IIETA International Information and Engineering Technology Association
Advancing the World of Information and Engineering

European Journal of Electrical Engineering
Vol. 22, No. 2, April, 2020, pp. 105-110
Journal homepage: http://iieta.org/journals/ejee

Management and Security Analysis of Blockchain Shard Storage for Monitoring Data on the State of Smart Substations

Chenxi Jia*, Hongyuan Ding, Chuanjin Zhang, Xing Zhang

School of Intelligent Manufacturing, Jiangsu Vocational Institute of Architectural Technology, Xuzhou 221116, China

Corresponding Author Email: 10758@jsjzi.edu.cn

https://doi.org/10.18280/ejee.220203

Received: 10 October 2019
Accepted: 11 January 2020

Keywords:
smart substations, blockchain shard storage, security analysis, ubiquitous power Internet of Things (UPIoT)

ABSTRACT

The ubiquitous power Internet of Things (UPIoT) provides a crucial platform for energy reform. The key features of blockchain, namely, decentralization, openness, and transparency, are in line with the spirits of the UPIoT. By integrating blockchain and the UPIoT, this paper analyzes the security strategy of the state monitoring system (SMS) for smart substations, constructs a blockchain network for smart substations, and designs a shard storage and management for the proposed model. Unlike the existing plans, our plan shards the transaction data to be stored in the blockchain. The sharding both localizes the data storage system, and maintains the scalability of the security system. Security analysis shows that our plan keeps the information secure, reliable, and private, while reducing the storage occupation of each node. The research results promote the application of blockchain in smart substations.

1. INTRODUCTION

Blockchain is a decentralized and trustless technical solution that collectively maintains a reliable database. Decentralization, transparency, and traceability are three defining features of this solution. Blockchain is hailed as the fifth disruptive computing paradigm, after mainframe, personal computer (PC), the Internet, and mobile/social network [1-4].

Blockchain technology registers all the processes that require traceability in a confidential and distributed manner, facilitating information exchange between smart meters, production systems, and distribution systems. In this way, the subjects of the sensor network could build up mutual trust in information exchange.

The key features of blockchain, namely, decentralization, openness, and transparency, are in line with the spirits of ubiquitous power Internet of Things (UPIoT) [5-7]. The combination between blockchain and the UPIoT enables precise digital management of energy, and could be extended to various scenarios of the Internet of energy: tracking and authentication, distributed transaction microgrid, energy finance, asset and supply chain management, carbon credit transaction, green credit issuance, and electric vehicles [8-11].

For real-time management and control of equipment, smart substations under the UPIoT rely on a sensor network that can sense various external information, and identify, locate, track, and monitor equipment automatically, such as to trigger corresponding events. The current automation systems for smart substations mostly adopt the data interface model defined in the IEC61850 standard. The low energy adaptive clustering hierarchy (LEACH) is the common structure of these systems, because this architecture protects the data security in the security mechanism of wireless sensor network (WSN) and meets the performance required for the clustering algorithm [12].

Ferraro et al. [13] designed a low-cost secret sharing plan for sensor network: the basic building blocks were provided to establish secure communications, and the secret is shared by exchanging the keys of neighboring nodes. Jiang et al. [14] prepared several plans to protect the data aggregation, secret sharing, and information dissemination: the sensor splits the secret into sub-secrets, adds them to the message to be transmitted, and forwards the message to multiple disjoint paths. In the above plans, lots of information must be transmitted to create a key system, which is energy-consuming and inefficient.

In the context of the UPIoT, Kuo et al. [15] explored the application of blockchain in communication network of distribution system, and mentioned the science and technology program of Shenzhen Power Supply Bureau: "Blockchain-based access for ubiquitous services of communication network of distribution system". This is the first program in CHina that applies blockchain technology to the trusted access of the communication network of distribution system, shedding light on the implementation of blockchain in energy fields.

Blockchain technology still has many defects and vulnerabilities. For example, it is difficult to apply blockchain in the UPIoT scenarios with large data volume, due to the problem of data storage [16-25]. This paper firstly reviews the security strategy of the state monitoring system (SMS) for smart substations, and then constructs a blockchain network for smart substations based on secret sharing technology. Next, a shard storage and management plan was designed for the model. The performance and security of the proposed plan were analyzed in details. The results show that our plan boasts good security, high storage efficiency, low energy consumption, and good connectivity. The research results provide a reference for the promotion of blockchain to other UPIoT scenarios.

2. SECURITY STRATEGY OF SMART SUBSTATION SMS

Smart substations are important units of the substation system in smart grid. The WSNs of smart substations serve as supporting nodes of the UPIoT. The normal operation of smart substations requires efficient, reliable, and intelligent technologies to integrate multiple sensors, as well as acquire and fuse information from multiple sources.

