Study on privacy node encryption method for wireless sensor networks based on edge computing

Yun Wei* and Lingnan Zhou

College of Electronic and Information Engineering,
Henan Polytechnic Institute,
Nan'yang 473000, China
Email: annie000592@163.com
Email: nyzl333@163.com
*Corresponding author

Abstract: Aiming at the problem of poor encryption effect of the existing wireless sensor network privacy node encryption method, a wireless sensor network privacy node encryption method is designed based on edge computing. Firstly, the wireless sensor network structure and protocol stack structure are clarified, the composition structure of privacy nodes and the set of neighbour nodes are determined, and then the privacy node sensitivity is obtained through the adjacency matrix, and the privacy node location of wireless sensor network is realised by the trilateral positioning method. Finally, the edge computing method is introduced to aggregate the number of edge nodes of privacy nodes, complete the division of privacy node datasets, set terminal encryption keys for them, and realise wireless sensor network privacy node encryption. The experimental results show that the positioning error of this method is up to 0.9%, which can effectively improve the positioning accuracy of privacy nodes and improve the security of the network.

Keywords: edge calculation; privacy node; encryption; differential privacy; undirected graph; encryption key.

Reference to this paper should be made as follows: Wei, Y. and Zhou, L. (2023) 'Study on privacy node encryption method for wireless sensor networks based on edge computing', *Int. J. Reasoning-based Intelligent Systems*, Vol. 15, No. 1, pp.63–70.

Biographical notes: Yun Wei graduated from Huazhong University of Science and Technology in 2013 with a Master's degree in Electrical Engineering. Currently, she is a Lecturer at the College of Electronic and Information Engineering, Henan Polytechnic Institute. Her research direction is Computer application technology research and teaching.

Lingnan Zhou received his Bachelor's degree in Information Technology from Henan Normal University. Currently, he works at the College of Electronic and Information Engineering, Henan Polytechnic Institute. His research interests include network technology, software and big data technology.

1 Introduction

The industrial development of information technology is constantly promoting the transition changes of electronic technologies such as electronics and digital communication, and thus multi-functional wireless sensors have emerged, which can be used to form a complex wireless sensor network (Wang et al., 2022) for data communication in human production. This network is a self-organising grid system composed of a large number of sensors, which has the characteristics of no fixed central point, diversified topology and multi-hop routing (Prateek et al., 2021). Effective information acquisition can be carried out in a fixed area (Qi et al., 2021). In the operation process of the network, the nodes play a key role of the hub, through which the relevant communication information can be continuously transmitted. These nodes are combined together independently according to the needs of information transmission, and achieve the purpose of operation through their specific functions (Nancy et al., 2020). Among them, through its own functions, the privacy node can effectively coordinate the key information needed to complete data processing and conversion between communication protocols. The critical degree of this node is related to the security of this network (Abbasikesbi et al., 2020). Therefore, encryption of privacy nodes in wireless sensor networks is the main method to improve network security. Therefore, relevant researchers have carried out a lot of research and designed some privacy node encryption schemes.

