Eng Int Syst (2022) 6: 453–463

Engineering
Intelligent Systems

Security Optimization of Convergence Nodes in the Sensing Layer of the Power Internet of Things Based on Fuzzy Clustering

Tong Li[2], Yang Liu[2], YaoDong Tao[1,*], DongHua Huang[1], Hongbi Geng[2] and Qian Sun[2]

[1] *Liaoning Electric Power Research Institute,Liaoning 110055,China*
[2] *Beijing DualPi Intelligent Security Technology Co. Ltd, Beijing 100088, China*

The use of computer networks has made daily life more convenient. However, malicious attacks and data theft by attackers with ulterior motives plague a large number of Internet users and data security is an urgent need. In this context, this article studies the security optimization of the sensory layer convergence node of the Power Internet of Things using the clustering algorithm to make it more reliable. Therefore, this paper proposes to improve the clustering algorithm through the improved type-2 fuzzy C-means clustering algorithm to explore data security, and design a simulation experiment, and through the three different attack modes of RFID system defense, the intrusion capability is compared, and the optimal type-2 fuzzy C-means clustering algorithm is obtained. The improved algorithm improves the system's anti-intrusion success rate by 50%, which can well protect the computer network and protect user data.

Keywords: Fuzzy Clustering Algorithm, Power Internet of Things, Internet of Things Perception Layer, Convergence Node Security Optimization

1. INTRODUCTION

The number of computer networks in the world is increasing every day. These growing networks are all directly or indirectly connected to the Internet. There is no doubt that access to the Internet greatly increases the access to and exchange of information and the resulting opportunities. However, with the increase in opportunities, various types of networks will face diverse dangers, such as online theft and obstruction due to the widespread connection of the Internet. Attackers may change 'a user's homepage in a prank, implement a denial-of-service attack or carry out other attacks. When technology reaches a certain level, an attacker can eavesdrop on network information such as user passwords and database information, tamper with database content, and forge user IDs. Moreover, attackers may destroy database content, network nodes, computer virus releases, etc. Computer network security has become a major issue affecting national independence and security, economic operation and development, and social stability and prosperity.

Network security is an important part of information security. However, as a new technology that integrates high-precision technologies such as computers and communications, computer networks have penetrated all fields of the information society, and computer networks have become the main carrier and dissemination tool of modern social information. The computer cannot be separated from the network, and the network is carried by the computer. Therefore, in a certain sense, network security is information

*Address for correspondence: YaoDong Tao, Liaoning Electric Power Research Institute; Liaoning 110055, China, Email: taoyaodong@dualpi.com.

security. The most extensive research which has been conducted on network security is the security optimization of the aggregation node of the perception layer of the Internet of Things. With the continuous expansion of the scale of the Internet of Things, the types of devices connected to it continue to increase, and all types of devices need to collect the data they collect. Furthermore, the number of devices in the Internet of Things has also increased exponentially. The total amount of data that needs to be transmitted in the network has increased sharply, resulting in an increase in network load. Massive data not only affects the transmission rate, it creates the urgent need to consider data security issues.

With the globalization of the network brought about by the development of science and technology, some ulterior motives of network security attacks have come along, making more and more network users suffer. To solve this problem, more people start Invested in the work of security optimization, in which the clustering algorithm is used most frequently and reliably for information security optimization. For example, to discover the detailed information contained in infrared images, Zhou proposed an intuitive fuzzy entropy clustering algorithm for image segmentation. Due to the fuzzy characteristics of infrared images, an intuitive fuzzy set is selected for infrared image segmentation. The conditions of the intuitionistic fuzzy entropy clustering algorithm are studied. An iterative algorithm is derived to calculate the Lagrangian multiplier coefficient and the degree of membership. Finally, the experiment results prove the ability of the intuitionistic fuzzy entropy clustering algorithm to segment infrared images [1]. Although this document studies the use of image segmentation technology, the author's use of fuzzy clustering algorithms is still worth learning. Aminanto ME's attacks on computer networks are developing rapidly. Traditional intrusion detection systems based on pattern matching and static signatures have obvious limitations, so they proposed ACA to determine clusters. The fuzzy method is used to detect anomalies in the new monitoring data by combining two distance-based methods. The results show that, compared with several traditional and new technologies, the proposed hybrid method achieves a higher detection rate and a lower false alarm rate [2]. It also involves research on network security technology. This article still has absolute reference value for the research topic of this article. Karunambigai et al. [3] proposed algorithms for clustering fuzzy graphs (FG) and intuitionistic fuzzy graph (IFG) vertices. These algorithms are based on the edge density of a given graph and the authors applied the algorithm to practical problems to derive the most prominent clusters. Also, the parameters of the intuitionistic blur graph are introduced [3]. Although the idea is very good, the article is mainly based on the theoretical basis to explore, and does not consider the reliability of the conclusion through the actual experimental area. Lee proposed a method of combining separate moving objects into one moving object using the FCM clustering algorithm to solve the problem of moving objects lost in the process of moving objects extraction. In the proposed method, the color histogram is extracted from the feature information of each moving object, and the histogram is continuously accumulated to avoid being sensitive to noise or changes. When multiple moving objects overlap and separate, the color histogram is stored compared each other to correctly identify each moving object [4]. This article details the design of the experiment clearly, and it is worth learning. Kesemen [5] states that cluster analysis is a useful tool commonly used in data analysis. The purpose of cluster analysis is to divide data sets into subsets based on their similarities and differences. Different to other methods, FCM4DD uses angle difference as a similarity measure. Therefore, the proposed algorithm is a more consistent clustering algorithm than other algorithms. The main advantage of FCM4DD is that the proposed method is actually a non-distributed directional data clustering method. Kesemen et al.'s work presents a relatively in-depth study of fuzzy clustering analysis algorithms which can assist our research on security optimization. Caytan [6] proposes a novel collaborative design paradigm for antenna collectors for wireless nodes operating in an IoT environment. This strategy results in a compact and highly integrated unit capable of establishing a reliable and energy-efficient wireless communication link and collecting energy from up to three different sources at the same time. To demonstrate this method, two different SIW cavity-backed slot antennas and a new compact dual linearly polarized SIW antenna are introduced. These topologies help to integrate additional hardware without degrading performance. The study of the Power Internet of Things is also important. This article optimizes the integration unit by designing it. Jiang [7] proposed a light-weight Power Internet of Things data security protection method for security problems caused by the rapid increase in the amount and frequency of a large number of new advanced metering system equipment access and new business data interaction. First, based on the "cloud-side-side" AMI system architecture a multi-level anonymous authentication method is proposed, and a lightweight data packet reassembly protocol is introduced. The work in [7] is roughly consistent with the research content of this article, and we can draw on the author's experience in the process of inquiry. To improve the reliability and continuity of the power distribution system, Kong built a Power Internet of Things analysis and monitoring system and proposed a fault location method that considers the distributed phasor measurement unit (D-PMU) information and the symmetry characteristics of the network. According to the load symmetry of the distribution network, different positioning algorithms are obtained. For the three-phase symmetric system, a fault location method based on line distribution parameters is adopted, and a fault location method based on line impedance is proposed for a three-phase asymmetric system [8–9]. The above documents mainly focus on the research of fuzzy clustering algorithm and the Power Internet of Things, but they have not been combined to optimize security.

