Research on Security Access Control Method of Wireless Network based on Blockchain Technology

Xie Zeqiang[1], Azizol Abdullah[2], Abdullah Muhammed[3] and Masnida Hussin[4]

[1]Faculty of Computer science and Information technology

University Putra Malaysia, Serdang, Malaysia

Email: xzq01123255210@gmail.com

[2] Faculty of Computer science and Information technology

University Putra Malaysia, Serdang, Malaysia

Email: azizol@upm.edu.my

[3] Faculty of Computer science and Information technology

University Putra Malaysia, Serdang, Malaysia

Email: abdullah@upm.edu.my

[4] Faculty of Computer science and Information technology

University Putra Malaysia, Serdang, Malaysia

Email: masnida@upm.edu.my

Abstract—This study aims to address problems of large access delay and low encryption efficiency of existing wireless network access control methods. The wireless network is exposed to malicious attacks by hackers, data theft and unauthorized access. Limitations on current methods such as CP-ABE and Fuzzy encryption requires a new technique to solve the security problem. Therefore, a new wireless network security access control method based on blockchain technology is proposed. To control the security of wireless network access, this method analyzed the characteristics of the blockchain structure system and constructed a wireless network security access control model. According to the access control model, the trust level of wireless network users is divided, hence, based on the results of the trust level division, the user is authorized to access. Based on findings, the experiments are implemented to combine with the elliptic curve group and the bilinear mapping method to ensure that the wireless network security access control is accomplished. Comparative empirical results indicate that the proposed control method has less access delay and shorter encryption time, consequently having a higher practical application value.

Index Terms – blockchain technology, wireless network access control, computer network, access control.

I. Introduction

In the context of the rapid development and popularization of wireless networks and the continuous increase in network communication range, people's work and livelihoods are inseparable from wireless networks. A wireless network can no longer make people's communication limited by time and place, regardless of where people are, given nowadays, people can utilize mobile terminal equipment to access the network [1-3]. In other words, the wide application of wireless networks has promoted the development of society. Currently, the principal applications of wireless networks include wireless sensor networks, wireless mesh networks and ad-hoc wireless networks. Compared to a traditional wired network, the wireless network these days is more flexible, and the consumption of the spectrum and power is on the ground, so the development scale of a wireless network can be quickly expanded.

Wireless networks can accomplish daily data transmission, network access, and other work in helping people in gaining more convenient access to the relevant information they require. However, the security of the wireless network is also a concern. The security of accessing the wireless network is affected by a variety of factors, for instance, malicious attacks, data theft, unauthorized access, and network access tracking. Therefore, to improve the access security governing wireless networks is vital to study the benefits of effective wireless network access security control methods [4].

Visibility is the priority of access control. From patching to monitoring to isolation, visibility should be established for any device connected to the Internet. As the number of wireless network devices continues to grow, the first problem to be solved is processing speed. Access control solutions also need to be seamlessly synchronized with network and security control measures to ensure continuous tracking and uniform policy enforcement of devices and their applications across distributed networks. Access control must also be able to send device information to other secure, networked, and managed devices to baseline and monitor data flows and to identify rogue devices using techniques such as behavior analysis. An integrated security approach to access control and security policies not only provides the visibility required for security, but also enables automated processes to detect, prevent, and respond to threats.

Tu Yuanfei et.al. [5] propose a security access control method for wireless networks based on CP-ABE (Ciphertext-Policy Attribute-Based Encryption). The ciphertext

