Alexandria Engineering Journal (2021) 60, 337–346

HOSTED BY

Alexandria University

Alexandria Engineering Journal

www.elsevier.com/locate/aej
www.sciencedirect.com

Design of a dynamic key management plan for intelligent building energy management system based on wireless sensor network and blockchain technology

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

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

Received 6 July 2020; revised 29 July 2020; accepted 20 August 2020
Available online 19 September 2020

KEYWORDS

Intelligent building energy management system (IBEMS);
Dynamic key;
Blockchain;
Ubiquitous Power Internet of Things (UPIoT)

Abstract In modern buildings, the intelligent building energy management system (IBEMS) faces several problems with its centralized architecture: the difficulty in the networking between end devices, the lack of flexibility, and the limited sharing of underlying information. To overcome these problems, this paper probes into the framework of the wireless sensor network (WSN), and designed a network model of the IBEMS. Next, the security of blockchain technology was fully examined, and a dynamic key management strategy was proposed based on the blockchain for the IBEMS. The feasibility of the proposed plan was verified through experiments. The experimental results show that the proposed plan reduces the data storage time and space of each sensor, and optimizes the control of the IBEMS. The research results provide a reference for setting up a safe and reliable IBEMS based on spatial distribution, and help promote blockchain technology in other scenarios of the UPIoT.

1. Introduction

The blockchain integrates various computer technologies into a novel decentralized basic framework and distributed computing paradigm [1–4]. Decentralized, open, and transparent, the blockchain fully demonstrates the principles of ubiquitous power Internet of Things (UPIoT) [5–7]. Coupled with the UPIoT, the blockchain will realize precise digital management of energy, and adapt to multiple scenarios of the Internet of energy, such as energy finance, electric vehicles, and green credit issuance, to name but a few [8–11].

In modern buildings, the power supply/distribution management system (PSDMS) adopts a centralized control architecture, which is inconsistent with the topology of building space. The system faces a high configuration cost, and difficulty in onsite construction, not to mention cross-system information sharing. The local systems and information terminals are not integrated or networked efficiently, and the subsystems are loosely connected.

The above problems are generally solved by three energy management strategies. The first strategy collects the information from the regional sensors on the spatial scale, through the electrical energy exchange within the building area [12–15]. The

* Corresponding author.
E-mail address: 10758@jsjzi.edu.cn (C. Jia).
Peer review under responsibility of Faculty of Engineering, Alexandria University.

https://doi.org/10.1016/j.aej.2020.08.019
1110-0168 © 2020 The Authors. Published by Elsevier B.V. on behalf of Faculty of Engineering, Alexandria University.

second strategy relies on energy storage technology to smooth power fluctuations on the time scale, and provides energy backup to keep power supply continuous and stable [16–19]. The third strategy shares electric energy with the aid of energy storage technology. The common defects of the three strategies include complex algorithm, poor privacy, and high communication cost [20–21]. Olivares et al. prove, a hierarchical energy management architecture of photovoltaic battery supercapacitor for DC microgrid system was built [22]. Askarzadeh prove, a Bess energy management method was proposed for the energy storage power station in the photovoltaic energy storage combined system [23], which can realize the functions of stabilizing fluctuation and time of use price at the same time. To sum up, most of the current research on building energy management is based on information collection and control state, while the research on energy flexible control method considering information sharing in the management process is less.

This paper fully considers the problems in the centralized architecture of intelligent building energy management system (IBEMS), namely, the difficulty in the networking between end devices, the lack of flexibility, and the limited sharing of underlying information. To solve the problems, the authors analyzed the framework of the wireless sensor network (WSN) for the PSDMS, and designed a network model of the IBEMS. Through the security analysis of the blockchain technology, a blockchain-based dynamic key management strategy was proposed for the IBEMS. Experimental results show that the proposed plan reduces the data storage time and space of each sensor, and optimizes the control of the IBEMS. The research results help promote blockchain technology in other scenarios of the UPIoT.

2. Architecture of the IBEMS

In intelligent buildings, sensors replace manual alarms and traditional alarm devices. The equipment and line signals could be identified, located, tracked, monitored, and responded automatically in real time. The main monitoring targets include lightning, air conditioning, fire, security, and operating state of energy management equipment. Compared with the PSDMS in traditional buildings, the IBEMS of intelligent buildings can effectively sense and respond to external changes and abnormalities, and ensure the security of distributed power generation, smart home interactive terminals, and centralized reading/transmission of information (e.g. power consumption).

The anti-intrusion system of the IBEMS relies on the collaboration between multiple sensors capable of detecting, analyzing, blocking, delaying, checking, and responding to security threats. The typical deployment of the WSN in the IBEMS is illustrated in Fig. 1.

Most IBEMS has three layers and two networks. The three layers refers to the station control layer, the separation layer and the process layer. The equipment on each layer are configured according to the required functions. The two networks stand for the station control layer network and the process layer network, which enable equipment on different layers to exchange information.

The three-layer two-network structure can realize real-time automatic control and intelligent adjustment of information collection, measurement, control, protection, measurement and detection, but it creates multiple independent information transmission networks, hindering the information sharing and interaction across station. Besides, the sheer number of switches and optical fibers complicates the network structure and wiring, and undermines the reliability of network equipment. Thus, the real-time performance of Ethernet must be improved by various methods, such as switched Ethernet, virtual local area network, and Rapid Spanning Tree Protocol (RSTP). In addition, Route Processor Redundancy (RPR) and High-Availability Seamless Redundancy (HSR) should be adopted to maintain the reliability of the communication network, equipment and software of the IBEMS.

3. Network structure of the IBEMS

In order to improve the flexibility and security of terminal equipment networking of intelligent building energy management system, in view of the existing deployment form of wire-

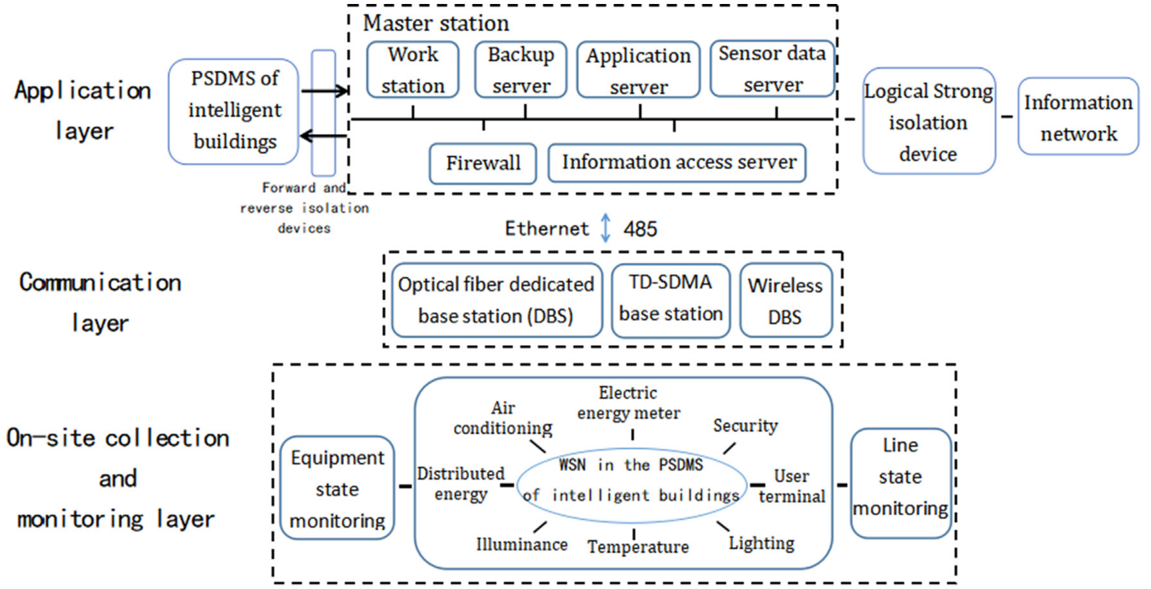


Fig. 1 The typical deployment of the WSN in the IBEMS.