The innovation of this paper is to improve the fuzzy clustering algorithm. The improved fuzzy clustering algorithm is used in the security optimization of the sensing layer of the Power Internet of Things to discuss the improvement of its security performance, and to design a simulation experiment to RIFD. The anti-intrusion effect of the system under three different attack modes is compared, and the most suitable type-2 fuzzy C-means clustering algorithm is summarized,

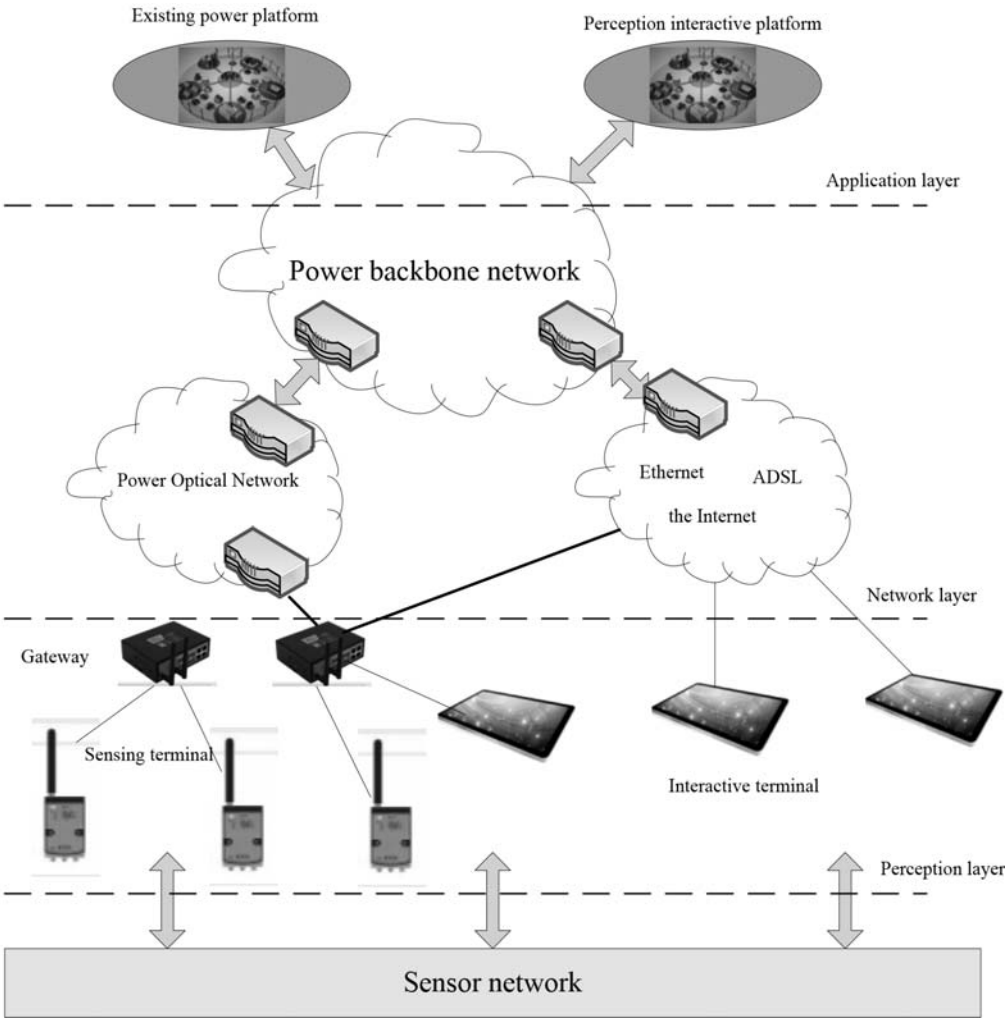


Figure 1 The main structure diagram of the Power Internet of Things.

which can greatly improve the security protection ability of the system and has significant research value.

2. SAFETY OPTIMIZATION METHOD

2.1 Power Iot Perception Layer System Architecture

As the development of the Internet of Things has risen to the height of national strategy, several unique security problems relating to the Internet of Things have also become prominent. Since the Internet of Things inherits, to a large extent, the things of the original Internet network, there are several existing security problems of the Internet. The first is that the terminal is unattended, and the equipment security and communication channel security cannot be guaranteed; the second is the massive number of terminal nodes which has a great impact on the application of the Internet of Things. Due to the huge number, due to economic feasibility considerations, the price of a single terminal is bound to be very low, leading to restrictions on the resources and capabilities of most terminals in IoT applications, such as power supply, storage, and computing; third, diversified communication terminal forms; fourth, combining the original communication network with things The integration of networked perception networks; fifth, the application of the Internet of Things is more extensive [10]. The main structure of the Internet of Things is shown in Figure 1:

Due to the aforementioned characteristics of the Internet of Things, the Internet of Things has some special security issues that are different from Internet security issues, as follows.