The modern WSN technology should be fully utilized to monitor the state of each smart substation. The online monitoring functions include oil, gas, and partial discharge of transformers, dynamic features of circuit breaker, moisture content, mutual inductors, arrester insulation, and substation security. Table 1 lists the sensors on the acquisition layer of a smart substation.

The smart substation SMS differs greatly from the SMSs for power transmission equipment and data center in the UPIoT. In the smart substation SMS, the monitoring terminal is not easily contacted, and does not use wide area communication. Therefore, the site perimeters and communication layer could have a relatively low level of security protection. There is no need to guarantee network security by IoT techniques, such as gateway encryption authentication, border intrusion detection, border security monitoring, and transmission information security protection.

However, security measures should be taken at the sensing layer, due to the use of open radio waves. Four kinds of security mechanisms could be adopted, namely, access authentication, access control, source and integrity check, and data encryption, to contain network risks like the attempt to eavesdrop the state or relevant security information of the substation, accessing the network and sending wrong information in disguise of legitimate nodes, and the denial of service attack.

Table 1. The sensors on the acquisition layer of a smart substation

Test items	Sensor deployment	Monitoring information
Power cabinet for station (substation)	Power cabinet	Main incoming line voltage, Current, Power, Power factor; Switch working state
Temperature detection	Secondary chamber of acquisition protection cabinet and Switch cabinet; Main control room, Automation host, Main control unit and Network switch	Environment, Cable temperature rise and Early warning
Air conditioning monitoring	Air conditioning lower part and Interface connection	Water immersion detection and Early warning; Operation status information collection; Remote control start stop, Set temperature and humidity
Environmental monitoring	GIS room, Power distribution device room, Secondary equipment room, Capacitor room, Battery room, Cable layer	Temperature and humidity monitoring; Smoke monitoring; Access control and security
Arrester monitoring	Incoming and Outgoing line of arrester	Action current; Leakage current; Action times
Equipment operation status monitoring	Electrical equipment	Environmental temperature and humidity; Energy acquisition unit status; Energy storage unit status; Real-time voltage and current
Line condition monitoring	Cable	Environmental temperature and humidity; Energy acquisition unit status; Energy storage unit status; Real-time voltage and current

3. SMS MODEL FOR SMART SUBSTATIONS

Figure 1 illustrates our blockchain network for smart the substation SMS. The model was designed based on improved LEACH and secrete sharing technology.

Before clustering, the base station (BS) assigns each sensor a uniform verification data block K_{init} and a unique identity number *ID*. With a large storage and strong computing power, the BS could select a polynomial for the cluster corresponding to each sensor, and construct the sub-secret and data block corresponding to each sensor.

It is assumed that the network has m-1 clusters. Each cluster $C_i(i=1, \ldots, m\text{-}1)$ has a cluster head and k-1($k \geq t$) ordinary sensors. In cluster C_i, the cluster head and ordinary sensors are denoted as CH_i and $C_{ir}(r=1, \ldots, k\text{-}1)$, respectively.

In our blockchain network, the sensors self-organize into three groups: the CH, ordinary sensors, and other sensors. The other sensors are consensus sensors other than the CH and ordinary sensors. The CH splits the monitoring data recorded on the blockchain into n sub-secrets, and constructs n data blocks to store the n sub-secrets. Next, the CH sends n-1 blocks to n-1 ordinary sensors in the blockchain network. Upon receiving a block, an ordinary sensor will verify its correctness before linking it to the blockchain. Each other sensor either requests for data block from one of its n neighboring sensor, or receives the block broadcasted by the CH and links it to the blockchain.