less sensor network, this paper constructs the network architecture of intelligent building energy management system using device ring network. Considering the deployment of the WSN, the IBEMS devices were organized into rings. The ring structure can be applied effectively to the IBEMS.

As shown in Fig. 2, the ring-based IBEMS is arranged based on building units. The energy management portal in the figure is used to provide energy for wireless communication network and building units, and the power sales terminal management system is connected with the power department to provide electricity information and settle electricity charges. The building power distribution units are connected end to end through intelligent interactive terminals (IITs) to the DBS in the communication layer, creating the topology of a ring network. The IITs communicate with each other based on blockchain technology.

Within each building unit, there is a ring of sensors corresponding to various electrical devices. The interconnected sensors also communicate with each other based on blockchain technology.

The DBS assigns a unique identification (ID) number for each IIT and each sensor, selects a polynomial for the ring network of each building unit, and sets up a sub-secret and a data block for each sensor according to the sensor ID.

The network has m-1 building units $C_i(i = 1, \ldots, m\text{-}1)$, each of which contains an IIT CH_i and k-1($k \geq t$) ordinary sensors $C_{ir}(r = 1, \ldots, k\text{-}1)$.

The above network structure tolerates single point failure and maintains the normal operation of the ring network, and this is the most important feature of the traditional model. If there is a fault point in the network, the ring topology will automatically change to a linear topology, which maintains the normal communication of network data, and accurately detect the fault point for alarm and repair, ensuring the reliable transmission of various signals.

Moreover, the sensors of the electrical equipment in each system can be directly plugged into the ring network, allowing the host to collect and control the information of building units in real time. In this way, the subsystems with different functions in the same building area could exchange information smoothly. However, there are many sub units in the network model, so it is difficult to guarantee the communication security, which requires technical support.

4. Security of the IBEMS blockchain technology

The blockchain network for the WSN of the IBEMS boasts the advantages of decentralization, openness, autonomy, anonymity, and tamper-proof. If some sensors are attacked and damaged, the entire blockchain network will not be undermined. Even so, the blockchain network for the WSN of the IBEMS still face various security threats.

Take the proof of work (PoW) mechanism adopted by Bitcoin for example. The potential risk of blockchain to be attacked was analyzed by the attack model proposed by Zhang et al. [1]. The success rate q_s of tampering by the attacker can be calculated by:

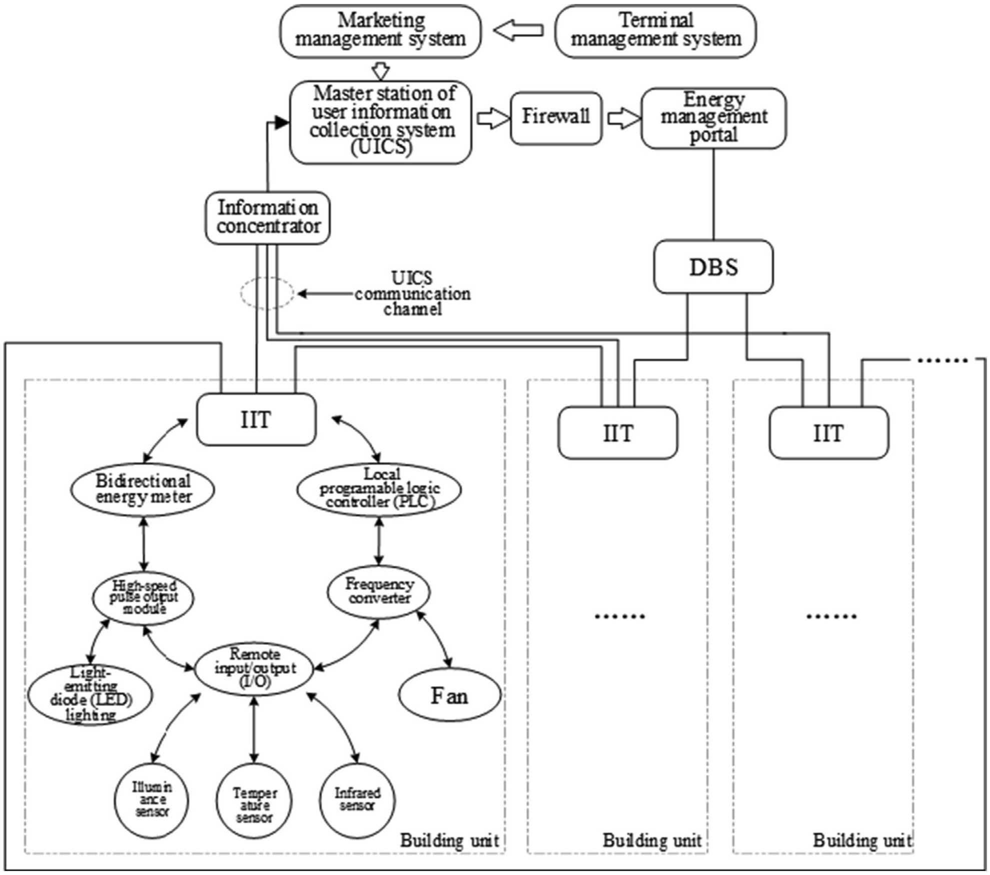

Marketing management system
Terminal management system
Master station of user information collection system (UICS)
Firewall
Energy management portal
Information concentrator
DBS
UICS communication channel
......
IIT
IIT
IIT
Bidirectional energy meter
Local programable logic controller (PLC)
High-speed pulse output module
Frequency converter
Light-emitting diode (LED) lighting
Remote input/output (I/O)
Fan
Illuminance sensor
Temperature sensor
Infrared sensor
......
......
Building unit
Building unit
Building unit

Fig. 2 The network structure of the IBEMS.

$$q_s = \sum_{k=0}^{\infty} \frac{\lambda^k e^{-\lambda}}{k!} \begin{cases} \left(\frac{q}{p}\right)^{z-k}, k \leqslant z \\ 1, k > z \end{cases}$$

where, p and q are the probabilities for the honest node and attack node to acquire the accounting power of the next block, respectively; λ is the attacker's block extension length; z is the block gap.