corresponds to an access structure, and the key corresponds to an attribute set, decrypted if and only if the attributes in the attribute set satisfy the access structure. This design is close to the real application scenario, which can pretend that each user obtains the key from the attribute organization according to their conditions or attributes, and then the cipher formulates the access control to the message. This method uses the revocable attribute-based on CP-ABE (Ciphertext-Policy Attribute-Based Encryption) to construct the initial construction of the access control tree of the wireless network, generating the access control [secret] key. Through the attribute and association of the encryption control algorithm towards improving the effectiveness of network access control, the wireless network security access control method is based on CP-ABE (Ciphertext-Policy Attribute-Based Encryption). However, the data throughput of applying this method is relatively low. Conversely, reference [6] suggests a wireless network security access control method based on fuzzy theory. The method uses an analytic hierarchy process to calculate the risk value of wireless network interaction tasks, constructing a fuzzy evaluation model according to the calculation results. It then uses the fuzzy evaluation model to expand the access control task of the wireless network. According to the extension processing risk of the model, the access rights are dynamically controlled, although the access delay is considerably high. In another study, reference [7] recommends an attribute-based access control method of wireless networks. According to the traceable authorization of wireless networks, the access control method of wireless networks is formulated based on attributes. Based on this scheme, a wireless network security access policy supporting arbitrary monotone linear is constructed through an encryption algorithm, though the encryption efficiency of this method is low. Therefore, aiming to address the problems associated with the methods, this article proposes a new wireless network security access control method based on blockchain technology. Based on this access control method, this method is applied to the wireless network access control of the International shipping port.

The highlight of wireless self-organization is "self-organization", which focuses on weakening the core nodes of wireless networking (decentralization), increasing the universality of nodes, enhancing security, and reducing the difficulty of networking. Decentralization is the network that does not need a core node, such as a "base station". All nodes are each "base station", and each "base station" is connected to another "base station", so that the network organized, "network breakdown" will not be caused by "single node failure". The benefit of "single node failure" is that instead of shutting down the entire network, all nodes are disable at the same duration and separated from it.

II. Wireless Network Security

A. Blockchain

With increasing security needs and requirements, blockchain technology has rapidly developed. Currently, the mainstream blockchain technology used is version 3.0, which significantly improves security. The blockchain structure is divided into five levels: the network layer, data layer, contract layer, formula layer, and application layer. The overall structure of the blockchain is illustrated in Figure 1 [8-10].

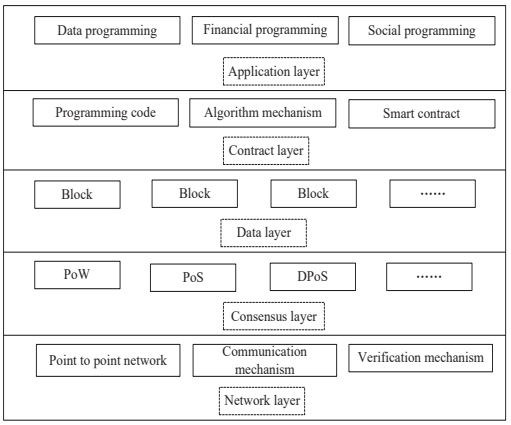

Fig. 1. Blockchain architecture.

Analysis of the blockchain architecture is shown in Fig. 1. The main distribution in the network layer is the peer-to-peer network, which this architecture is responsible for network data dissemination and access verification. The consensus layer mainly consists of several consensus mechanisms; the data layer stores network data in block form for subsequent access and call. The contract layer includes programming scripts and the intelligent algorithm, which is to encrypt the blockchain. All data is displayed at the application layer and blockchain of application scenarios [11-13].

Given the particularity of its structure, the blockchain has the characteristics associated with storage security and flexible operation, offering users a powerful logical security framework. On the premise of ensuring data security, the blockchain can lessen the time used for data transmission. The relevant characteristics of the blockchain are illustrated in Fig. 2.

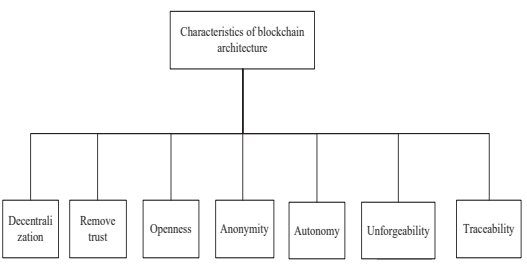

Fig. 2. Characteristics of blockchain architecture.

B. Access control

a) Characteristics of wireless network

The overall structure of the wireless network is the OSI system structure which mainly includes the data link layer, the transmission layer, and the application layer. However, different wireless networks have different structural levels. Based on acquiring the characteristics of the wireless network, it is necessary to establish the relevant factors of the wireless network security evaluation to realize better the access control of the wireless network [14-16].