The first is the local security problem of terminal equipment at the perception layer of the Internet of Things [11]. Due to the application requirements of the Internet of Things, its perception layer devices are mostly deployed in an unattended and monitored environment. Attackers or criminals can easily access these devices to steal or destroy them.

Secondly, in most cases, the information on the Internet of Things depends on wireless transmission. The transmission signal may be intercepted and cracked, causing the leakage of communication content. At the same time, because the Internet of Things has a large number of terminal nodes, a large number of centralized communications may occur if data is sent at the same time, and a denial of service attack may occur due to network congestion [12].

The third is the business security issue of the Internet of Things. Since the nodes of the Internet of Things terminal

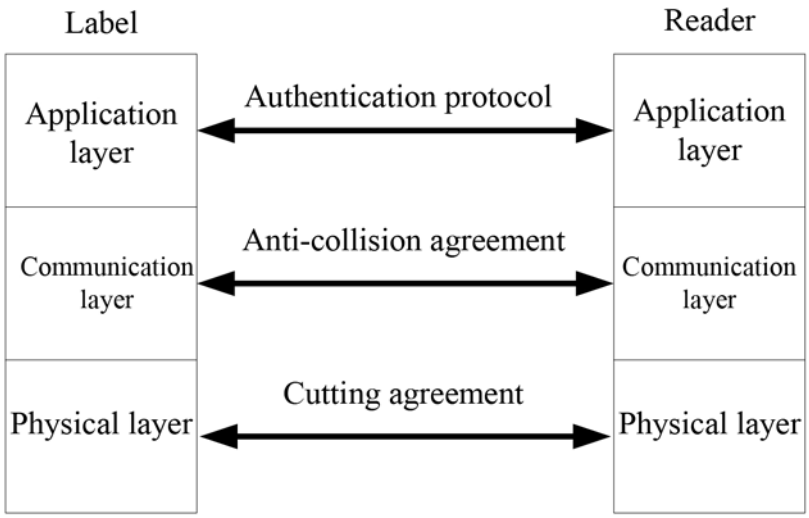


Figure 2 Reader and tag communication model.

are not managed by anyone and may exist dynamically, the security of the Internet of Things business information configuration link cannot be guaranteed, and the security of the remote contracting process of the equipment cannot be guaranteed under the Internet of Things application. At the same time, the existing communication network is constructed from the human-to-human communication demand mode in terms of security, and is not completely suitable for the secure communication between things and devices and devices under the Internet of Things.

Finally, there are personal privacy and security issues. Because radio frequency identification technology is a very important technology in the Internet, privacy and security issues exist in the radio frequency identification system. This is because items or personal information are placed in the tag, and the attacker intercepts the tag and the reader. If the user makes a call or breaks a label, they may get items or personal information, causing personal privacy or item information to be leaked.

For the perception layer, its security issues can be classified into three categories: local device security, personal privacy security, and information transmission security. Of these, the latter two security issues are reflected in the two main categories of the IoT perception layer, namely Technology-RFID technology and wireless sensor network technology [13–14]. The communication model of the radio frequency system is shown in Figure 2:

The communication model between the reader and the electronic tag has 3 layers. The highest layer is the application layer, and the design of the security authentication protocol of the radio frequency identification system is aimed at this layer. The communication layer is located between the application layer and the physical layer. It is a transition between the two layers and the communication layer must handle readers and multiple tags and conflict prevention problems in communication. The physical layer is at the bottom, and the cutting protocol of this layer can solve the problem that the same reader is compatible with multiple tags [15].

2.2 Classification of Intrusion Detection Systems

(1) On the basis of host intrusion detection, through a single host, obtain his log information, and use this to understand his activities, and analyze them to detect whether there has been an intrusion recently, the most important of which is the intrusion operation of the Internet is carried out through the host computer. The logical view of HIDS is shown in Figure 3.

The advantages and disadvantages of the host intrusion detection system:

Relatively speaking, the benefits of host intrusion can be analyzed in advance of upcoming attacks. Such analysis data is clearer. The error detection rate is low, and, in this case, the monitoring process of the host is simpler, and the complexity of the system is also reduced. The disadvantage is usually that it is installed on the equipment that needs to be protected. As a result, the efficiency of the application system is reduced and additional security issues will arise, depending on the inherent log and monitoring. The function of the server will result in an unexpected performance impact to the running commercial system [16].

(2) Network-based intrusion detection system

Through data analysis under certain restrictions, the protocol attack can be identified and discovered, and the program can be started to identify its possible behavior characteristics and determine whether there is an intrusion behavior [17–18]. The logical view of the network-based intrusion detection system (NIDS) is shown in Figure 4.

Advantages and disadvantages of the network intrusion detection system:

The advantage is that these attacks from the network can be detected, and illegal access beyond the permission can be detected. The network intrusion detection system does not need to change the configuration of the server or other hosts. The disadvantage is that it can only check communication with the directly connected network segment, and cannot detect network packets in different network segments.