The above formula shows that the larger the value of block gap z, the lower the success rate of tampering. However, when the value of block gap z remains unchanged, the success rate of block forgery increases with the computing power of the attacker.

When the attacker has over 50% of the computing power of the entire network, the blockchains of the IBEMS can be paralyzed by recalculating the confirmed blocks or generating new blocks. Then, the information of sensors will no longer propagate to new blocks.

Currently, the key management plan of the IBEMS cannot resist offline dictionary attacks, because the keys are encrypted and stored uniformly by the DBS. This defect must be overcome to ensure the security of system communication. For this purpose, it is necessary to develop a dynamic key management strategy based on the distributed storage structure, which promotes the reissuance and management of keys.

5. Dynamic key management strategy based on blockchain

5.1. Basic ideas of Shamir's secret sharing

The basic idea of Shamir's (t, n) threshold secret sharing plan is as follows: The base station divides the initial secret into n shared sub-secrets, and distributes them to the sensors. The secret cannot be reconstructed unless t or more sensors combine their sub-secrets.

Under this plan, the secret is decomposed and reconstructed through Lagrange interpolation. After selecting independent random numbers a_1, a_2, $\ldots a_{t\text{-}1}$, the following t-1-order polynomial can be defined as:

$$f(x) = f(0) + a_1 x + a_2 x^2 + \cdots + a_{t-1} x^{t-1}$$

A total of n sub-secrets $f(x_i)$ are calculated and distributed to the sensors. During secret reconstruction, any t or more sensors can obtain t different points (x_i, $f(x_i)$) on polynomial f(x) by combining their sub-secrets, and then reconstruct the polynomial through Lagrange interpolation. Then, the initial secret can be restored by computing $f(x_i)$:

$$f(x) = \sum_{i=1}^{t} f(x_i) \left(\prod_{i \neq j} \frac{x - x_j}{x_i - x_j} \right)$$

In our blockchain-based dynamic key management plan for IBEMS, a complete management cycle consists of six stages: initialization, generation of sub-secrets, generation of data blocks, distribution and storage of data blocks, acquisition of data blocks, and secret reconstruction.

In the first four stages, the input is the data requested to be stored in the blockchain in this cycle, while the output is the data blocks that will be distributed to the IITs or ordinary sensors and linked to the blockchain.

5.2. Initialization

Suppose the blockchain network has m-1 building blocks. The network can be initialized in two steps (see Fig. 3):

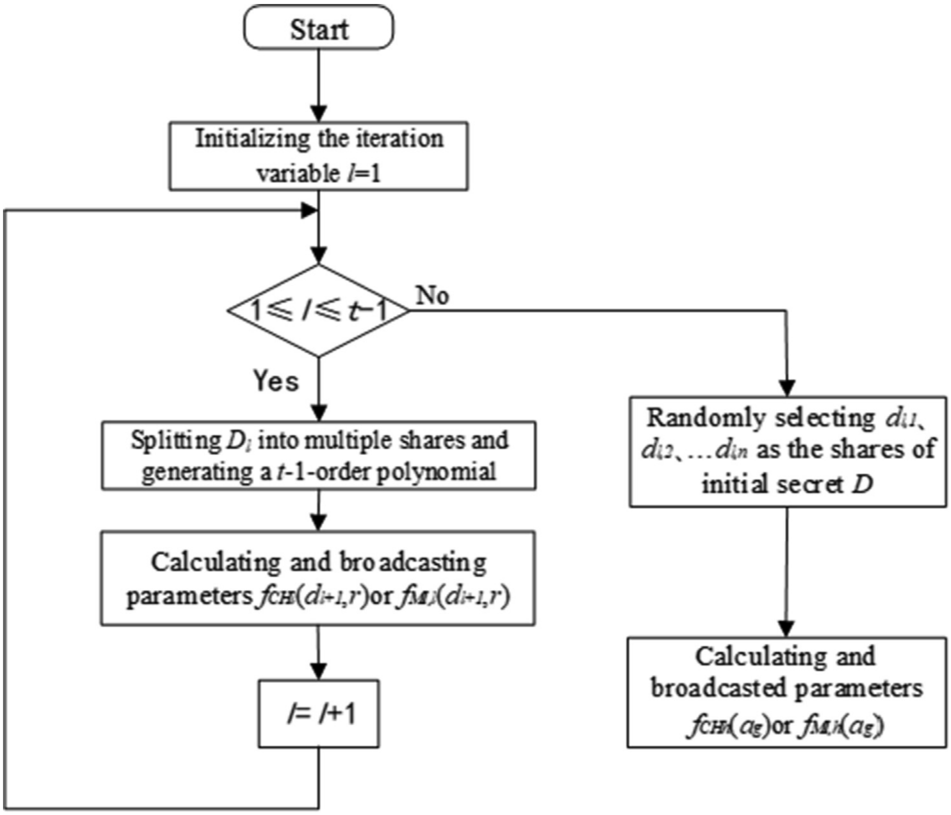

Start
Initializing the iteration variable l=1
$1 \leqslant l \leqslant t\text{-}1$
No
Yes
Splitting D_l into multiple shares and generating a t-1-order polynomial
Calculating and broadcasting parameters $f_{CH}(d_{l+1,r})$or $f_{MA}(d_{l+1,r})$
l= l+1
Randomly selecting d_{l1}、d_{l2}、…d_{ln} as the shares of initial secret D
Calculating and broadcasted parameters $f_{CH}(a_g)$or $f_{MA}(a_g)$

Fig. 3 The workflow of initialization.

Step 1. The DBS assigns each node a unique ID. The IITs are numbered as ID_{CHi} (i = 1, ...m-1) and the sensors are numbered as $ID_{MI,\ j}$ (j = 1, ...k-1; i = I) (the i value is a constant, because the power distribution unit is fixed).

Step 2. In each cycle, the DBS generates m t-1-order polynomials. One of them will be used for the blockchain communication between the DBS and the IITs, and the rest for that between IIT and the ordinary sensors in its ring.

Take the communication polynomial between the DBS and the IITs for instance. The threshold parameters [t, n] ($t \langle n$) 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 reconstruct the initial secret.

Next, the data D' requested by the IITs or sensors to be stored in the blockchain are stringified, and decimalized into data D. Data D are split into $t \times h$ shares, where h is the number of recursive layers. In other words, each sub-secret D_l is segmented into $d_{l,\ 1}$, $d_{l,\ 2}$, ...$d_{l,\ t\text{-}1}$(l = 1, 2, ...h).