In a wireless network, the security load of each transmission node is related to its previous-hop or next-hop node. The transmission diagram of the wireless network node is illustrated in Fig. 3.

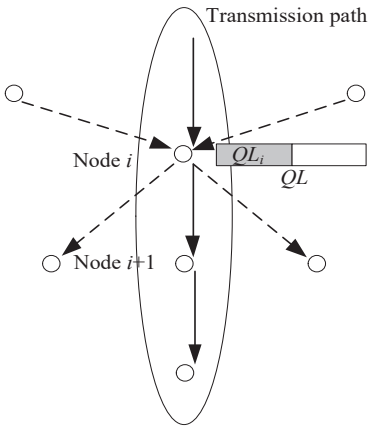

Fig. 3. Schematic diagram of wireless network node transmission.

As shown in Fig. 3, node i in a wireless network is the last hop node of node $i+1$, which is also the next-hop node of node $i-1$. When the channel state of the wireless network is stable, node i will only be affected by the data transmission of node $i+1$. Notably, when the overall receiving rate of a wireless network is greater than the sending rate, the secure transmission of wireless network data will be affected. Accordingly, the increase of load degree of wireless network nodes seriously reduces the quality of data transmission, thereby affecting the wireless network's security [17].

According to the above analysis, through a load of a wireless network node, the security degree of the wireless network node access is analyzed, and the factors such as waiting time of transmission, receiving, and sending rate are analyzed. The process of safety degree analysis is as follows:

$$\mathrm{LONLi} = \frac{\mathrm{QL_i} + \sum \mathrm{b_j \cdot ET_j} - \alpha \sum \mathrm{b_m \cdot ET_m}}{\mathrm{b_i}} \mathrm{ETX_i} \qquad (1)$$

In the formula, QL_i is the waiting time of node i; b_j is the data transmission rate of node j; α is the implicit influence factor of security; b_m is the transmission rate of node m; and b_i is the transmission rate of node i. The speed of a node and the security of a node in a wireless network are determined by the value of transmission wait time, receiving rate and sending rate, LONLi is load of a wireless network node.

According to formula (1), the data transmission rate of wireless network nodes is variable, though the limit transmission rate of different nodes is different. If the limit transmission rate of nodes in a wireless network is B_i, then the calculation formula of limit is as follows:

$$\lim_{\substack{\mathrm{b_i} \to \mathrm{E_i} \\ \sum \mathrm{b_j \cdot ET_j}}} \frac{\mathrm{QL_i} + \sum \mathrm{b_j \cdot ET_j} - \alpha \sum \mathrm{b_m \cdot ET_m}}{\mathrm{b_i}} \mathrm{ETX_i} = \mathrm{Z} \qquad (2)$$

According to formula (2), when the transmission rate of the wireless network node i is close to the limit rate B_i, the load of the last hop node of node i is large; thus, the transmission rate at this time is close to the limit value Z. As such, the access security of the wireless network is affected, regardless of whether the transmission rate of the node is adjusted or the effect of the implicit influence factor.

Consequently, wireless network security access is judged according to the transmission rate of the node and the implicit influence factor.

b) Access control model

Different wireless networks have different requirements of usage for access models. To ensure the security and integrity of access data, access control to wireless networks is performed hierarchically [18-20]. Access control at all levels of a wireless network can effectively improve the effectiveness of access control. The specific structure of wireless network security access control is displayed in Fig. 4.

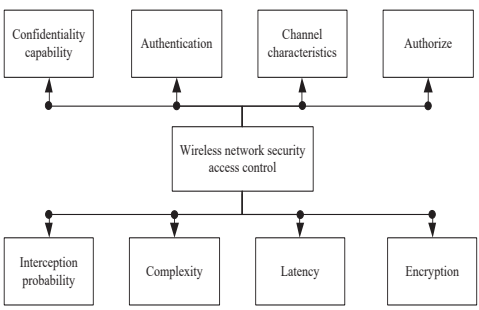

Fig. 4. Wireless network security access control.