Chen et al. (2021) designed an improved AES encryption algorithm to encrypt wireless sensor networks. Firstly, the algorithm analyses the distribution of nodes in WSN, determines the complexity of nodes through the cooperation of these nodes, and encrypts the nodes using AES. Although the operation process of this method is simple and the information transmission speed of the encrypted nodes is fast, the encryption effect is not ideal because it can only encrypt all nodes in the network, and cannot encrypt private nodes specially. Lv (2021) proposed a method to protect private location information of source nodes in wireless sensor networks. This method through the design of key nodes defence model as the foundation, through the panda-hunter optimisation defence node location privacy protection model, then the network nodes randomly hop for statistics, with the help of probability calculation of the probability of nodes can reach to summarise point, determine the privacy coefficient of node, to complete the source of the wireless sensor network node location information privacy protection. In the process of encrypting network privacy nodes, this method does not locate their specific positions, so there are errors in determining information, the encryption effect is poor, and the application time is long. Jiang et al. (2021) designed a new secure encryption method for wireless sensor networks. The method is introduced into polynomial key distribution will take place in the network node clustering technology, and the nodes in the communication data after clustering key distribution, and then by using the particle swarm algorithm to calculate the energy of the nodes and the communication distance, and the clustering performance after the optimal node loss calculation, and through the degree of polymerisation values iterative calculation of all nodes remaining energy, determine privacy node energy, And encrypt it. This method mainly determines the location of the privacy node by calculating the node energy, but it has some limitations. It can only determine the location range of the privacy node, but cannot achieve accurate positioning, so its encryption effect is poor. The above three methods are not ideal for network privacy node encryption, mainly because the specific location of the privacy node cannot be confirmed, leading to errors in node information, so the encryption effect is not ideal.

Aiming at the limitations of the above encryption methods, this paper designs a privacy node encryption method based on edge computing in wireless sensor networks. First and its network structure of wireless sensor network node analysis, the distribution of composition and neighbour node set of privacy of network to determine, and then through the sensitivity of the privacy node adjacency matrix, established by the method of trilateral positioning of the wireless sensor network node location privacy, finally USES the complete privacy calculation method of edge node dataset, set encryption key for its terminal to realise encryption of privacy nodes. It is hoped that the research of this paper can provide references for the research on encryption and decryption of privacy nodes in wireless sensor networks.

2 Location analysis of wireless sensor networks and private nodes

2.1 Analysis of wireless sensor network structure and node structure

In order to realise privacy node encryption in wireless sensor networks, the structure of wireless sensor networks and the basic distribution of its key privacy nodes need to be clarified first, which provides a theoretical basis for subsequent encryption. Wireless sensor network is a multi-hop self-organising network, which is composed of a large number of different nodes to form a complex communication network and is managed and organised by different networks with obvious advantages (Jiang et al., 2021). The basic structure is shown in Figure 1.

It can be seen from Figure 1 that the operation process of the network can be completed after the information to be transmitted by the node is transmitted to the SINK node and processed by its management centre. In the continuous communication of the network, the protocol stack of its nodes is very important. The protocol stack mainly includes physical layer, data link layer, network layer, transmission layer and application layer (Karimi-Bidhendi et al., 2020). In these layers, by following the data transmission protocol and the underlying communication protocol, the main task of the link layer of different data is designed as medium access, etc., and the high-speed operation of the whole network can be realised through the effective routing between the nodes receiving and sending packets.

Based on the network structure, the encryption method of its privacy nodes is studied. Therefore, it is necessary to analyse the distribution of nodes in the network, find out the location of key privacy nodes, and encrypt them. Wireless sensor network nodes are generally composed of four modules, which are mainly energy supply module, perception module, processing module and communication module. Among them, the energy supply module mainly provides the energy of each module of the node. The sensing module is mainly responsible for sensing and collecting relevant data. The processing module, as its name implies, is the function of processing data. It is the control centre of nodes and shares the storage of transmitted data (Juneja et al., 2022). Communication module is responsible for data transmission with other nodes. The node structure of wireless sensor network is shown in Figure 2.