Let F_{p} be a finite field, with $p = 2^{\lambda}$ be the safety parameter ($t\lambda > 80$). Then, the polynomial generation of the DBS can be realized in the following steps:

(1) Randomly take the sub-secret D_l in each layer as the coefficient to generate a t-1-order polynomial. If the polynomial is used for the communication between the DBS and the IITs, then:

$$f_{CHl}(x) = d_{l,1} + d_{l,2}x + \cdots + d_{l,t-1}x^{t-1}$$

If the polynomial is used for the communication between an IIT and sensors, then:

$$f_{MI,l}(x) = d_{l,1} + d_{l,2}x + \cdots + d_{l,t-1}x^{t-1}$$

(2) Under the interval of $1 \le l \le t$-1, substitute sub-secret D_{l+1}, i.e. $d_{l+1,\ 1}$, $d_{l+1,\ 2}$, ...$d_{l+1,\ t\text{-}1}$(l = 1, 2, ...h) into the above formula as an explanatory variable, and calculate and broadcast the parameter $f_{CHl}(d_{l+1,\ r})$ or $f_{MI,\ l}(d_{l+1,\ r})$(r = 1, ...t-1) for sub-secret D_{l+1}.

(3) On the last recursive layer, randomly select $d_{l,\ 1}$, $d_{l,\ 2}$, ...$d_{l,\ n}$ as the shares of the initial secret D, and calculate and broadcast parameters $f_{CHh}(a_g)$ or $f_{MI,h}(a_g)$(g = 1, ...n).

5.3. Block generation and data recovery between building units

5.3.1. Block construction and distribution

The DBS calculates and broadcasts parameter $f_{CHl}(d_{l+1,\ r})$. Then, the IITs will send (ID_{CHi}, $f_{CHl}(d_{l+1,\ r})$)(i = 1, ...m-1) to the DBS for sub-secret calculation in the stage of secret reconstruction.

From the polynomial obtained in the previous step, m-1 points can be obtained to serve as m-1 sub-secret data: $d_{l,\ 1}$ = [ID_{CH1}, $f_{CHl}(d_{l+1,\ 1})$], $d_{l,\ 2}$ = [ID_{CH2}, $f_{CHl}(d_{l+1,\ 2})$], ..., $d_{l,\ m\text{-}1}$ = [$ID_{CHm\text{-}1}$, $f_{CHl}(d_{l+1,\ m\text{-}1})$). The system will construct m-1 data blocks according to the block structure of the IITs and the existing data parameters, and calculate the hash values. Then, m-1 IITs will be selected, and assigned with m-1 data blocks. Fig. 4 shows the structure diagram of the data block, where Merkle tree root refers to a value finally obtained through multiple hash operations for all the accesses contained in this block.

To make the block data of the IITs verifiable, a bivariate collision-resistant hash function H(x, y) is introduced into the sub-secret recursive distribution module. The function generates a message authentication code for generating secret shares. The code helps to check the structure of data blocks, and compute whether the hash value of the header in the previous block agrees with that in the header of the current block:

Step 1. Select and broadcast a random number R, and calculate $u_{\mathrm{g}} = H(R,\ a_g)$($g$ = 1, ...n) as pseudo shares of the secret.

Step 2. Calculate and broadcast $U_{\mathrm{g}} = H(R,\ u_g)$ and $f_{CHh}(u_g)$ (g = 1, ...n), and distribute u_1, u_2, ...u_n to different IITs.

Step 3. Link the data blocks to the blockchain by the IITs.

5.3.2. Restoration and reading of block data

In the latter two stages of the management cycle, the input is the location index of the blocks to be read, i.e. the IDs of

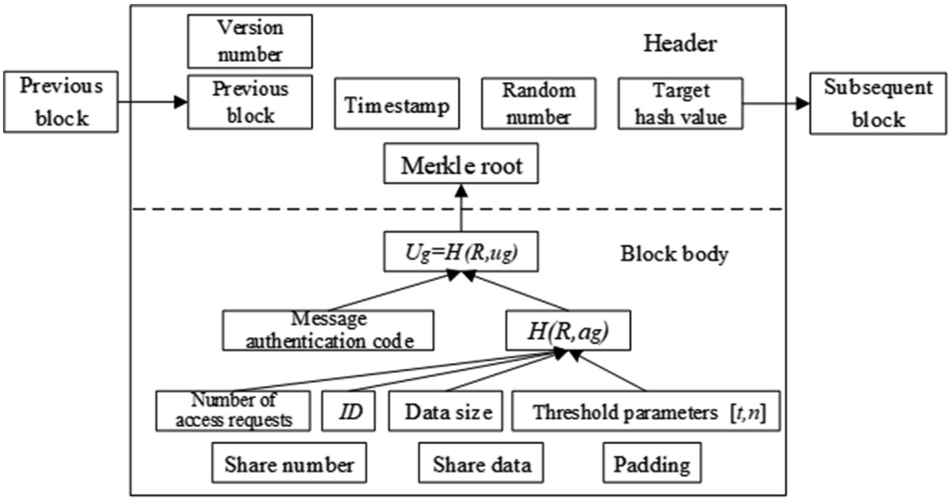


Fig. 4 The structure of data block.

the IITs, and the output is the information of the blocks at the specified locations.

Each IIT keeps requesting the DBS to respond to the data of the blocks with the requested IDs, until it receives the t sub-secrets for secret reconstruction. Upon receiving all the data, the IIT will start to reconstruct the initial secret.

Suppose the t sub-secrets obtained by the IIT are $d'_1 = [ID_{CH1}{}', f_{CHl}(d'_{l+1,1})]$, $d'_2 = [ID_{CH2}{}', f_{CHl}(d'_{l+1,2})]$, …, $d_{l,\ t}{}' = [ID_{CHt}{}', f_{CHl}(d_{l+1,\ t}{}')]$. Then, the IIT will calculate its sub-secrets based on the broadcasted data and the block data in its storage by the following polynomial:

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

$$f_{CHl}(x) = \sum_{i=1}^{t} f_{CHl}(d_{l+1,i}) \prod_{j=1,j\neq i}^{t} \frac{x - ID_{CHj}}{ID_{CHi} - ID_{CHj}}$$

where, $1 \leq g \leq t$-1. From the above formula, the following coefficients are extracted in turn: $_{CHh}(d_{h,\ t\text{-}1})$, $f_{CHl}(d_{h,\ t\text{-}2})$, …, $f_{CHl}(d_{h,\ 1})$, that is, $[ID_{CH1}, f_{CHh}(d_{h,\ 1})]$, $[ID_{CH2}, f_{CHh}(d_{h,\ 2})]$, …, $[ID_{CHt\text{-}1}, f_{CHh}(d_{h,\ t\text{-}1})]$. On this basis, the sub-secret data are all obtained as D_1, D_2, …$D_{t\text{-}1}$.

If $1 \leq l \leq h$-1, the shared polynomial $f_{CHl}(x)$ is derived from the coefficients of $f_{CHl+1}(x)$ $(d_{l+1,\ 1}, d_{l+1,\ 2}, \ldots d_{l+1,\ t\text{-}1})$ and the broadcasted parameters $(f_{CHl}(d_{l+1,\ 1}), f_{CHl}(d_{l+1,\ 2}), \ldots f_{CHl}(d_{l+1,\ t\text{-}1}))$, resulting in the sub-secrets D_l. Finally, the sub-secrets are stitched in turn into a decimal data D, which is outputted as the reconstructed initial secret.