Access control of wireless networks enhances the security of wireless networks and prevents illegal or unauthorized users and legitimate users from operating beyond their authority. Therefore, the wireless network security access control model is developed. In this model, the different permissions of wireless network access are configured, and the corresponding access rights can only access the data within the authority to avert information from being stolen. Access control is principal to determine the user's credit rating to authorize different access users. The basic model of wireless reservation access control is shown in Fig. 5.

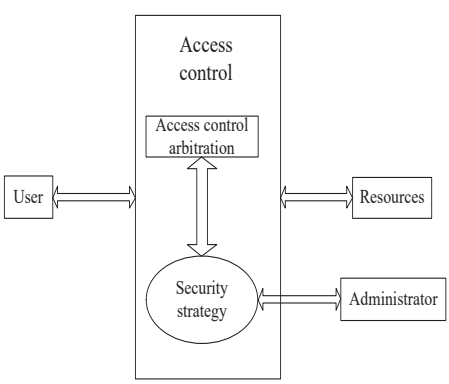

Fig. 5. The basic model of access control.

Once the basic wireless network security access control model is constructed, the user trust level is segmented. The trust level is mainly classified into trustworthy and untrustworthy, recorded as 1 and 0, respectively. The trust level mainly considers the number of DOS attacks from wireless network access. The number of attacks is inversely proportional to the trust level. The higher the number of attacks, the lower the trust level, and vice versa. For example, the number of incorrect logins of users n as an example; the trust level is divided by the value of n:

$$\begin{cases} N = 0 & \text{The trust level is 5} \\ N \in [1,3] & \text{The trust level is 4} \\ N \in [4,6] & \text{The trust level is 3} \\ N \in [7,9] & \text{The trust level is 2} \\ N \in [10,12] & \text{The trust level is 1} \\ N \in [12,+\infty] & \text{The trust level is 0} \end{cases} \quad (3)$$

The trusted value of user behavior can be expressed by a specific value. Here, the basic trusted value can be calculated by the following consensus:

$$m_i = \frac{d_i - 1}{W_i - 1} \quad (4)$$

The formula d_i represents the credit rating evaluation results of wireless network access users and W_i represents the credit rating-related data of wireless network access users, m_i represents the trusted value of user behavior.

To improve the accuracy of the calculation of the credit value, a series of user access data is marked as $(B_1, B_2, \ldots, B_{n-1}, B_n)$ by weight coefficient. For a specific behavior B_i, the weight coefficient is used to represent $t_i$where $t_i \in [0,1]$ and $\sum_{i=1}^{n} t_i = 1$; the credit rating data is used to represent W_i; the credit rating of the current behavior is represented by d_i, where $d_i \in [0, W_i - 1]$, and the trusted value is represented by M.

According to the parameter analysis result as mentioned above, the credible value M of the user requesting wireless network access is calculated, where the user's credit rating is then judged:

$$M = \frac{\sum_{i=1}^{n} t_i m_i}{\sum_{i=1}^{n} t_i} = \frac{\sum_{i=1}^{n} t_i \frac{d_i - 1}{W_i - 1}}{\sum_{i=1}^{n} t_i} \left(\begin{matrix} t_i \in [0,1], \ \sum_{i=1}^{n} t_i = 1 \\ d_i \in [0, W_i - 1] \end{matrix} \right) \quad (5)$$

The formula t_i represents the weight coefficient, and its value is judged according to the importance of wireless network access behavior, $t_i \in [0,1]$, $\sum_{i=1}^{n} t_i = 1$.

By comparing the importance of wireless network access user behavior, the importance degree results of different access behavior are acquired, and the weight coefficient is calculated according to the result.

According to the trust value calculated above, when the trust level of user access behavior is high enough, users are assigned in different degrees of access rights. There are six kinds of access trust levels in wireless networks, which correspond to different trust values. The specific corresponding relationship between them is shown in Table 1.