Figure 1 Schematic diagram of the basic structure of WSN

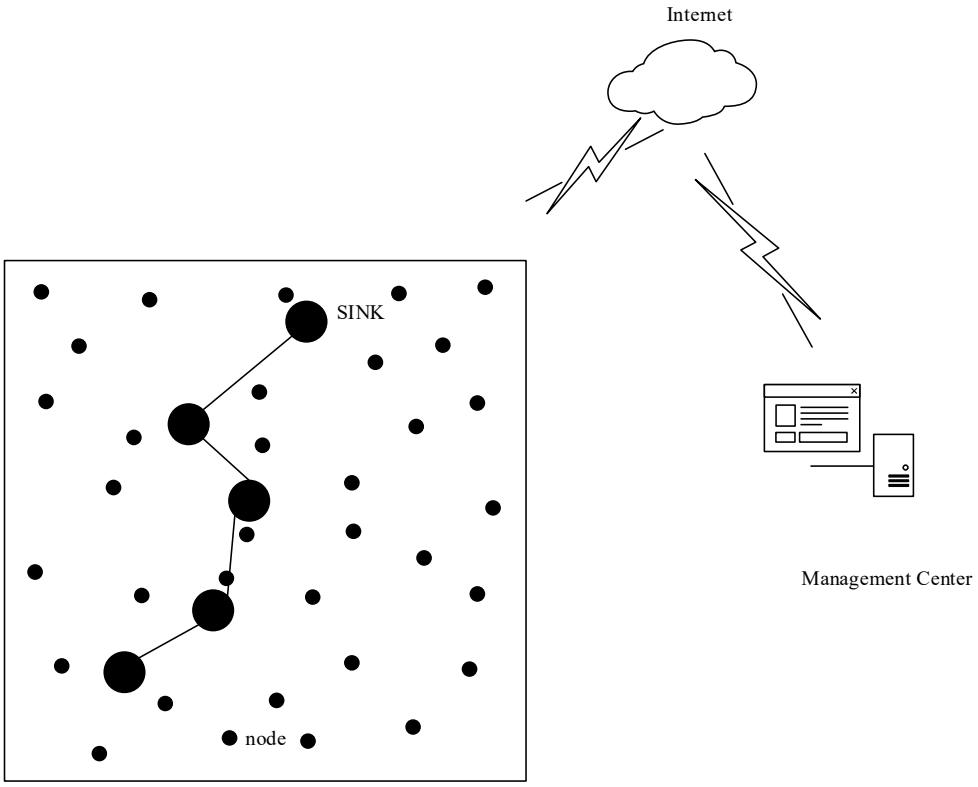
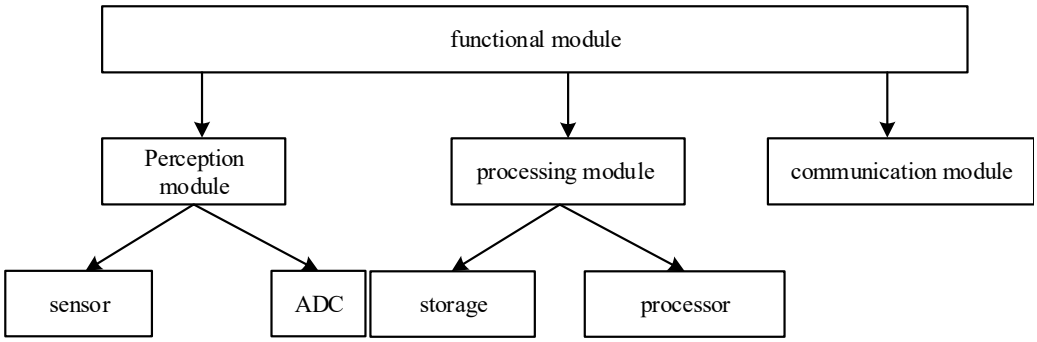