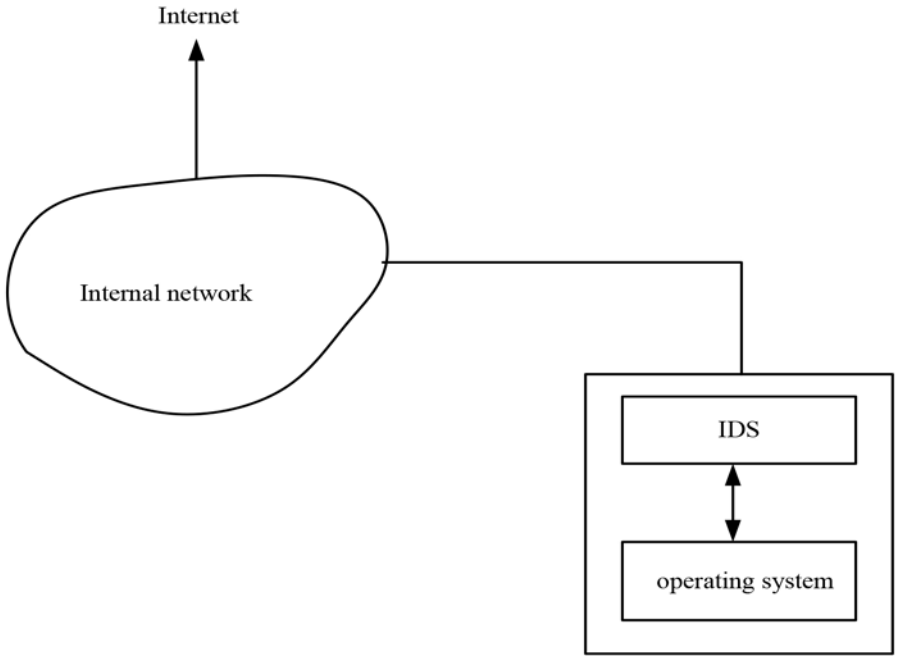


Figure 3 HIDS logical view.

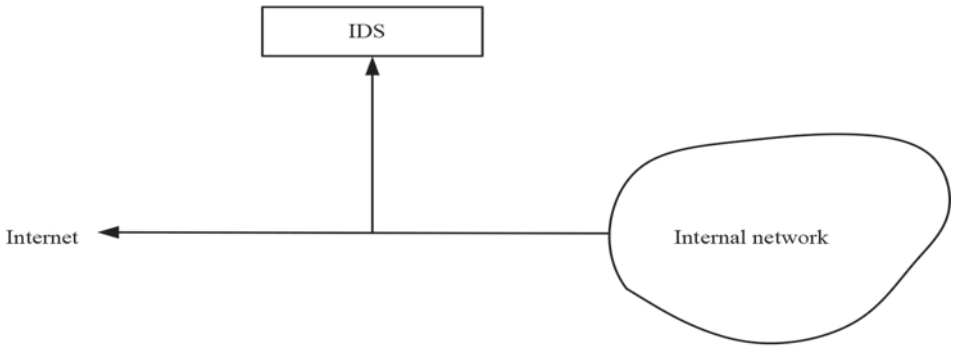


Figure 4 NIDS logical view.

Advantages and disadvantages of the distributed intrusion detection system:
The distributed intrusion detection system (DIDS) belongs to the network IDS, but the distributed architecture is being further developed. DIDS configures multiple detection nodes in various places in the network, collects and organizes information according to established rules, and sends it to the central control node. The central master control node analyzes and judges the information according to the rules, and makes judgments about intrusion attacks based on this. Figure 5 shows the logical view of DIDS.

Information is collected in multiple network segments and the information is used to run intrusion detection through the middle connection node. In this way, the monitoring efficiency of the system can be better improved, and multiple monitoring can be run at the same time. Precisely because of this, the monitoring behavior is too dependent on the master node, which shows that as long as the intrusion behavior attacks the master node, it can crash the entire system [19]. This is also the reason why DIDS is not safe.

2.3 Improved Fuzzy c-Means (FCM) Clustering Algorithm

(1) FCM algorithm

The FCM clustering algorithm has been successfully and widely used in various research fields such as intrusion detection and numerical analysis. The FCM algorithm completes the task of classifying data without generic labels by minimizing and optimizing to solve the objective function based on a certain clustering prototype and a certain norm. The basic idea of the FCM clustering algorithm [20] is as follows:
Let $W = \{W_1,\ W_2, \cdots W_x\} \in R_y$ represent a given sample set, where x represents the number of samples, y represents the dimension of the sample space, and $c(c > 1)$ represents the division of W clusters quantity. The FCM algorithm can be explained as follows.

$$J_{fcm}(U, V) = \sum_{i=1}^{c} \sum_{j=1}^{x} u_{ij}^{m} d_{ij}^{2} \tag{1}$$

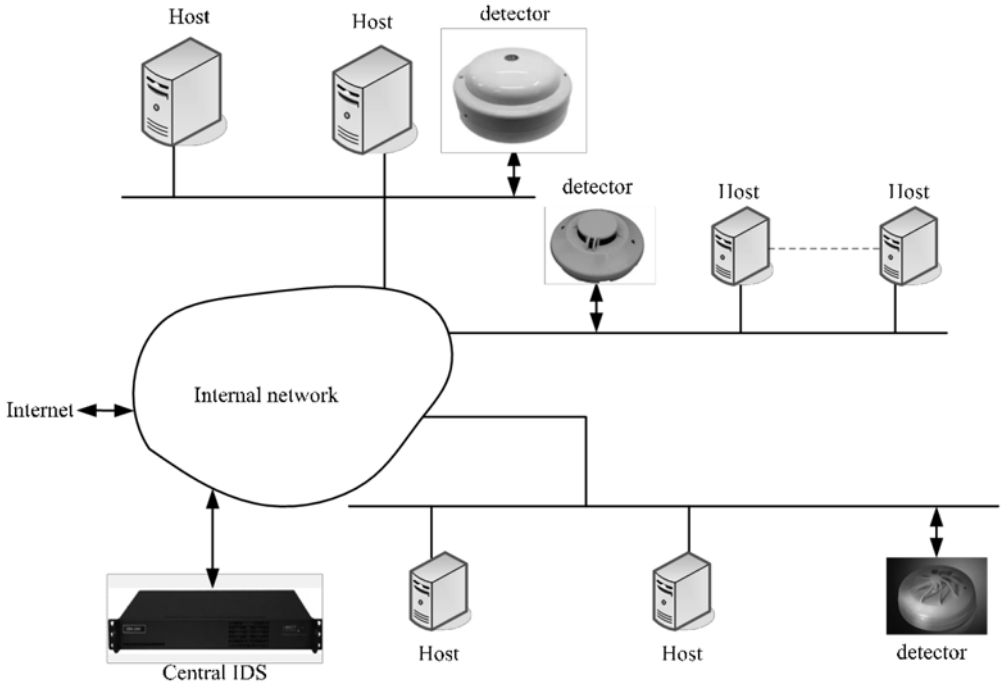


Figure 5 DIDS logical view.