TABLE I
CLASSIFICATION OF TRUST LEVEL

Trust level	0	1	2	3	4	5
Credibility	Completely untrustworthy	Generally untrustworthy	Generally credible	More credible	Basically credible	Completely credible
Credible value	[0-0.1]	[0.1-0.3]	[0.3-0.5]	[0.5-0.7]	[0.7-0.9]	[0.9-1.0]

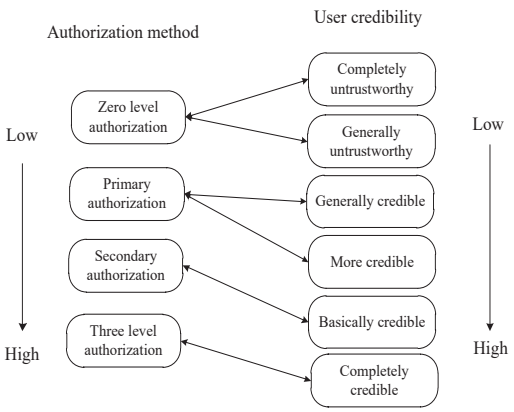

Fig. 6. Correspondence between user trust and authorization mode.

c) Encryption algorithm

The goal of this research is to ensure the security of wireless network access, in which the elliptic curve group algorithm is applied to encrypt wireless networks. In the elliptic cryptography encryption scheme, this kind of group is composed of the points on the elliptic curve. They should be Z_p^* (p is the prime number) when they are applied to wireless network encryption.

Conversely, it is challenging to solve the discrete logarithm problem in the group to ensure it is relatively safe. Most wireless network security encryption based on elliptic curve group encryption that analyze the corresponding group in a completely generalized manner without considering the specific group in the specific encryption scheme. The specific encryption process is as follows.

Let p be a prime number. Consider the equation of variables A and B:

$$y^2 = x^3 + Ax + B \bmod p \quad (6)$$

In the formula, $A, B \in Z_p$, so that equation $x^3 + Ax + B = 0 \bmod p$ has no multiple roots, A, B need to be constants in satisfying the inequality $4A^3 + 27B^2 \neq 0 \bmod p$. $\hat{E}(Zp)$ is the set of number pairs $(x, y) \in (Z_p)^2$ satisfying the above equation:

$$\hat{E}(Zp) = \{(x, y) | x, y \in Z_p \ and \ y^2 = x^3 + Ax + B \bmod p\} \quad (7)$$

The double line group is defined by $\{p, G_1, G_2, G_i, e\}$, where p is a prime number with a large value related to the security constant λ of wireless network, and G_1, G_2, G_i are multiplication operation groups of a prime number p. According to the above analysis, bilinear mapping is defined as $e: G_1 \times G_2 \rightarrow G_i$, which must satisfy the following conditions:

(1) Bilinear: the mapping e is bilinear, if for any $g_1 \in G_1$, $g_2 \in G_2$ and $a, b \in Z_p$ the equation $e(g_1^a, g_2^b) = e(g_1, g_2)^{ab}$ holds.

(2) Non degeneracy: if there is $g_1 \in G_1$, $g_2 \in G_2$ such that $e(g_1, g_2) \neq 1$ $1 \in G_i$, then it is not orthogonal.

(3) Measurability: there is $g_1 \in G_1$, $g_2 \in G_2$, using the wireless network security constant p to construct the probability polynomial to calculate $e(g_1, g_2)$.

If $G_1 = G_2$ the bilinear group is referred to as the symmetric bilinear group; otherwise, it is called the asymmetric bilinear group.

At the same time, bilinear mapping has the following properties:

(1) For any $g, h, g_1 \in G_1$, there is $e(g, h, g_1) = e(g, g_1)e(h, g_1)$.
(2) For any $g, h, g_1 \in G_1$, there is $e(g_1, g, h) = e(g_1, g)e(g_1, h)$.
(3) $e(g^a, g^b) = e(g, g)^{ab} = e(g^b, g^a)$.

By the above calculations, block-based chain structure, to build a wireless network access control model, using an algorithm and the elliptic curve group bilinear mapping of a combination of the radio access network is encrypted, improving the wireless network security access, and complete the access control procedure.

III. Experimental Verification

The above process investigated the control method from a theoretical perspective. Here, the actual application performance of the control method needs to be verified for a comparative verification to be undertaken. The experimental data is sqlserver2008, the operating system is Windows 7, and the software used is Visual Studio 2012. The specific experimental parameter setting results are shown in Table 2.

