiaonian, Zhang Chuyun, et al. Clustering routing protocol based on improved PSO algorithm in WSN [J]. Journal of Communications, 2019, 40 (12): 114–123 (in Chinese).
[5] Li Daoquan, Zhang Yuxia, et al. Energy Consumption Balanced Clustering Algorithm for Wireless Sensor Network Based on Clustering Analysis [J]. Computer Engineering, 2019, 45 (10): 116–121 (in Chinese).
[6] Shen Changxiang, Zhang Dawei, et al. The Strategy of TC 3.0: A Revolutionary Evolution in Trusted Computing [J]. Strategic Study of CAE, 2016, 18 (06): 53-57 (in Chinese).
[7] Yao Rui, Zhao Manfei, Wang Ren, et al. Design and implementation of high speed trusted computing platform based on FPGA [J]. Computer Engineering and Design, 2019, 40 (08): 2151-2160 (in Chinese).
[8] Hu Jun, Diao zipeng. vTCM: a virtualized trusted cryptography module based on the virtualization of physical trusted computing environment [J]. Journal of Shandong University (Natural Science), 2019, 54 (07): 77-88 (in Chinese).
[9] Liu Ziwenn, Feng Dengguo. TPM-Based Dynamic Integrity Measurement Architecture [J]. Journal of Electronics & Information Technology, 2010, 32 (04): 875-879 (in Chinese).
[10] Tan Liang, Chen Ju. Remote Attestation Project of the Running Environment of the Trusted Terminal [J]. Journal of Software, 2014, 25 (06): 1273-1290 (in Chinese).
[11] Liu Chuanyi, Wang Guofeng, et al. Practical Construction and Audit for Trusted Cloud Execution Environment [J]. Chinese Journal of Computers, 2016, 39 (02): 339-350 (in Chinese).
[12] Shao Qifeng, Jin cheqing, et al. Blockchain: Architecture and Research Progress [J]. Chinese Journal of Computers, 2018, 41 (05): 969-988 (in Chinese).
[13] Huang gen, Zou Yibo, et al. Performance Analysis and Research of Merkle Trees with Blockchain [J]. Computer System Applications, 2020, 29 (09): 237-243 (in Chinese).