Figure 2 Schematic diagram of wireless sensor network node structure



2.2 Location analysis of private nodes in wireless sensor networks

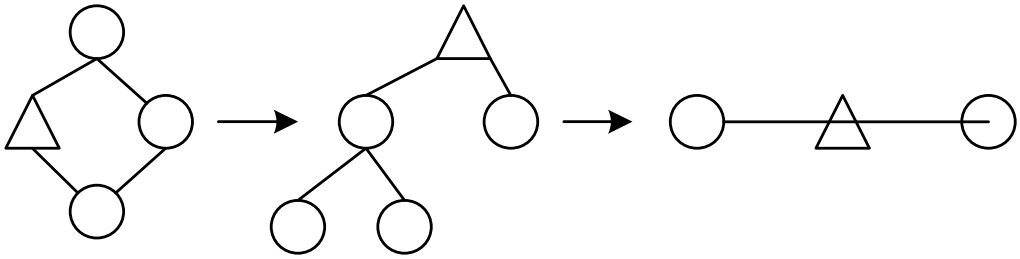
According to the structural characteristics of the above analysis, in order to improve the accuracy of privacy node encryption, it is necessary to determine the location of the privacy node, that is, to conduct positioning research on the privacy node. Privacy node location is actually a kind of privacy location determination, which is very important in wireless sensor networks, mainly related to the monitoring of target location, routing protocol and information transmission quality. Once the privacy node location is used improperly, it will lead to serious security problems.

In the privacy node location, this paper mainly detects the way in which the attacker attacks the privacy node. It is necessary to determine the location of the protection data source of the privacy node in the communication mode through the random route selection mechanism. When the attacker attacks the privacy node, the gradually changing structure type of the node can reflect the strength of the privacy node (Kanwar and Kumar, 2021). Therefore, node-refining access is performed on the privacy nodes first. Set a node a in the network, V_0 represents the weakest access point of the node, and set φ as an empty set of unlabeled graph, return any node $V_1(a)$ to the visited path, $V_2(a)$ to multiple sets of neighbour degrees, and get the collection of visited nodes is:

$$V_i(a) = \left\{V_{i-1}(a_1), V_{i-1}(a_2), \ldots, V_{i-1}(a_m)\right\} \tag{1}$$

where $a_1, \ldots, a_m$ represents the neighbour node of the visited node.

Figure 3 Node local structure expansion mode



Through the determination of neighbour nodes, expand the local structure of all nodes in the network, control any node around the target privacy node, and determine the strength of the privacy node by determining the access strength of the node (Vijayalakshmi et al., 2021). The local structure expansion mode of the node is shown in Figure 3.

When the local structure of the node is expanded, the information loss degree of the privacy node needs to be calculated in order to determine whether the extended node is a privacy node. The calculation formula of the information loss degree of the node is as follows:

$$S(x, y) = [E(x) \cup E(y)] - [E(x) \cap E(y)] \tag{2}$$

where $E(x)/E(y)$ represents the set of different nodes, respectively, and $S(x, y)$ represents the degree of information loss.

After the information loss degree of nodes is determined, the degree of participation of nodes in the whole network should be determined according to their utilisation. In a network operation cycle, the entropy value of the number of times the node is continuously forwarded can reflect the probability value of the node being utilised (Yilmaz et al., 2021), which can be obtained as follows:

$$P(n) = -\sum_{i=1}^{n} \frac{\vartheta_i}{h} \log \frac{\vartheta_i}{h} \tag{3}$$

where ϑ_i represents the number of times the nodes are forwarded, n represents the sum of the number of occurrence of all nodes in the network, and h represents the node forwarding entropy value.

The appearance of nodes in the wireless sensor network can be regarded as an undirected graph, which displays the total node location of the network through the adjacency matrix, that is, the nodes in the network are set as B_1/B_2. If the two nodes are exactly the same, the two nodes run in the undirected graph, namely $K(B_1) = K(B_2)$, then the arbitrary output results of the two nodes are:

$$Q(x) = N(B_1) \sum N(B_2) g \tag{4}$$

Specifically, $Q(x)$ represents the differential privacy result of the node, and g represents the probability that the privacy node appears.

After determining the probability of the occurrence of the private node in the network node, in order to determine the location of the private node, it is necessary to further determine the sensitivity of the private node, and obtain:

$$\Delta d = R \max \left\| d(B_1 - B_2) \right\| \tag{5}$$

where R represents the space of the real number of nodes of the map, and d represents the query dimension of the privacy nodes.