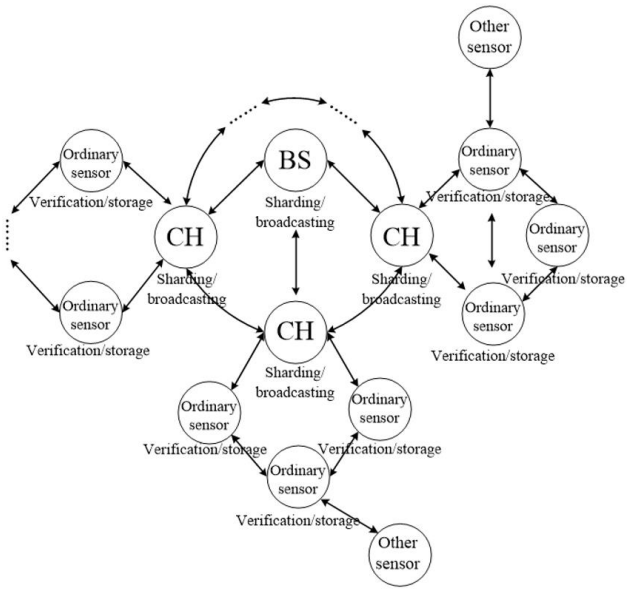

Figure 1. Our blockchain network for smart the substation SMS

4. SHARD STORAGE AND MANAGEMENT PLAN

4.1 Initialization

In the proposed shard storage and management plan, a complete management cycle contains six phases: initialization, sub-secret generation, blockchain construction, data block distribution and storage, data block acquisition, and self-secrete stitching. The first four phases receive the data requested to be stored in the blockchain in this cycle, and output the data blocks that will be distributed to CH or ordinary sensors and linked to the blockchain.

Suppose the blockchain network has m-1 clusters. The network can be initialized in two steps:

Step 1. The BS selects two large prime numbers x and y. There must exist $p=2x+1$ and $q=2y+1$. Then, n is defined as the product between p and q. The BS will select a generator g randomly from $[n^{1/2}, n]$, and also selects a large prime $P>n$. After that, the BS will broadcast (n, g, P) to all sensors in the network. Each sensor will be assigned a unique ID: ID_{CHi} for the CHs, and $ID_{\mathrm{Mi,\,r}}$ for ordinary sensors, where $i=1, \ldots m\text{-}1$ and $r=1, \ldots k\text{-}1$.

Step 2. In each cycle, the BS generates m t-1-order polynomials. One of them will be used for the blockchain communication between the BS and the CHs, and the other for that between each CH and the ordinary sensors in its cluster.

Take the communication polynomial between the BS and the CHs for example. The threshold parameters [t, n] ($t<n$) are configured based on the real-time state of the blockchain network, where n is the number of sub-secrets and t is the minimum number of sub-secrets needed to restore data. Next, the data D' requested to be stored in the blockchain are stringified and then decimalized into data D. Data D was split into $t-1$ parts, forming a sequence $d_1, d_2, \ldots d_{t-1}$.

The specific steps for generating polynomials are as follows:

(1) Select a random number a to generate a curve:

$$f_{CH_1}(x) = ax + d_1$$

(2) Select two points $A_{\mathrm{CHt1}}(1)=f_{\mathrm{CH1}}(1)$ and $A_{\mathrm{CHt1}}(2)=f_{\mathrm{CH1}}(2)$ on the generated curve;

(3) Perform polynomial generation within $2\le i\le t-1$. First, generate the following polynomial based on the selected two points and d_i:

$$f_{CH_i}(x) = A_{CH_{i-1}}(i)x^i + A_{CH_{i-1}}(i-1)x^{i-1} + \cdots + A_{CH_{i-1}}(1)x + d_{CHi}$$

If $i!=t-1$, select i+1 points on the curve as the sub-secrets to be shared, and delete the previously generated sub-secrets; if $i=t-1$, output the t-1-order polynomial:

$$f_{CH_{t-1}}(x) = A_{CH_{t-2}}(t-1)x^{t-1} + A_{CH_{t-2}}(t-2)x^{t-2} + \cdots + A_{CH_{t-2}}(1)x + d_{t-1}$$

Similarly, if $i=t$-1, the communication polynomial between each CH and the ordinary sensors in its cluster can be outputted as:

$$f_{M_{t-1}}(x) = A_{M_{t-2}}(t-1)x^{t-1} + A_{M_{t-2}}(t-2)x^{t-2} + \cdots + A_{M_{t-2}}(1)x + d_{t-1}$$

4.2 Block generation and data recovery between the BS and the CHs

4.2.1 Data block construction and distribution

During the block construction, the BS computes the sub-secret $f_{\mathrm{CHi}}(ID_{\mathrm{CHi}})$ of each CH based on the ID_{CHi}. Then, $\{ID_{\mathrm{CHi}}, f_{\mathrm{CHi}}(ID_{\mathrm{CHi}})\}$ will be adopted for the communication between the BS and each CH.

Specifically, the BS randomly selects an x_0 from $[t, n]$, which is relatively prime to p-1 and q-1, and computes $y_0=g^{x0}$. Then, each CH selects an x_{CHi} from $[t, n]$ and computes $y_{\mathrm{CHi}}=g^{x\mathrm{CHi}}$. The CH will send $(ID_{\mathrm{CHi}}, y_{\mathrm{CHi}})(i=1, \ldots m\text{-}1)$ to the BS, which will be used to restore the sub-secret. The BS must ensure that there is no $y_{\mathrm{CHi}}=y_{\mathrm{CHj}}$ under $ID_{\mathrm{CHi}}\neq ID_{\mathrm{CHj}}$. Otherwise, reselection will be performed.