To verify the authenticity of the data block in an IIT, t out of n pseudo shares are selected by random for secret reconstruction. First, the message authentication code is employed to verify whether that pseudo shares are authentic. If $U_g = H(R, u_g)$, then the pseudo shares are effective. The shared polynomial about the sub-secrets can be expressed as:

$$f_{CHh}(x) = \sum_{i=1}^{t} f_{CHh}(a_g) \prod_{j=1,j\neq i}^{t} \frac{u - u_j}{u_i - u_j}$$

$$f_{CHl}(x) = \sum_{i=1}^{t} f_{CHl}(d_{l+1,i}) \prod_{j=1,j\neq i}^{t} \frac{u - u_{CHj}}{u_{CHi} - u_{CHj}}$$

5.4. Block generation and data recovery in each building unit

5.4.1. Block construction and distribution

The IIT calculates and broadcasts parameter $f_{MI,l}(d_{l+1,\ r})$. Then, the sensors will send $(ID_{MI,j}, y_{MI,\mathrm{j}})(j = 1, \ldots k\text{-}1)$ to the IIT.

From the polynomial obtained through initialization, k-1 points can be obtained to serve as k-1 sub-secret data: $d_{l,\ 1} = [ID_{MI,1}, f_{MI,\ l}(d_{l+1,\ 1})]$, $d_{l,\ 2} = [ID_{MI,2}, f_{MI,\ l}(d_{l+1,\ 2})]$, …, $d_{l,\ k\text{-}1} = [ID_{MI,k\text{-}1}, f_{MI,\ l}(d_{l+1,\ k\text{-}1})]$. For the IIT, there is $d_{l,\ 0} = [ID_{CHl}, f_{MI,\ l}(d_{l+1,\ 0})]$.

Similarly, the IIT will construct k-1 data blocks according to the block structure of the sensors and the existing data parameters, and calculate the hash values. Then, k-1 sensors will be selected, and assigned with k-1 data blocks.

Next, the block data of each sensor will be authenticated, and the distributed blocks will be linked to the blockchain.

5.4.2. Restoration and reading of block data

In the latter two stages of the management cycle, the input is the location index of the blocks to be read, i.e. the IDs of the sensors, and the output is the information of the blocks at the specified locations, i.e. the data collected by the sensors.

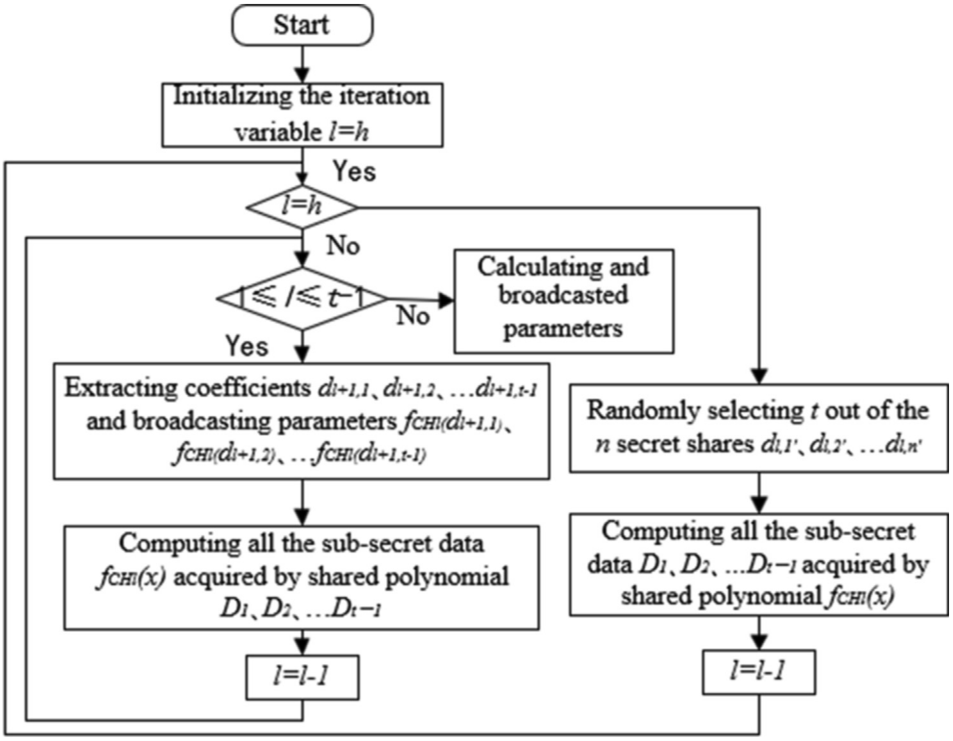

Start
Initializing the iteration variable $l=h$
Yes
$l=h$
No
$1\leqslant l \leqslant t-1$
No
Calculating and broadcasted parameters
Yes
Extracting coefficients $d_{l+1,1}$、$d_{l+1,2}$、…$d_{l+1,t-1}$ and broadcasting parameters $f_{CHl}(d_{l+1,1})$、$f_{CHl}(d_{l+1,2})$、…$f_{CHl}(d_{l+1,t-1})$
Randomly selecting t out of the n secret shares $d_{l,1'}$、$d_{l,2'}$、…$d_{l,n'}$
Computing all the sub-secret data $f_{CHl}(x)$ acquired by shared polynomial D_1、D_2、…D_t-_1
Computing all the sub-secret data D_1、D_2、...D_t-_1 acquired by shared polynomial $f_{CHl}(x)$
$l=l-1$
$l=l-1$

Fig. 5 The workflow of the restoration and reading of block data.

Each sensor checks its block in the blockchain according to $ID_{MI,j}$, and keeps requesting the IIT and then the DBS to respond to the data of the blocks with the requested IDs, until it receives the t block data. Upon receiving all the data, the sensor will start to reconstruct the initial secret.

Suppose the t sub-secrets obtained by the sensor are $d'_{l,0}$ = [ID_{CHI}', $f_{MI,l}(d'_{l+1,0})$] of the IIT, and $d'_{l,t-1}$ = [$ID'_{MI,t-1}$, $f_{MI,l}(d'_{l+1,t-1})$] of t-1 sensors. Then, each sensor will calculate its sub-secrets based on the broadcasted data and the block data in its storage.

Through Lagrange interpolation, all the sub-secret data D_1, D_2, …D_t-1 are obtained from the t-1-th order polynomial $f_{MI,l}(x)$. Finally, the sub-secrets are stitched in turn into a decimal data D, which is outputted as the reconstructed initial secret (see Fig. 5).

To verify the authenticity of the data block in each sensor, t out of n pseudo shares are selected by random for secret reconstruction.