where

$$\sum_{i=1}^{c} u_{ij} = 1, 1 \le j \le x \tag{2}$$

$$\sum_{j=1}^{x} u_{ij} > 0, 1 \le i \le c \tag{3}$$

$$u_{ij} \ge 0, 1 \le i \le c, 1 \le j \le x \tag{4}$$

The calculation formulas of membership degree Uij and cluster center Vi in the iterative process in formula (3) are shown in formula 5 and formula 6 respectively:

$$u_{ij} = \left[(d_{ij})^{1/m-1} \sum_{r-1}^{c} \left(\frac{1}{d_{rj}} \right)^{1/m-1} \right]^{-1} \tag{5}$$

$$v_i = \frac{\sum_{j=1}^{x} u_{ij}^m n_j}{\sum_{j=1}^{x} u_{ij}^m} \tag{6}$$

In this paper, the average value of the sum of distance pairs between all objects in the data set is used as the threshold radius r, as shown in Equation 7.

$$r = \frac{\sum_{i-1}^{x-1} \sum_{j=i+1}^{x} |n_i - n_j|}{x(x-1)/2} \tag{7}$$

Thus, the point density value of each object within the threshold radius r is calculated:

$$Minpts = \frac{\sum_{i=1}^{X} \rho_{n_1}}{X} \tag{8}$$

Then, calculate the value of MinPts according to formula 8, and judge the cluster center from this.

3. IMPROVED FCM ALGORITHM EXPERIMENT

3.1 The Security and Privacy of the Rfid System in the Perception Layer of the Internet of Things

The security of RFID mainly focuses on protecting the business secrets of enterprise users, protecting the privacy of individual users, preventing attacks on the RFID system, and security countermeasures using RFID technology. An important countermeasure to solve RFID security is to design more complex microprocessors and large-capacity memory. Then, more complex encryption algorithms are installed on the RFID to prevent incorrect data leakage. The method to improve the security of RFID tags is the main direction of our research [21].

Because RFID tags have a longer scanning range, there are no various attacks, including authentication and copies, which may be scanned by malicious readers. Therefore, in order to ensure privacy and authentication between tags and readers, a specific RFID security protocol is required. In the following, we outline various security methods that have been proposed in recent years.

(1) Original password question

Currently, for RFID systems, the main obstacle to security implementation is cost. RFID achieves the desired security with the following characteristics: for passive tags, it has a 96-bit read-only memory that stores the tag ID number, which is unique for each tag. If the chip can read 200 times per second, it is estimated that within an economically acceptable range, a maximum of 2000 door operations can be allocated to ensure safety. Taking into account Moore's Law, the upper limit can now reach 4000–5000 gate operations. Therefore, only certain specific hidden primitives can be selected, including

Table 1 Table of related tags of different protocols.

protocol	ID	Key
Hash-Lock	56151458	165165156
Hash chain	66549549	3216516fs2
Random Hash-Lock	15541656	Adfasf1216

Table 2 Table of simulation times of RFID systems subjected to different types of attacks.

Attack type	Hash-Lock	Hash chain	Random Hash-Lock
Host-based IDS	3000	5000	6800
Web-based IDS	3000	5000	6800
Distributed IDS	3000	5000	6800

Table 3 Data related to host-based IDS attacks.

Attack type	Hash-Lock	Hash chain	Random Hash-Lock
Number of attacks	3000	5000	6800
Number of successes	2835	4226	5826
Attack time	60S	100S	136S
Attack cost	Low	middle	middle

Table 4 Relevant data of network-based IDS attacks.

Attack type	Hash-Lock	Hash chain	Random Hash-Lock
Number of attacks	3000	5000	6800
Number of successes	2498	4215	6008
Attack time	90S	150S	204S
Attack cost	high	Low	high

Table 5 Data related to distributed IDS attacks.

Attack type	Hash-Lock	Hash chain	Random Hash-Lock
Number of attacks	3000	5000	6800
Number of successes	2945	4826	6571
Attack time	120S	200S	272S
Attack cost	Low	high	middle

most obviously lightweight AES and lightweight DES [22].
(2) RFID system simulation

The communication simulation system between the RFID reader and the RFID tag mainly realizes the two main functions of the simulation system of the communication between the RFID reader and the RFID tag and the simulation attack on the system [23–24].

After opening the simulation system, we can see that we only set one label for each protocol, and we need to add it. The label data of different protocols is shown in Table 1:

We can also get the mark directly. First read and activate the tag, and let it start to run and play a role. Secondly, open the communication reader, operate the related tags, and select different protocols to attack. The data obtained every time will be counted and recorded for later analysis [25].
(3) Simulation of RFID system under attack

Before the attack simulation experiment, you the user first need to activate and connect the tag and open the communication reader to select the attack method and the number of attacks. After the selection is made, different types of attacks are carried out on different protocols, and the maximum support is 100,000 times number of attacks [26].

After completing the above steps, we can start the attack. The progress of the attack is shown in Table 2:

At the same time, statistical comparisons are made for the number of attacks, the number of successes, and the time and cost of attacks for different protocols under different attack types, as shown in Table 3, Table 4, and Table 5:

When we design related protocols, we must consider the issue of the computing power of the protocol label. It is very important for the realization of design computing power. It also explains several common protocols [27].