From the polynomial obtained in the previous step, m-1 points can be obtained, that is, $d_1=[ID_{\mathrm{CH1}}, f_{\mathrm{CHt-1}}(ID_{\mathrm{CH1}})]$, $d_2=[ID_{\mathrm{CH2}}, f_{\mathrm{CHt-1}}(ID_{\mathrm{CH2}})]$, …, $d_{\mathrm{m\text{-}1}}=[ID_{\mathrm{CHm\text{-}1}}, f_{\mathrm{CHt-1}}(ID_{\mathrm{CHm\text{-}1}})]$. These points will serve as m-1 sub-secrets. Then, m-1 CHs will be selected according to the parameters (and their hash values) required for block structure computation. After that, m-1 data blocks can be constructed based on the existing data and parameters. Next, the BS will broadcast the following information:

$$\left\{\begin{array}{l} y_0, [ID_{CH1}, f_{CHt-1}(ID_{CH1})(y_{CH1})^{x_0}], \\ [ID_{CH2}, f_{CHt-1}(ID_{CH2})(y_{CH2})^{x_0}], \\ \cdots, \\ [ID_{CHm-1}, f_{CHt-1}(ID_{CHm-1})(y_{CHm-1})^{x_0}] \end{array}\right\}$$

Then, the m-1 data blocks will be distributed to m-1 CHs. Each CH needs to check the correctness of the block it receives: whether the block structure is reasonable and whether the hash value in the block header agrees with that in the header of the previous block. After the check, the CH will link the data block to the blockchain.

4.2.2 Block data recovery and reading

The last two phases of the cycle receive the location index of the block information to be read (i.e. the ID of each CH block) and output the blocks at specified CHs. The data reading is completed as follows:

First, each CH checks its block according to ID_{CHi}, and obtains a series of information, including the BS address and the threshold parameters [t, n]. Then, the CH requests the BS to provide the block with the serial number ID until receiving the t-th block. Once receiving all the information, the CH starts to stitch the sub-secrets. Let $d_1'=[ID_{\mathrm{CH1}}', f_{\mathrm{CHt-1}}(ID_{\mathrm{CH1}}')]$, $d_2'=[ID_{\mathrm{CH2}}', f_{\mathrm{CHt-1}}(ID_{\mathrm{CH2}}')]$, …, $d_t'=[ID_{\mathrm{CHt\text{-}1}}', f_{\mathrm{CHt-1}}(ID_{\mathrm{CHt}}')]$ be the t sub-secrets obtained by the CH. Then, each CH computes its share of sub-secrets based on the broadcasted information and its own block data. To obtain data d_{CHi}, the t−1-th order polynomial $f_{\mathrm{CHt-1}}(x)$ can be obtained through Lagrange interpolation:

$$f_{CHt-1}(x) = \sum_{i=1}^{t} f(ID_{CHi}) \prod_{t}^{j=1, j\neq i} \frac{x - ID_{CHj}}{ID_{CHi} - ID_{CHj}}$$

$$d_{CHi} = f_{CHt-1}(0) = \sum_{i=1}^{t} f(ID_{CHi}) \prod_{t}^{j=1, j\neq i} \frac{-ID_{CHj}}{ID_{CHj} - ID_{CHj}}$$

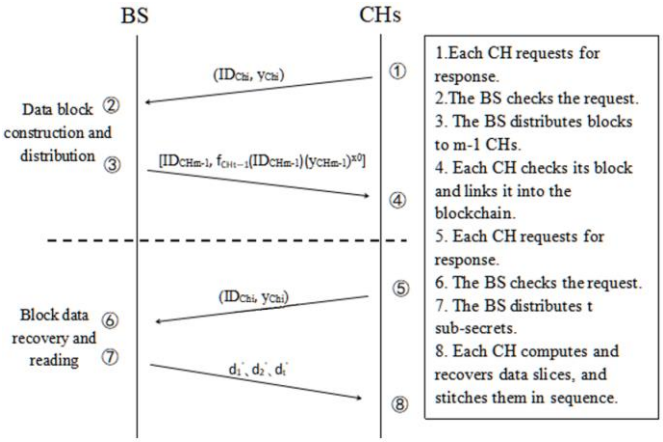

Figure 2. Workflow of the block generation and data recovery between the BS and the CHs

From the above formulas, the following coefficients could be extracted in turn: $A_{\text{CHT-2}}(t-1)$, $A_{\text{CHT-2}}(t-2)$, …, $A_{\text{CHT-2}}(1)$, i.e. $[ID_{\text{CH1}}, f_{\text{CHt}-2}(ID_{\text{CH1}})]$, $[ID_{\text{CH2}}, f_{\text{CHt}-2}(ID_{\text{CH2}})]$, …, $[ID_{\text{CHt-1}}, f_{\text{CHt}-2}(ID_{\text{CHt-1}})]$. Then, Lagrange interpolation is implemented again to obtain the t－2-th order polynomial $f_{\text{CHt}-2}(x)$ and obtain data slices d_{t-2}. The above process is repeated to obtain all sub-secrets d_1, d_2, …d_{t-1}. These sub-secrets are stitched in sequence into a decimal data D, making the completion of data recovery.