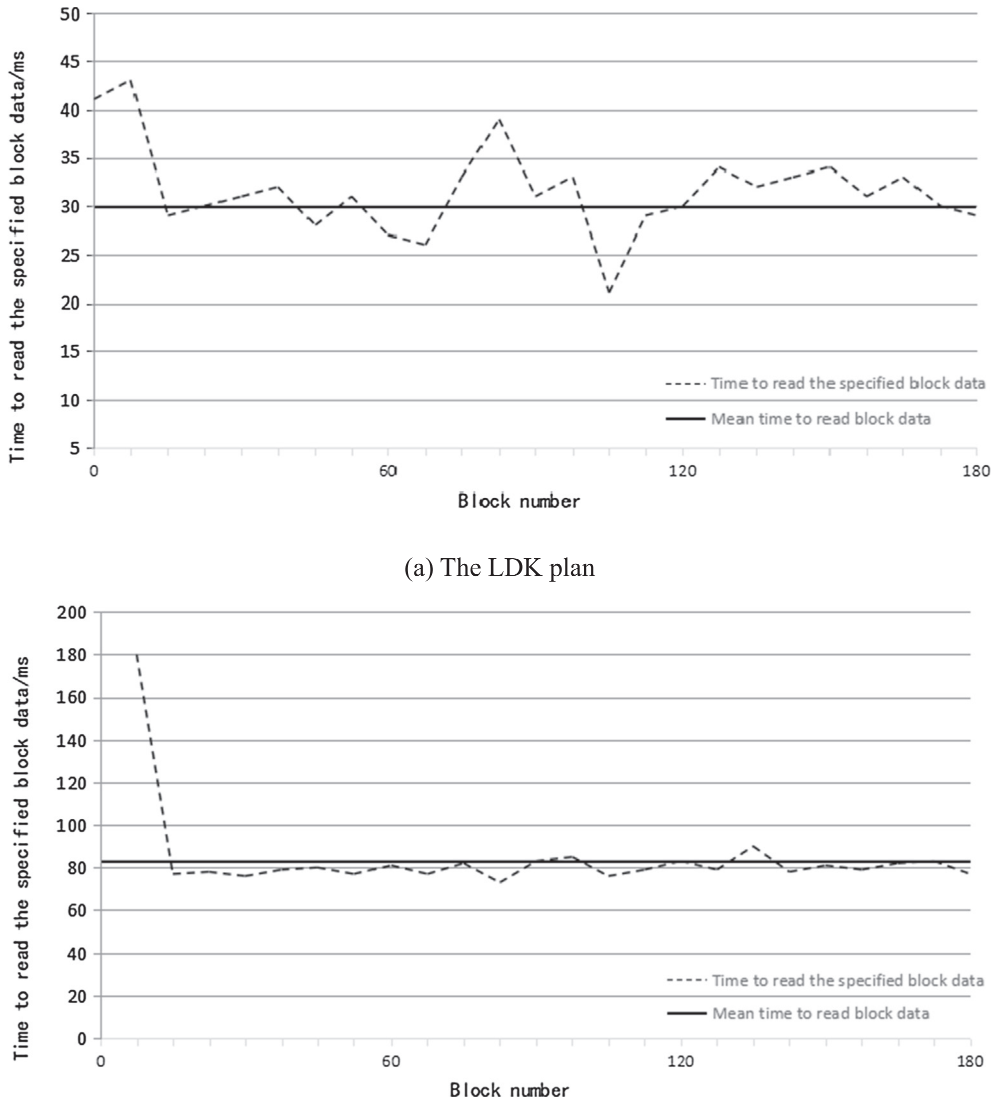
6. Simulation and results analysis

6.1. Verification of storage efficiency

The first simulation focuses on the communication between building units. A total of 20 different IITs were created locally by setting up different server ports with the computer. Each IIT supports data storage and verification, and runs its own blockchain code. The threshold parameters were set as t = 8 and n = 20.

The performance of the traditional location-dependent key (LDK), Hierarchical Key Management Scheme (HKMS)、Low Energy Adaptive Clustering Hierarchy (LEACH) management plans was compared with that of our blockchain-based dynamic key management plan, in terms of complexity, dynamics, and share length.

A total of 180 blocks were generated in the simulation. Three data were recorded during the simulation: (1) The time



(a) The LDK plan

(b) Our plan

Fig. 6 The lengths of a full management cycle of the LDK plan and our plan.

consumed by each node from receiving the data of the 20th transaction to linking the transaction data into the blockchain; (2) The time consumed to read the block data whose serial number is a multiple of 5; (3) The size of the file that records every 5 newly generated blocks.

As shown in Fig. 6, the LDK plan consumed 31 ms to complete a full management cycle, while our plan consumed 83 cm on average. Our plan is more time-consuming in communication and calculation than the LDK plan, but it can be accepted. Because it spent more time in data reading than the latter: the DBS needs to request data from the IITs that have been assigned data blocks, and the data block needs to be restored by Lagrange interpolation.

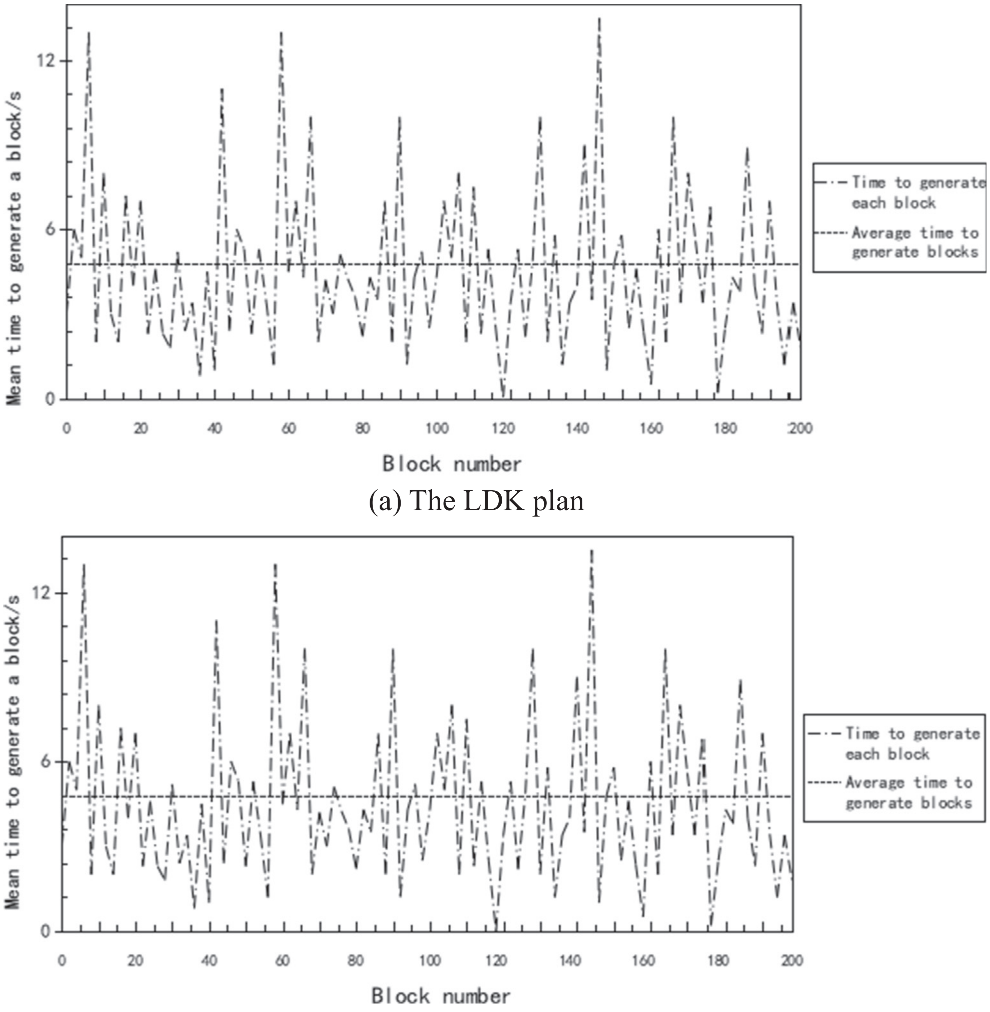
Based on the advantages of decentralization, openness, autonomy, anonymity and unforgeability of information, the introduction of blockchain technology into wireless sensor network of intelligent building energy management system can greatly improve the security and confidentiality. In terms of processing rate, as shown in Fig. 7, the LDK plan took 4.786 s on average to generate, link and verify a block, while our plan took 5.091 s. Combined with the calculation results, it can be found that the scheme is more complex in data processing, but the two plans differed slightly in the time to generate, link and verify a block. Our plan consumed slightly longer time, for the system needs to generate the secret shares to construct the block at each IIT.