TABLE II
Experimental Parameters

Parameter	Numerical value
Number of CCH/SCH channels	1/6
Channel rate	6 Mpbs
SIFS	10 us
Service message length	100 bits
Number of nodes	70
Routing protocol	AODV
Node mobility rate	60 m/s
Network area	1000 m*1000 m

A comparative verification experiment is conducted under the constraints of the above experimental environment and experimental parameters. The overall scheme of the experiment is as follows: the proposed method is compared with reference [6] (based on the fuzzy theory method) and reference [7] (based on the attribute method) with throughput, access delay, and encryption efficiency as the comparative indicators.

a) Throughput comparison

Throughput refers to the ability of the wireless network to process data. The higher the throughput, the higher the control performance. The throughput comparison results of the four methods are shown in Fig. 7.

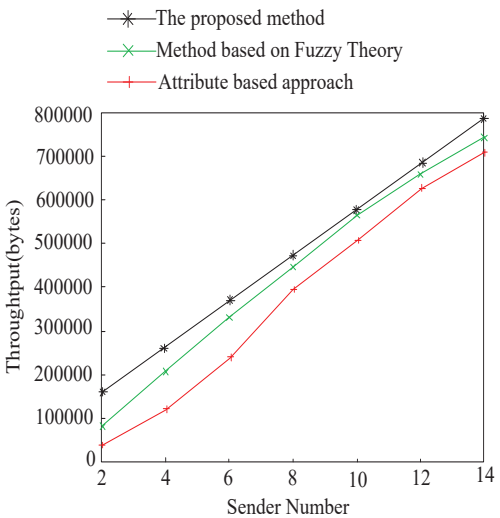

Fig. 7. Throughput comparison results

The throughput comparison results in Fig. 7 show that the throughput of the proposed method is always higher than fuzzy and attribute approach comparison methods when the number of transmitters continues to increase. When the number of senders reaches 14, the throughput of the proposed method reaches 790000 bytes, whereas that of the fuzzy theory-based method is 730000 bytes, and that of the attribute-based method is 700100 bytes.

b) Access delay comparison

The access delay comparison results of the three methods are shown in Fig. 8.

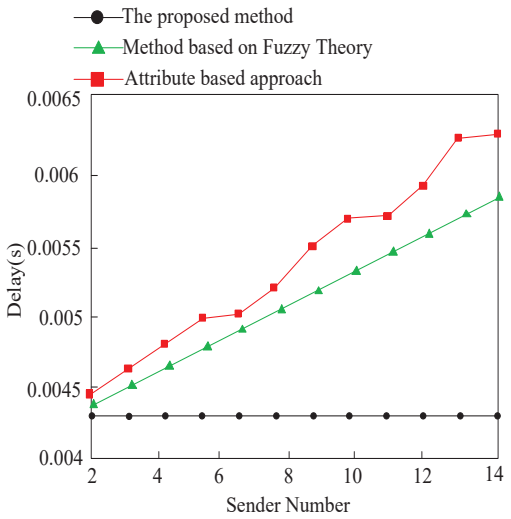

Fig. 8. Access delay comparison results

As observed from the comparison result of the access delay in Fig. 8, the proposed method is continually lower than the access latency of the two kinds of comparative literature methods and substantially the absence of fluctuations. When the number of transmitters increases, the access delay of the proposed method is constantly kept at 0.0043s, while the access delay of the two literature comparison methods is continually rising; therefore, it demonstrates that the proposed method has a low access delay.

c) Encryption efficiency

The comparison results of encryption efficiency of the three methods are shown in Fig. 9.