The workflow of the block generation and data recovery between the BS and the CHs is explained in Figure 2 above.

4.3 Intra-cluster block generation and data recovery

4.3.1 Data block construction and distribution

During the block construction, the CH computes the sub-secret $f_{\text{Mi}}(ID_{\text{Mi, r}})$ of each ordinary sensor based on the $ID_{\text{Mi, r}}$. Then, $\{ID_{\text{Mi, r}}, f_{\text{Mi}}(ID_{\text{Mi, r}})\}$will be adopted for the communication between the CH and each ordinary sensor.

Specifically, the CH randomly selects an x_{CHi} from $[t, n]$, which is relatively prime to p-1 and q-1. Then, the BS computes $y_{\text{CHi}} = g^{x\text{CHi}}$. Meanwhile, each ordinary sensor selects an $x_{\text{Mi, r}}$ from $[t, n]$ and computes $y_{\text{Mi, r}}=g^{x\text{Mi, r}}$. The BS will broadcast $(ID_{\text{CHi}}, y_{\text{CHi}})(i=1, \ldots m\text{-}1)$ to each sensor, and each sensor will return $(ID_{\text{Mi, r}}, y_{\text{Mi, r}})(i=1, \ldots m\text{-}1, r=1, \ldots k\text{-}1)$ to the BS. The BS must ensure that there is no $y_{\text{Mi, r}}=y_{\text{Mi, z}}$ under $ID_{\text{Mi, r}}\neq ID_{\text{Mi, g}}$. Otherwise, reselection will be performed.

From the polynomial obtained in the initialization phase, k-1 points can be obtained from each cluster, that is, $d_1=[ID_{\text{Mi, 1}}, f_{\text{Mt-1}}(ID_{\text{Mi, 1}})]$, $d_2=[ID_{\text{Mi, 1}}, f_{\text{Mt-1}}(ID_{\text{Mi, 1}})]$, …, $d_{\text{k-1}}=[ID_{\text{Mi, k}}, f_{\text{Mt-1}}(ID_{\text{Mi, k}})]$. These points will serve as k-1 sub-secrets. For each CH, there is $d_0=[ID_{\text{CHi}}, f_{\text{CHt-1}}(ID_{\text{CHi}})]$.

After the BS makes the broadcast, k-1 ordinary sensors will be selected according to the parameters (and their hash values) required for block structure computation. After that, k-1 data blocks can be constructed based on the existing data and parameters. Next, the k-1 data blocks will be distributed to k-1 ordinary sensors. Each ordinary sensor needs to check the correctness of the block it receives, and link the checked data block to the blockchain.

4.3.2 Block data recovery and reading

The last two phases of the cycle receive the location index of the block information to be read (i.e. the ID of each ordinary sensor block) and output the blocks at specified ordinary sensors (i.e. the monitoring data on substations). The data reading is completed as follows:

First, each ordinary sensor checks its block according to $ID_{\text{Mi, r}}$, and obtains the relevant information. Then, the ordinary sensor requests the CH and the BS to provide the block with the serial number ID until receiving the t-th block. Once receiving all the information, the ordinary sensor starts to stitch the sub-secrets. Suppose the t sub-secrets are the sub-secret $d_0'=[ID_{\text{CHi}}', f_{\text{Mt-1}}(ID_{\text{CHi}}')]$ of the CH and the sub-secrets $d_{\text{t-1}}'=[ID_{\text{Mi, r}}', f_{\text{Mt-1}}(ID_{\text{Mi, r}}')]$ of t-1 ordinary sensors. Then, the CH and each ordinary sensor will compute its share of sub-secrets based on the broadcasted information and its own block data: $f_{\text{Mt-1}}(ID_{\text{CHi}})*(y_{\text{Mi, r}})^{x\text{CHi}}/(y_{\text{CHi}})^{x\text{Mi, r}}=f_{\text{Mt-1}}(ID_{\text{CHi}})$ and $f_{\text{Mt-1}}(ID_{\text{Mi, r}})*(y_{\text{CHi}})^{x\text{Mi, r}}/(y_{\text{CHi}})^{x\text{CHi}}=f_{\text{Mt-1}}(ID_{\text{Mi, r}})$. All the sub-secrets d_1, d_2, …d_{t-1} could be obtained by solving the t－1-th order polynomial $f_{\text{CHt}-1}(x)$ through Lagrange interpolation. These sub-secrets are stitched in sequence into a decimal data D, making the completion of data recovery.