As shown in Fig. 8, the lengths of shares to be stored in the IITs in the four plans increased linearly, with the growing number of blocks linked into the blockchain. The total storage space required by the IITs in the LDK plan was about 5 times that of our plan. Hence, our plan has a clear advantage in blockchain storage.

6.2. Verification of energy consumption and connectivity

Based on Visual C+ + and MATLAB, the second simulation mainly compares the energy consumption and connectivity of the two plans. A total of 100 different sensor nodes were created locally by setting up different server ports with the computer. The simulation parameters were configured as follows: area, 150 × 150; location of the DBS, (55, 200); cluster radius, 50 m; initial energy, 2J; packet size, 500Bytes.

For the LDK plan, with the increase of IITs, more messages need to be transmitted during the generation of the



(a) The LDK plan

(b) Our plan

Fig. 7 The time to generate blocks of the LDK plan and our plan.

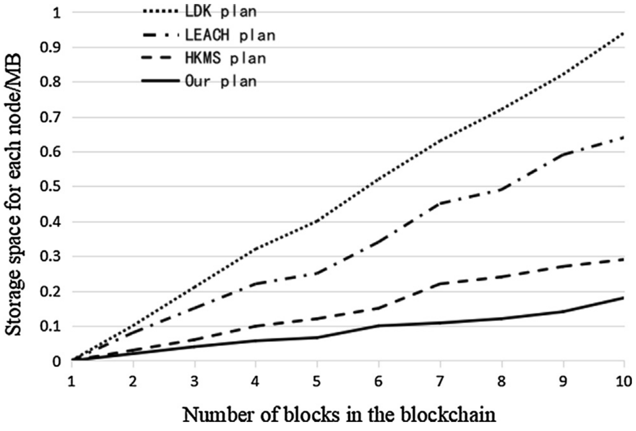


Fig. 8 The length of shares stored in the IITs of the LDK plan and our plan.

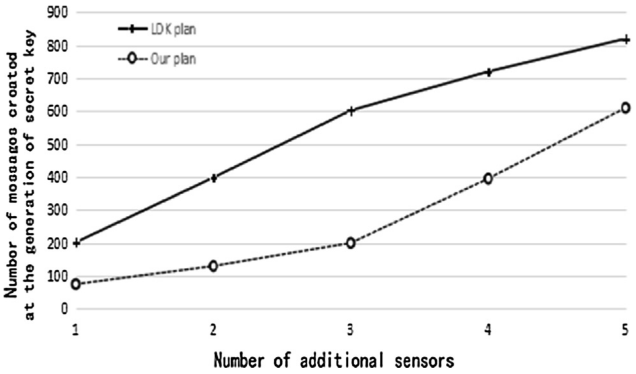


Fig. 9 Energy consumed for additional sensors of the LDK plan and our plan.

key, pushing up the energy consumption. For our plan, with the increase of IITs, the key management requires a limited number of messages. This is because some parameters are contained in block data, although the number of messages to be transmitted also increases during key generation. As shown in Fig. 9, our plan only consumed 70% of the energy needed by the LDK plan to form the secrete key management system. However, the energy consumption became obvious when there were more than 5 IITs, owing to noise and attenuation.

As shown in Fig. 10, in the same building unit, a single IIT can reconstruct the key timely, as more and more blocks are linked into the blockchain. Due to the spatiotemporal correlation of the WSN in the IBEMS, only some IITs are required to report when an event occurs. The relevant information is stored locally, which suppresses the frequency of key reconstruction. Therefore, the key update plan is feasible, suitable, lower communication costs and energy efficient.

Fig. 11 compares the network connectivity of the two plans under the same simulation environment. For the LDK plan, as the number of IITs increased, the coverage rate grew, while the attenuation increased exponentially under noise, making it difficult to forward or group messages. For our plan, all IITs are connected into a chain, such that the IITs can communicate with each other and store information locally; the cluster size could be balanced through adjustment. As a result, our plan outperformed the LDK plan in connectivity.

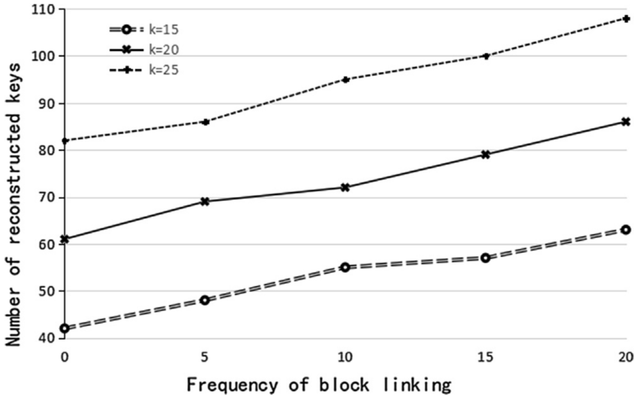


Fig. 10 Energy consumed for additional linked blocks of our plan.

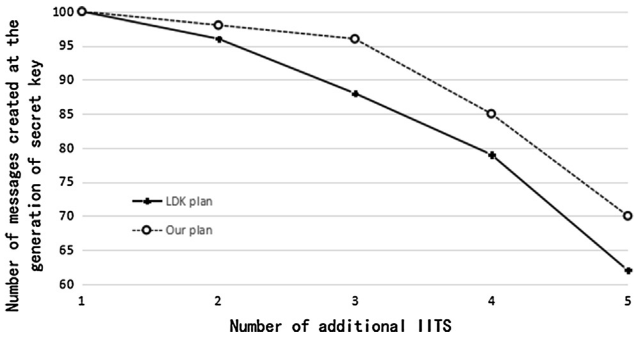


Fig. 11 Network connectivity for additional IITs of the LDK plan and our plan.