3.2 Related Experiments of the Perceptual Layer Connectivity Algorithm

In the NS2 simulation environment, the connection algorithm of the sensing layer nodes of the Internet of Things is used to connect the sensing layer devices. If the relationship between the number of device nodes in the sensing layer and the number of devices in the control set and the time required establishing a connection is calculated, it can be concluded that this is the number of devices that dominate the set and the time required to establish it. All connections are proportional to the number of device nodes in the sensing layer. As a test environment, the Internet of Things equipped with 1,000 devices was selected. Among various perception layer devices, various types of

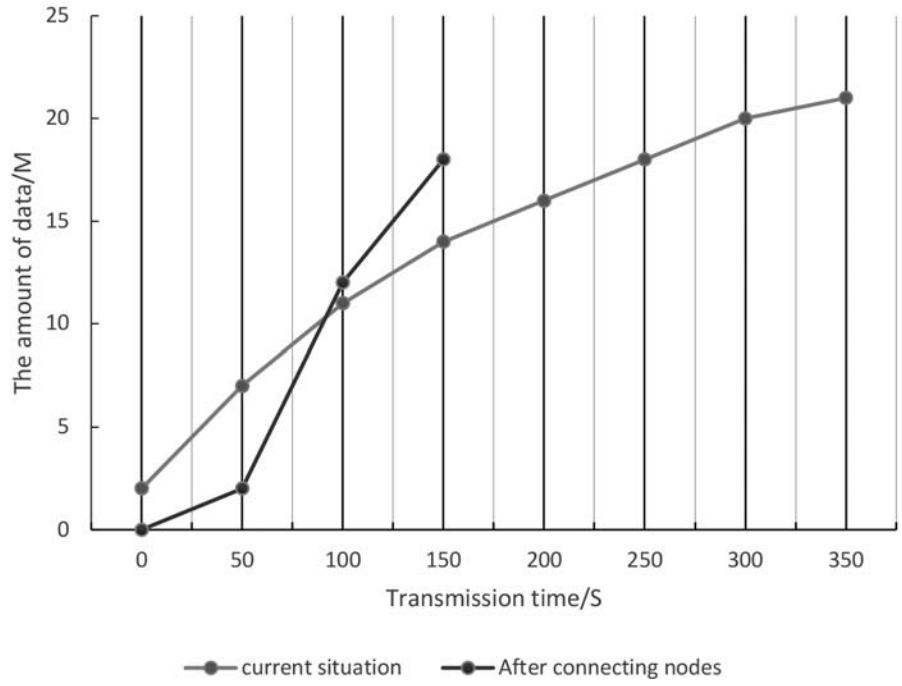


Figure 6 Comparison of the total time of real-time data transmission.

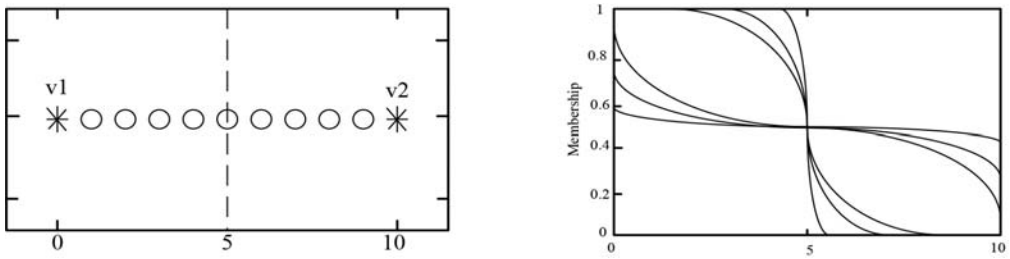


Figure 7 The influence of parameter m on the degree of membership.

networks are connected through hierarchical sub-gateways and the integrated CoAP communication protocol is adopted [28]. We set the sending data rate of the sensing layer device to 1Kbps, and we set the selected communication bandwidth to 256Kbps. In the Internet simulation environment of objects, we compare the relationship between the total sending time of the previous processing strategy and the processing strategy proposed in this article and the total amount of real-time data transmission. The statistical results are shown in Figure 6:

Related research shows that about one-tenth of the real-time processing tasks of the data processed by the Internet of Things can give processing results or control instructions through analysis and processing within three times. For such data tasks, the processing strategies proposed in this article can be used. The devices on the perception layer of the Internet of Things cooperate to process.

4. FUZZY CLUSTERING ALGORITHM

4.1 Performance Analysis

Choosing the fuzzy weight value has a great influence on the clustering effect. This section starts with the meaning and effect of the fuzzy weighting value, and explains the specific changes of the fuzzy weighting value in the two-type fuzzy clustering algorithm. The essential meaning of that change [29].

First, this article uses an example to illustrate the influence of parameter selection on the membership function. Taking the division of the two cluster centers as an example, we take the corresponding cluster centers $v1 = 0$, $v2 = 10$, and take 11 data points from $x1 = 0$, $x2 = 1$ to $x11 = 10$ as sample points. Obtain $m = 20$ from the fuzzy weight $m = 1.1$. If the value of m is different, Figure 7 shows the changes in the membership relationship between two different cluster centers and different sample points x.

Our observation shows that the membership degree of the sample points belonging to a particular cluster center changes with the change of the fuzzy weighting index m. Therefore, the value of the fuzzy weighting index m cannot be a correct value. When $m = 1.1$, the division tends to be a hard division. The membership of all the sample points from 0 to 4 and v1 is 1, and all are classified as cluster centers $v1 = 0$. The membership of all the sample points from 6 to 10 and v2 is 1, and all are classified as cluster center $v2 = 10$. If $m = 20$, all points belong to the membership level 0.5 of the two cluster centers v1 and v2. Only in the case of $m = 2$, the membership degree of different sample points close to the cluster center is smaller, and the membership degree of the

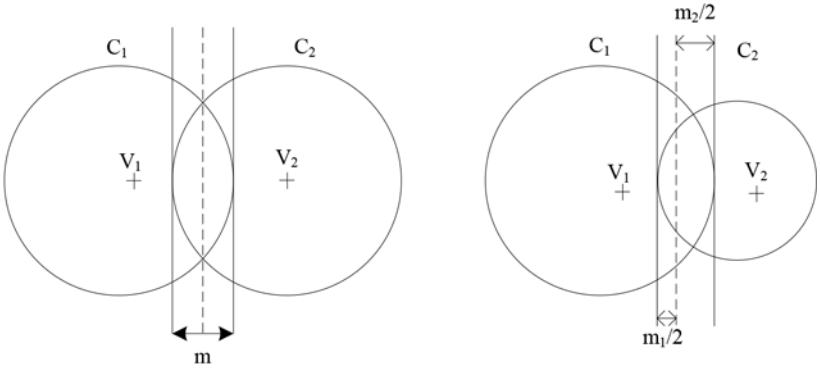


Figure 8 Identical and different divisions of clustering structure.

far cluster center is larger, which is consistent with the actual situation. Therefore, the fuzzy weighting index cannot be a specific value. According to the type of data to be processed, there must also be a relatively optimal fuzzy weighting index suitable for the data structure. In other words, there are objectively excellent response data.