The workflow of the block generation and data recovery within a cluster is explained in Figure 3 below.

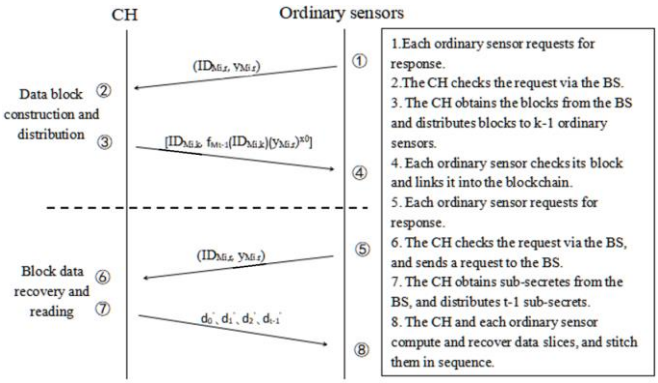

Figure 3. Workflow of intra-cluster block generation and data recovery

5. PERFORMANCE AND SECURITY ANALYSIS

In the SMS of smart substations, the sensors are assumed to fall into the following clusters:

(1) Security cluster M_1, including visible light sensors and infrared sensors.

(2) Transformer cluster M_2, including precision current sensors, semiconductor sensors, and broadband current sensors.

(3) Circuit breaker cluster M_3, including displacement sensors, vibration sensors, precision current sensors, and film capacitance sensors.

(4) Mutual inductor cluster M_4, including precision voltage sensors, and precision current sensors.

(5) Arrester cluster M_5, including precision current sensors.

This paper collects the basic operating data of grids from the above clusters, and treats these clusters as the units of command execution. On this basis, the performance and security of our shard storage and management plan are analyzed as follows:

5.1 Blockchain security

Our plan improves the Shamir's Secret Sharing algorithm. Under our plan, the monitoring data could be transmitted in an efficient and reliable manner, and linked into the blockchain

with high security. Taking the common forking attack for instance, the success rate of the attack can be computed by:

$$1-\sum_{i=0}^{h}\frac{\lambda^i e^{-\lambda}}{i!}(1-(\frac{a}{b})^{h-i})$$

where, h is the number of sensors that are unlikely to be attacked successfully. Suppose the attacker leads the competition in the previous cycle, i.e. $b>a$, and $\lambda=ha/b$. Then, it can be seen that the success rate of the attack decreases exponentially with the growing number of blocks h, that is, the success of the attack only depends on the values of p and q. In other words, the computing power of each sensor determines whether it will be successfully attacked, regardless of whether it stores data. Therefore, our plan inherits the superiority of blockchain technology in terms of security.

5.2 Scalability

If a new sensor is added and needs to join the network in the next cycle (e.g. a new infrared sensor is added to the security cluster M_1), then the new sensor S_1 will select a random integer x_{S1} from $[t, n]$, compute $y_{S1}=g^{xS1}$, and keep x_{S1} confidential. After that, the sensor will randomly select an $ID_{M1,\,s1}$, and send ($ID_{M1,\,s1}$, y_{S1}) to the BS. The BS will check the legitimacy of $ID_{M1,\,s1}$, and ensure that there is no $y_{Mi,\,s1}=y_{Mi,\,r}$ under $ID_{M1,\,s1}\neq ID_{M1,\,r}$($r=1, \ldots k$-1). If both conditions are fulfilled, then the sensor S_1 could be admitted to the network, and allocated to cluster M_1. The BS will construct a data block and distribute sub-secret to that sensor.

If the revocation of a sensor is detected by its CH or neighboring sensor (e.g. a visible light sensor S_2 is removed from security cluster M_1), then the CH of M_1 will capture the ID_{S2} of the sensor, and broadcast the ID to the BS and other CHs. The BS and other CHs will record ID_{S2} into their revocation sets.

At the start of a new cycle, the network only needs to reselect the private keys for the sensors added or revoked in the previous cycle, and send the IDs and private keys to the BS for verification. In this way, the network can be initialized for the new cycle.

5.3 Storage ability

Based on blockchain technology, our plan stores the monitoring data of substation state locally, reducing the storage pressure of each sensor to $1/(t-1)$ of the original pressure. In our plan, some sensors frequently engaging in communication face relaxed requirements on computing and storage capacities, while the entire blockchain network of the SMS face stricter requirements. Hence, our plan can be applied well in large substations, whose main demand is to store monitoring data in blockchain.