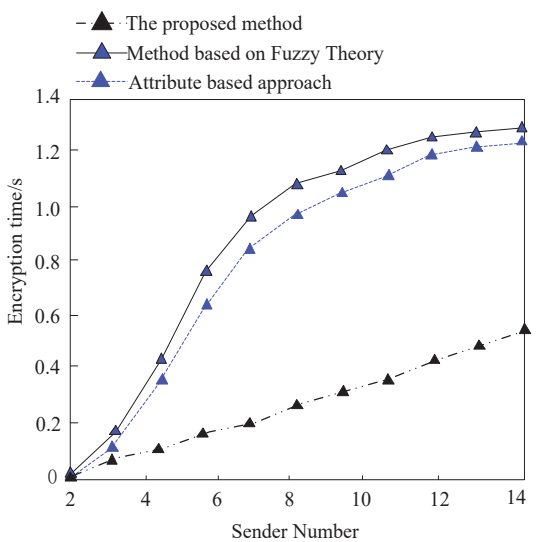

Fig. 9. Comparison results of encryption efficiency

Corresponding to the experimental results of the encryption efficiency comparison in Fig. 9, the encryption time of the proposed method is the shortest. When there are 14 transmitters, the encryption time of the proposed method is only 0.57 s. In contrast, the encryption time based on the fuzzy theory method and attribute method reach 1.29 s and 1.19 s, respectively. Therefore, the proposed method has higher encryption efficiency.

IV. Conclusion

To improve the security of wireless networks, a new wireless network security access control method is proposed in this study based on blockchain technology. The following conclusions are proven from both theoretical and experimental perspectives. This method has lower access delay and higher encryption efficiency in wireless network security access control. Specifically, compared to the control method based on fuzzy theory, the access delay is significantly reduced, and the access delay is always kept at 0.0043s; compared to the control method based on an attribute, the encryption efficiency is significantly improved, where the maximum encryption time is only 0.57s. Therefore, the proposed control method based on blockchain can better meet the requirements of wireless network security access control.

References

[1] Ding Ying, Huang Jihai and Ma Wenyue. “Design of security auto-identification system based on CA technology for wireless sensor networks”, Modern Electronics Technique, vol. 42, no. 2, pp. 54-61, 2019.

[2] Nie Liying and Wang Tingting. “Secure Access Control Algorithm for Wireless Sensor Network”, Microelectronics and Computer, vol. 34 no. 11, pp. 124-127, 2017.

[3] Li Mingfei, “Multi-channel Access Control Simulation of Self-organizing Network Based on Blockchain”, Computer Simulation, vol. 36, no. 5, pp. 480-483, 2019.

[4] Liu Haitao and Yang Qiong, “Research on secure access control of office resources in mobile cloud service environment”, Machine Tool and Hydraulics, vol. 46, no. 12, pp. 134-138, 2018.

[5] Tu Yuanfei, Gao Zhenyu and Li Rongyu, “Removable Attribute Encryption Access Control Algorithm Based on CP-ABE”, Computer Science, vol. 45, no. 11, pp. 176-179, 2018.

[6] Liu Hao, Zhang Lianming and Chen Zhigang, “Task-based access control mode of peer-to-peer network based on fuzzy theory”, Journal on Communications, vol. 38, no. 2, pp. 44-52, 2017.

[7] Li Qi, Zhu Hongbo and Xiong Jinbo, “Multi-authority attribute-based access control system in mHealth with traceability”, Journal on Communications, vol. 39, no. 6, pp.1-10, 2018.

[8] Yin Xueyuan, Chen Xingshu and Chen Lin, “Research on Security Domain and Access Control Model for Virtualization IaaS Environment”, Journal of Chinese Computer Systems, vol. 40, no. 1, pp. 111-116, 2019.

[9] Lei Linan and Li Yong, “CP-ABE based data access control scheme with multi-authorities”, Application Research of Computers, vol. 35, no. 1, pp. 248-252, 2018.

[10] Zhang Dafang, Xu Hongyue and Li Rui, “Privacy Preserving kNN Query Protocol for Wireless Body Sensor Networks”, Journal of University of Electronic Science and Technology of China, vol. 46, no. 5, pp. 722-727, 2017.

[11] Ma Mingxin, Li Fenghua and Shi Guozhen, “ECC based hierarchical key management scheme for perceptual layer of IoT”, Journal on Communications, vol. 39, no. S2, pp. 5-12, 2018.

[12] Li Qi, Xiong Jinbo and Huang Lizhi, “Attribute-based access control scheme in smart health”, Journal of Computer Applications, vol. 38, no. 12, pp. 3471-3475, 2018.