7. Conclusions

This paper analyzes the framework of the WSN in the IBEMS, and designs a network model for the IBEMS. Then, the security of blockchain technology was verified. On this basis, a blockchain-based dynamic key management plan was developed for the IBEMS.

Referring to Shamir's Secret Sharing, each management cycle in our key management plan for IBEMS was divided into six stages: initialization, generation of sub-secrets, generation of data blocks, distribution and storage of data blocks, acquisition of data blocks, and secret reconstruction.

Simulation results show that our plan inherits the high safety of blockchain technology, and excels in storage efficiency, energy consumption, and network connectivity. To promote blockchain in the UPIoT and similar scenarios, the future research will further refine the proposed plan, namely, rationalize the threshold t, and optimize the conversion of initial secret into decimal data.

Acknowledgements

Project Supported by Qinglan Project for the University Key Teacher From Jiangsu Education Department (2020), China; The Natural Science Foundation of the Jiangsu Higher Education Institutions (19KJB470018), China; The Science and Technology Project of Jiangsu Province Construction System

(2018ZD065), China; The Key Research and Development Program of the XuZhou Municipal (KC19224), China.

References

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

[2] D. Kraft, Difficulty control for blockchain-based consensus systems, Peer-to-Peer Network Appl. 9 (2) (2016) 397–413, https://doi.org/10.1007/S12083-015-0347-X.

[3] Y. Sasaki, L. Wang, K. Aoki, Preimage Attacks on 41-Step SHA-256 and 46-Step SHA-512, IACR Cryptol. ePrint Arch. 479 (2009).

[4] W. Hu, H.H. Li, Y.W. Hu, W.H. Yao, A blockchain-based spot market transaction model for energy power supply and demand network, European J. Electrical Eng. 21 (1) (2019) 75–83, https://doi.org/10.18280/ejee.210112.

[5] Z.Z. Zhang, D.J. Bi, Protection for CA Private Key Based on Secret Sharing Scheme, Comput. Syst. Appl. 20 (1) (2011) 62–65.

[6] D. Ron, A. Shamir, Quantitative analysis of the full bitcoin transaction graph, International Conference on Financial Cryptography and Data Security, Springer, Berlin, Heidelberg, 2013, 10.1007/978-3-642-39884-1_2.

[7] Y. Zhang, Energy efficiency management and route optimization for wireless sensor network under the ubiquitous power internet of things, European J. Electrical Eng. 21 (2) (2019) 217–222, https://doi.org/10.18280/ejee.210213.

[8] G. Zyskind, O. Nathan, Decentralizing privacy: Using blockchain to protect personal data, in: In 2015 IEEE Security and Privacy Workshops, 2015, pp. 180–184.

[9] M.T. Alam, H. Li, in: Patidar A: Notice of violation of ieee publication principles bitcoin for smart trading in smart grid, IEEE, Beijing, 2015, pp. 1–2.

[10] H.M. Soliman, A. Leon-Garcia, Game-theoretic demand-side management with storage devices for the future smart grid, IEEE Trans. Smart Grid 5 (3) (2014) 1475–1485, https://doi.org/10.1109/TSG.2014.2302245.

[11] A.H. Mohsenian-Rad, V.W. Wong, J. Jatskevich, R. Schober, A. Leon-Garcia, Autonomous demand-side management based on game-theoretic energy consumption scheduling for the future smart grid, IEEE Trans. Smart Grid 1 (3) (2010) 320–331, https://doi.org/10.1109/TSG.2010.2089069.

[12] M. Zeng, X. Han, R. Li, Y.F. Li, L.L. Peng, N. Li, Multi-energy synergistic optimization strategy of micro energy internet with supply and demand sides considered and its algorithm utilized, Power Grid Technol. 41 (2017) 409–418.

[13] N. Liu, X. Yu, C. Wang, C. Li, L. Ma, J. Lei, Energy-sharing model with price-based demand response for microgrids of peer-to-peer prosumers, IEEE Trans. Power Syst. 32 (5) (2017) 3569–3583, https://doi.org/10.1109/TPWRS.2017.2649558.

[14] W. Lee, L. Xiang, R. Schober, V.W. Wong, Direct electricity trading in smart grid: A coalitional game analysis, IEEE J. Sel. Areas Commun. 32 (7) (2014) 1398–1411, https://doi.org/10.1109/JSAC.2014.2332112.

[15] J. Zhang, Y.B. Li, B.X. Liu, Y.Q. Wu, H.C. Yi, Forward modelling of circular loop source and calculation of whole area apparent resistivity based on TEM, Traitement du Signal 35 (2) (2018) 183–198, https://doi.org/10.3166/TS.35.183-198.

[16] M. Sechilariu, B. Wang, F. Locment, Building integrated photovoltaic system with energy storage and smart grid communication, IEEE Trans. Ind. Electron. 60 (4) (2012) 1607–1618, https://doi.org/10.1109/TIE.2012.2222852.

[17] R. Yu, J. Ding, W. Zhong, Y. Liu, S. Xie, PHEV charging and discharging cooperation in V2G networks: A coalition game approach, IEEE Internet Things J. 1 (6) (2014) 578–589, https://doi.org/10.1109/JIOT.2014.2363834.

[18] S. Belhadj, K. Belmokhtar, K. Ghedamsi, Improvement of energy management control strategy of fuel cell hybrid electric vehicles based on artificial intelligence techniques, J. Européen des Systèmes Automatisés 52 (6) (2019) 541–550, https://doi.org/10.18280/jesa.520601.

[19] G. Carpinelli, G. Celli, S. Mocci, F. Mottola, F. Pilo, D. Proto, Optimal integration of distributed energy storage devices in smart grids, IEEE Trans. Smart Grid 4 (2) (2013) 985–995, https://doi.org/10.1109/TSG.2012.2231100.

[20] G. Ye, G. Li, D. Wu, X. Chen, Y. Zhou, Towards cost minimization with renewable energy sharing in cooperative residential communities, IEEE Access 5 (2017) 11688–11699, https://doi.org/10.1109/ACCESS.2017.2717923.

[21] W. Tushar, B. Chai, C. Yuen, S. Huang, D.B. Smith, H.V. Poor, Z. Yang, Energy storage sharing in smart grid: A modified auction-based approach, IEEE Trans. Smart Grid 7 (3) (2016) 1462–1475, https://doi.org/10.1109/TSG.2015.2512267.

[22] D.E. Olivares, C.A. Cañizares, M. Kazerani, A centralized energy management system for isolated microgrids, IEEE Trans. Smart Grid 5 (4) (2014) 1864–1875, https://doi.org/10.1109/TSG.2013.2294187.

[23] A. Askarzadeh, A memory-based genetic algorithm for optimization of power generation in a microgrid, IEEE Trans. Sustain. Energy 9 (3) (2017) 1081–1089, https://doi.org/10.1109/TSTE.2017.2765483.