5.4 Security

The revoked sensor will not be assigned any data block in the new cycle. It is unknown where will the data block originally assigned to that sensor will be assigned. Thus, an attacker can at most obtain t-1 values from the broadcasted polynomial $f_{CHt-2}(x)$ or $f_{Mt-1}(x)$. The difficulty of recovering the first-order polynomial $f_{CHt-2}(x)$ or $f_{Mt-1}(x)$ from the t-1 values is equivalent to undermining the Shamir's Secret Sharing under the (t, n) threshold. This is not computationally feasible. Therefore, the attacker is unable to recover the first-order polynomial, not to mention restoring the original monitoring data.

For any cluster F_1, suppose there are fewer than t-1 sensors, all of which are added to the cluster after the current cycle. It can be derived that the attacker cannot restore the original monitoring data, even if he/she has obtained all the data blocks and sub-secrets in cluster F_1. This is because the attacker can only obtain t-1 values from polynomial $f_{CHt-2}(x)$ or $f_{Mt-1}(x)$. Similarly, the attacker is unable to restore the t-1-order polynomial nor recover the original monitoring data.

In terms of t-1 forward secrecy, suppose F_2 is the set of sensors revoked before the cycle. It can be proved that the attacker cannot acquire any information of the current cycle, even if he/she has obtained all the data blocks and sub-secrets in cluster F_1. In other words, the attacker can only obtain single points of the polynomial, but cannot restore the polynomial or acquire the monitoring data.

6. CONCLUSIONS

This paper analyzes the security strategy of the SMS for smart substations, and then designs the architecture of smart substations. Based on the security of blockchain technology, the authors proposed a blockchain network for smart substations, using the secrete sharing technology, and designed the corresponding shard storage and management plan. The proposed plan is superior in system security, and extends the network lifecycle. The superiority is mainly manifested in the following aspects: (1) Like blockchain information, the data under our plan cannot be tampered with; (2) Before deployment, the IDs are assigned randomly to ensure the communication safety between sensors in the same cluster; (3) During clustering, each CH communicates with the ordinary sensors in its cluster by crosschecking of data blocks, i.e. the layered shard storage and management, which guarantees the long-term security of the network; (4) During system operation, our plan supports the update of the BS, CHs, and ordinary sensors.

ACKNOWLEDGEMENTS

Project Supported by Qinglan Project for the University Key Teacher from Jiangsu Education Department (2020); The Natural Science Foundation of the Jiangsu Higher Education Institutions(19KJB470018); The Science and Technology Project of Jiangsu Province Construction System (2018ZD065); The Key Research and Development Program of the Xuzhou Municipal (KC19224).

REFERENCES

[1] Wang, A., Fan, J., Guo, Y. (2016). Application of blockchain in energy interconnection. Electric Power Information and Communication Technology, 9: 1-6.

[2] Zhang, N., Wang, Y., Kang, C., Cheng, J., He, D.W. (2016). Blockchain technique in the energy internet: preliminary research framework and typical applications. Proceedings of the CSEE, 36(15): 4011-4022.

[3] Li, B., Cao, W., Qi, B., Sun, Y., Guo, N., Su, Y., Cui, G. (2017). Overview of application of block chain technology in ancillary service market. Power System Technology, 41(3): 736-744.

[4] Xue, L., Teng, Y., Zhang, Z., Li, J., Wang, K., Huang, Q. (2017). Blockchain technology for electricity market in microgrid. In 2017 2nd International Conference on Power and Renewable Energy (ICPRE), pp. 704-708. https://doi.org/10.1109/ICPRE.2017.8390625

[5] Danzi, P., Angjelichinoski, M., Stefanović, Č., Popovski, P. (2017). Distributed proportional-fairness control in microgrids via blockchain smart contracts. In 2017 IEEE International Conference on Smart Grid Communications (SmartGridComm), pp. 45-51. https://doi.org/10.1109/SmartGridComm.2017.8340713

[6] Kim, G., Park, J., Ryou, J. (2018). A study on utilization of blockchain for electricity trading in microgrid. In 2018 IEEE International Conference on Big Data and Smart Computing (BigComp), pp. 743-746. https://doi.org/10.1109/BigComp.2018.00141

[7] Mengelkamp, E., Gärttner, J., Rock, K., Kessler, S., Orsini, L., Weinhardt, C. (2018). Designing microgrid energy markets: A case study: The Brooklyn Microgrid. Applied Energy, 210: 870-880. https://doi.org/10.1016/j.apenergy.2017.06.054

[8] Di Silvestre, M.L., Gallo, P., Ippolito, M.G., Sanseverino, E.R., Zizzo, G. (2018). A technical approach to the energy blockchain in microgrids. IEEE Transactions on Industrial Informatics, 14(11): 4792-4803. https://doi.org/10.1109/TII.2018.2806357

[9] Wang, G.N., Yang, J.F., Wang, S. (2019). Distributed optimization of power grid considering dispatching of electric vehicle battery swapping stations and data storage of blockchain. Automation of Electric Power Systems, 43(8): 110-117.