[13] Yang Tengfei, Shen Beisong and Tian Xue, “Access Control Mechanism for Classified and Graded Object Storage in Cloud Computing”, Journal of Software, vol 28, no. 9, pp. 2334-2353, 2017.

[14] Zhou Bo and Wang Shulei, “An inter-domain access control scheme for software defined network based on attribute-based encryption”, Chinese High Technology Letters, vol. 30, no. 4, pp. 43-53, 2020.

[15] Fang Liang, Yin Lihua and Li Fenghua, "Spectral-clustering-based abnormal permission assignments hunting framework", Journal on Communications, vol. 38, no. 12, pp. 63-72, 2017.

[16] Li Min and Yu Shi, "Application of UCON Based Improved Model in Virtual Access Control of Cloud Environment", Science Technology and Engineering, vol. 18, no. 21, pp. 87-92, 2018.

[17] Tan Yuesheng, Ning Yusheng and Wang Jingyu, "Research of cloud data access control based on Purpose-Based Access Control and Attribute-Based Encryption", Computer Engineering and Applications, vol. 54, no. 13, pp. 123-128, 2018.

[18] Yan Min, Zhang Yinghui and Zheng Dong, "Flexibly Accessed and Vaguely Searchable EHR Cloud Service System", Computer Science, vol. 45, no. 10, pp. 172-177, 2018.

[19] Shi Jinshan, Li Ru and Song Tingting, "Blockchain-based access control framework for Internet of things", Journal of Computer Applications, vol. 40, no. 4, pp. 931-941, 2020.

[20] Su Mang, Shi Zhenguo and Fu Anmin, "Proxy re-encryption based multi-factor access control scheme in cloud", Journal on Communications, vol. 39, no. 2, pp. 96-104, 2018.

[21] O. Alphand, "IoTChain: a blockchain security architecture for the internet of things", IEEE Wireless Communications and Networking Conference (WCNC), Barcelona, pp. 1–6, 2018.

[22] G. Bianchi, A.D. Stefano, C. Giaconia, L. Scalia, G. Terrazzino and I. Tinnirello, "Experimental assessment of the back of behavior of commercial" IEEE 802.11b network cards, in: In Proc. of IEEE INFOCOM 2007.

[23] M. Conoscenti, A. Vetrò and J.C. De Martin, 'Blockchain for the internet of things: a systematic literature review", in: 2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA), 2016.

[24] L. Ghiro, L. Maccari and R.L. Cigno, "Proof of networking: can blockchains boost the next generation of distributed networks?", in: 2018 14th Annual Conference on Wireless On-demand Network Systems and Services (WONS), Isola, 2018, pp. 29–32.

[25] M.T. Hammi, P. Bellot and A. Serhrouchni, "BCTrust: a decentralized authentication blockchain-based mechanism", in: 2018 IEEE Wireless Communications and Networking Conference (WCNC), Barcelona, 2018, pp. 1–6.

[26] D.B. Rawat and A. Alshaikhi, "Leveraging distributed blockchain-based scheme for wireless network virtualization with security and QoS constraints", in: 2018 International Conference on Computing, Networking and Communications (ICNC), Maui, HI, 2018, pp. 332–336.

[27] M. Selimi, A.R. Kabbinale, A. Anwaar, L. Navarro and A. Sathiaseelan, "Towards blockchain-enabled wireless mesh networks", in: Proceedings of the 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems (Cry- Block'18), ACM, New York, NY, USA, 2018, pp. 13–18.

[28] P. Patras, H. Feghhi, D. Malone and D.J. Leith, "Policing 802.11 MAC misbehaviours", IEEE Transactions on Mobile Computing, vol. 15, no. 7, pp. 1-14, 2014.

[29] S. Nakamoto, "Bitcoin: a p2p electronic cash system", 2009.

[30] M. Jakobsson and A. Juels, "Proofs of work and bread pudding protocols (extended abstract)", in: B. Preneel (Ed.), Secure Information Networks, The International Federation for Information Processing, vol. 23, Springer, 1999.

[31] A. Brincat, A. Lombardo, G. Morabito, and S. Quattropani, "On the use of Blockchain technologies in WiFi networks", Computer Networks, vol. 162, 106855, 2019.