Fuzzy set theory is understood as "different individuals have many different understandings of the same word", and this fuzzification is consistent according to the actual situation. Some fuzzy sets cannot reflect multiple ambiguities to a certain extent, and cannot fully describe and represent the uncertain factors caused by the irregularities and inherent ambiguities of the specific system environment. Therefore, this paper proposes for the first time to introduce two fuzzy weighted indexes to explain the uncertainty of parameter selection. Corresponding to this, the improved performance calculation function H of the clustering algorithm is as follows.

$$H_{m1} = \sum_{i=1}^{n}\sum_{h=1}^{C} u_k(X_i)^{m1} d_{ik}^2 \tag{9}$$

$$H_{m2} = \sum_{i=1}^{n}\sum_{h=1}^{C} u_k(X_i)^{m2} d_{ik}^2 \tag{10}$$

Because a single fuzzy weighted index cannot adjust the ideal fuzzy division of various types of data sets, to this end, as shown in Figure 8, we introduce multiple fuzzy weighted indexes to construct various fuzzy segmentations. A vaguer weighted index can more accurately explain the uncertainty of the algorithm, but it will also lead to an increase in dimensionality and complexity.

The sample between two clusters, that is, the overlapping part of the cluster structure, the membership degree of the sample points belonging to a particular cluster mainly depends on the choice of the fuzzy weighted index m. The cluster centered on v1 is c1, and the cluster centered on v2 is c2. When the value of m is close to 1, it means that there is no composite component between the structures of clusters c1 and c2. The samples can be distinguished by the vertical line connecting the v1 and v2 positions belonging to the c1 or c2 division. This is basically the same as hard segmentation. If the value of m is close to infinity, it is understandable. As a cluster between the clusters c1 and c2, the structure completely overlaps. It is found that the sample point of the cluster center belongs to the cluster center completely, and the membership degree of other sample point pairs is close to 0.5 in c1 and c2. In actual situations, c2 and c2 always partially overlap. In other words, this is a fuzzy field. The overlapping part of the two circles in the photo. When the structures of c1 and c2 are the same, the value of m is the same. When the structures of c1 and c2 are different, m needs two corresponding values m1 and m2. The m-weighted fuzzy value will affect the data structure, so when the clustering structure is different, it is better to use the two-type fuzzy C-means clustering algorithm. Compared with the first-type fuzzy C-means clustering algorithm, the second-type can improve the security protection of the system by 50% in actual use, which has great research value.

5. CONCLUSIONS

This article explores the research on the security optimization of the convergence node of the perception layer of the Power Internet-of Things based on fuzzy clustering. Through the improvement of the fuzzy clustering method, the improved fuzzy clustering algorithm is applied to the security optimization of the convergence node of the perception layer of the Power Internet-of-Things at the same time, and a simulation experiment was conducted. A large number of attacks were carried out on the improved RFID system using three different attack methods. The advantages of the three protocols were explored and a statistical analysis was performed. The security of the system is better improved and the protection against intrusion can be increased by 50%, which can greatly enhance the security of the system.

ACKNOWLEDGEMENTS

This work was supported by the science and technology project of the State Grid Corporation of China (2021YF-56).

REFERENCES

1. X Zhou, R Zhao, F Yu, et al. Intuitionistic fuzzy entropy clustering algorithm for infrared image segmentation. Journal of Intelligent & Fuzzy Systems, 30(3) (2016), 1831–1840.
2. M E Aminanto, H J Kim, K M Kim, et al. Another Fuzzy Anomaly Detection System Based on Ant Clustering Algorithm.