[10] Sharma, V. (2018). An energy-efficient transaction model for the blockchain-enabled internet of vehicles (IoV). IEEE Communications Letters, 23(2): 246-249. https://doi.org/10.1109/LCOMM.2018.2883629

[11] Casado-Vara, R., Chamoso, P., De la Prieta, F., Prieto, J., Corchado, J.M. (2019). Non-linear adaptive closed-loop control system for improved efficiency in IoT-blockchain management. Information Fusion, 49: 227-239. https://doi.org/10.1016/j.inffus.2018.12.007

[12] Su, Z., Wang, Y., Xu, Q., Fei, M., Tian, Y.C., Zhang, N. (2018). A secure charging scheme for electric vehicles with smart communities in energy blockchain. IEEE Internet of Things Journal, 6(3): 4601-4613. https://doi.org/10.1109/JIOT.2018.2869297

[13] Ferraro, P., King, C., Shorten, R. (2018). Distributed ledger technology for smart cities, the sharing economy, and social compliance. IEEE Access, 6: 62728-62746. https://doi.org/10.1109/ACCESS.2018.2876766

[14] Jiang, P., Guo, F., Liang, K., Lai, J., Wen, Q. (2017). Searchain: Blockchain-based private keyword search in decentralized storage. Future Generation Computer Systems, 107: 781-792. https://doi.org/10.1016/j.future.2017.08.036

[15] Kuo, T.T., Kim, H.E., Ohno-Machado, L. (2017). Blockchain distributed ledger technologies for biomedical and health care applications. Journal of the American Medical Informatics Association, 24(6): 1211-1220. https://doi.org/10.1093/jamia/ocx068

[16] Xu, C., Wang, K., Xu, G., Li, P., Guo, S., Luo, J. (2018). Making big data open in collaborative edges: A blockchain-based framework with reduced resource requirements. In 2018 IEEE International Conference on Communications (ICC), pp. 1-6. https://doi.org/10.1109/ICC.2018.8422561

[17] Lewison, K., Corella, F. (2016). Backing rich credentials with a blockchain PKI. Pomcor. com.

[18] Li, Y., Zheng, K., Yan, Y., Liu, Q., Zhou, X. (2017). EtherQL: A query layer for blockchain system. In International Conference on Database Systems for Advanced Applications, pp. 556-567. https://doi.org/10.1007/978-3-319-55699-4_34

[19] Li, Y., Huang, J.Q., Qin, S, Wang, R. (2017). Big data model of security sharing based on blockchain. In 2017 3rd International Conference on Big Data Computing and Communications (BIGCOM), pp. 117-121.

[20] Kang, J., Yu, R., Huang, X., Maharjan, S., Zhang, Y., Hossain, E. (2017). Enabling localized peer-to-peer electricity trading among plug-in hybrid electric vehicles using consortium blockchains. IEEE Transactions on Industrial Informatics, 13(6): 3154-3164. https://doi.org/10.1109/TII.2017.2709784

[21] Huang, X., Zhang, Y., Li, D., Han, L. (2019). An optimal scheduling algorithm for hybrid EV charging scenario using consortium blockchains. Future Generation Computer Systems, 91: 555-562. https://doi.org/10.1016/j.future.2018.09.046

[22] Darwish, M.A., Yafi, E., Al Ghamdi, M.A., Almasri, A. (2020). Decentralizing Privacy Implementation at Cloud Storage Using Blockchain-Based Hybrid Algorithm. Arabian Journal for Science and Engineering, 45: 3369-3378. https://doi.org/10.1007/s13369-020-04394-w

[23] Kurt Peker, Y., Rodriguez, X., Ericsson, J., Lee, S.J., Perez, A.J. (2020). A cost analysis of internet of things sensor data storage on blockchain via smart contracts. Electronics, 9(2): 244. https://doi.org/10.3390/electronics9020244

[24] Curbera, F., Dias, D.M., Simonyan, V., Yoon, W.A., Casella, A. (2019). Blockchain: An enabler for healthcare and life sciences transformation. IBM Journal of Research and Development, 63(2/3): 8-1. https://doi.org/10.1147/JRD.2019.2913622

[25] Nguyen, G.T., Kim, K. (2018). A Survey about Consensus Algorithms Used in Blockchain. Journal of Information Processing Systems, 14(1).