Ieice Transactions on Fundamentals of Electronics Communications & Computer Sciences, 100(1) (2017), 176–183.
3. M G Karunambigai, M Akram, Sivasankar S, et al. Clustering Algorithm for Intuitionistic Fuzzy Graphs. International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, 25(3) (2017), 367–383.
4. S M Lee, I Seong, Y H Joo. Recognition and tracking of moving objects using label-merge method based on fuzzy clustering algorithm. Transactions of the Korean Institute of Electrical Engineers, 67(2) (2018), 293–300.
5. O Kesemen, O Tezel, E Ozkul. Fuzzy c-Means Clustering Algorithm for Directional Data(FCM4DD). Expert Systems with Applications, 58(Oct.) (2016), 76–82.
6. O Caytan, S Lemey, S Agneessens, et al. SIW antennas as hybrid energy harvesting and power management platforms for the internet of things. International Journal of Microwave & Wireless Technologies, 8(4–5) (2016), 767–775.
7. , X Zhou, X Liang., Du, X., & Zhao, J. "Structure Based User Identification across Social Networks", IEEE Transactions on Knowledge and Data Engineering, 30(6), (2018), pp. 1178–1191.
8. W Jiang, Z Yang, Z Zhou, et al. Lightweight Data Security Protection Method for AMI in Power Internet of Things. Mathematical Problems in Engineering, 2020(5) (2020), 1–9.
9. X Kong, Y Xu, Z Jiao, et al. Fault Location Technology for Power System Based on Information about the Power Internet of Things. IEEE Transactions on Industrial Informatics, 16(10) (2020), 6682–6692.
10. Z A Jing, A YY, B Ch, et al. Architecture design and demand analysis on application layer of standard system for ubiquitous power Internet of Things. Global Energy Interconnection, 4(3) (2021), 304–314.
11. G Chen, Y Lu, Y Meng, B Li, K Tan, & D Pei, et al. Fuso: fast multi-path loss recovery for data center networks. IEEE/ACM Transactions on Networking, (2018), 1–14.
12. Y U Lu, H U Wei, X Zhang, et al. Automatic generation control of ubiquitous power Internet of Things integrated energy system based on deep reinforcement learning. Scientia Sinica Technologica, 50(2) (2020), 221–234.
13. D Griffith. Wake-Up Radio for Low-Power Internet of Things Applications: An Alternative Method to Coordinate Data Transfers. IEEE Solid-State Circuits Magazine, 11(4) (2020), 16–22.
14. K H Memon, D H Lee. Generalised fuzzy c-means clustering algorithm with local information. Fuzzy Sets & Systems, 11(1) (2018), 1–12.
15. V Bhatia, R Rani. A parallel fuzzy clustering algorithm for large graphs using Pregel. Expert Systems with Applications, 78(JUL.) (2017), 135–144.
16. M Bidaki, S Tabbakh. Efficient Fuzzy Logic-Based Clustering Algorithm for Wireless Sensor Networks. International Journal of Grid and Distributed Computing, 9(5) (2016), 79–88.
17. C Li, P Liu, C Zou, F Sun, J M Cioffi & L Yang. Spectral-Efficient Cellular Communications with Coexistent One-And Two-Hop Transmissions, IEEE Transactions on Vehicular Technology, 65(8), (2015), pp. 6765–6772.
18. Tiange, Q G Liu, et al. A contour-line color layer separation algorithm based on fuzzy clustering and region growing. Computers & Geosciences, , 88(Mar.) (2016), 41–53.
19. S Zhu, L Xu. Many-objective fuzzy centroids clustering algorithm for categorical data. Expert Systems with Applications, (2018), 96(APR.): 230–248.
20. S B Li. Analysis of Human-Land Coupled Bearing Capacity of Qiangtang Meadow in Northern Tibet Based on Fuzzy Clustering Algorithm. Mathematical Problems in Engineering, 2020(2) (2020), 1–9.
21. Y Gong, S Lin, F He, et al. Damage Identification of Prefabricated Reinforced Concrete Box Culvert Based on Improved Fuzzy Clustering Algorithm and Acoustic Emission Parameters. Advances in Materials Science and Engineering, 2021(7) (2021), 1–13.
22. Q Tang, Y Zhao, Y Wei, et al. Research on the Mental Health of College Students Based on Fuzzy Clustering Algorithm. Security and Communication Networks, 2021(3) (2021), 1–8.
23. I. Butun, P. Österberg and H. Song, "Security of the Internet of Things: Vulnerabilities, Attacks, and Countermeasures," in IEEE Communications Surveys & Tutorials, vol. 22, no. 1, pp. (2020), 616–644, Firstquarter doi: 10.1109/COMST.2019.2953364.
24. H Xu, R Hou, J, Fan et al. The unordered time series fuzzy clustering algorithm based on the adaptive incremental learning. Journal of Intelligent and Fuzzy Systems, 38(1) (2020), 1–9.
25. Y Li. Research on Sports Video Image Analysis Based on the Fuzzy Clustering Algorithm. Wireless Communications and Mobile Computing, 2021(3) (2021), 1–8.
26. W Wang, X Hu, Wang M. Fuzzy clustering algorithm for time series based on adaptive incremental learning. Journal of Intelligent and Fuzzy Systems 38(3), (2020), 1–8.
27. D Phamtoan, V Tai. Improving fuzzy clustering algorithm for probability density functions and applying in image recognition. Model Assisted Statistics and Applications, 15(3) (2020), 249–261.
28. Y Zhang, Y Zhang, R Zhang. Text information classification method based on secondly fuzzy clustering algorithm. Journal of Intelligent and Fuzzy Systems, 38(1) (2020), 1–12.
29. N Y Pehlivan, I B Turksen. A Novel Multiplicative Fuzzy Regression Function with A Multiplicative Fuzzy Clustering Algorithm. Romanian Journal of Information Science and Technology, 24(1) (2021), 79–98.

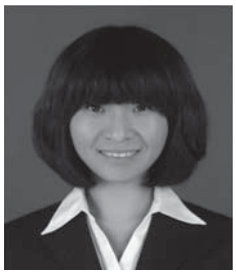
Tong Li was born in Benxi City, Liaoning Province. People's Republic of China, in 1990. He obtained a bachelor's degree from Beijing Jiaotong University in 2013. He received a master's degree in science from Beijing Jiaotong University in 2016. He is mainly engaged in the research and application of energy Internet technology, power system network security, digital twins, block chains, artificial intelligence and other fields.
Email:404708679@qq.com

Yang Liu was born in Ningcheng County, Inner Mongolia. People's Republic of China,in 1982. He received a bachelor's degree in information security from Hunan University in 2016 and a master's degree from Liaoning University in 2011. He is mainly engaged in computer

software and theory, network and information security and other fields.
Email:liuyang_dky@163.com

Yaodong Tao was born in Changchun, Jiangxi. P.R. China, in 1980. He received the bachelor's degree from Jilin University, in 2002. He received a master's degree in computer software and theory from Shenyang Institute of computing technology in Chinese Academy of Sciences, in 2005. He obtained a doctorate in computer application technology from the University of science and technology of China, in 2009. Now, He is the Chief scientist of Beijing DualPi Intelligent Security Technology Co. Ltd. His research interest include network security, information security and big data analysis.
E-mail: taoyaodong@dualpi.com

Donghua Huang was born in Changchun, Jilin. P.R. China, in 1981. She received the bachelor's degree from Jilin Normal University, in 2004. She received an MBA from Beijing University of Aeronautics and Astronautics, in 2011. Now, She is the deputy general manager of Beijing DualPi Intelligent Security Technology Co. Ltd. Her research interest include network security, information security and big data analysis.
E-mail: lanxi6089@163.com



Hongbi Geng was born in Shenyang, Liaoning Province. People's Republic of China, in 1985. She received a bachelor's degree in computer science and technology from Shenyang University of technology. She received a master's degree in computer software and theory from Shenyang University of technology. Her main research direction is 3D based GIS.
E-mail:1143267619@qq.com

Qian Sun was born in Xinxiang City, Henan Province. People's Republic of China, 1995. In 2017, She obtained a bachelor's degree in electrical engineering and automation from Northeast University. In 2020, she obtained a master's degree in power system and automation from Northeast University, mainly focusing on energy Internet and power communication.
E-mail:274846837@qq.com