There are many privacy nodes in wireless sensor networks, and the surrounding nodes may also be privacy nodes. Therefore, the privacy of the surrounding nodes is determined by using the three-way positioning method (Kumar and Agrawal, 2021), and the coordinates of the three nodes around the privacy node are set as $(x_a, y_a)/(x_b, y_b)/x_c, y_c)$, and the corresponding side lengths of the three-point coordinate are $l_a/l_b/l_c$, so the coordinate positions of the three surrounding privacy nodes are expressed as follows:

$$\begin{cases} v\sqrt{(x_a - y_a)^2 + (x - y_a)^2} = l_a \\ v\sqrt{(x - x_b)^2 + (x - y_b)^2} = l_b \\ v\sqrt{(x - x_c)^2 + (x - y_c)^2} = l_c \end{cases} \tag{6}$$

where $(x_a, y_a)/(x_b, y_b)/x_c, y_c)$ represents the trilateral position coordinates of the privacy node, and v represents the error system values in the positioning.

In the wireless sensor network node location privacy, through access to all the nodes in refining, determine the neighbour node set of privacy nodes, through the node entropy calculation of degree of node information loss, and privacy node sensitivity is obtained by adjacency matrix, the undirected graph with trilateral positioning method in wireless sensor network node location privacy.

3 Privacy node encryption in wireless sensor networks based on edge computing

After determining the location of privacy nodes in wireless sensor networks, this paper uses edge computing method to encrypt the nodes. The so-called edge computing mainly refers to the end services provided by an open platform that integrates network, computing, storage, and application core capabilities on the side close to the source of objects and data (Khan et al., 2021). This method can transfer the required information to the cloud server by changing the storage location of the edge device, and then process the data. Compared with other methods, this method has the

advantages of high real-time performance and fast transmission speed, which can reduce network bandwidth and energy consumption. It does not need to send data directly to the destination, but uses the edge of the network to process data, and has the advantages of low risk and good fault tolerance in the process of data storage. Therefore, this paper introduces this method in the privacy node encryption, treats the privacy node as a kind of data for marginal processing, and then designs the key for encryption research.

In the encryption of wireless sensor network, the random algorithm T is set and set T_m as a set of all privacy nodes that may encrypt. For any two close nodes f_1 and f_2 and any subset, the algorithm meets the formula (7), that is:

$$P\left[M(f_1)\in z_m\right] < EXP(e)\left[M(f_2)\in z_m\right] \tag{7}$$

Among them, P represents the degree of privacy node data centralisation, and $EXP(e)$ represents the privacy node protection parameter. The degree of differential privacy of the privacy nodes is determined by this stochastic algorithm.

Given the degree of differential privacy of privacy nodes determined above, the global and local sensitivity of privacy nodes needs to be determined. Set the function $f(x)$, the global sensitivity of the privacy node can be expressed as:

$$Gf(x) = r\min_{f_1,f_2}\left\|f(d_1)-f(d_2)\right\|u \tag{8}$$

where $f(d_1)$ and $f(d_2)$ represent the privacy nodes, r represents the real number of neutralisation in the mapping space, and u represents the dimension of the function.

Based on the global sensitivity calculation, the local sensitivity of the private nodes is expressed as:

$$\gamma f(x) = r\underset{f_1,f_2}{\mathrm{MAX}}\left\|f(d_1)-f(d_2)\right\|u \tag{9}$$

where $\gamma f(x)$ represents the local sensitivity of the privacy nodes, $\underset{f_1,f_2}{\mathrm{MAX}}$ represent the maximum change value in the acquisition process.

At this point, to decrease the difficulty of encrypted privacy node calculation method introduced edge, will be on the verge of privacy node data batch together and divided privacy through the calculation of edge node datasets, then will be assigned to different edge privacy node, reduce the distance between nodes, to improve the overall effect of privacy nodes, privacy node edge distance is expressed as:

$$dis(w) = \sqrt{w_1\left|1-w_1\right|^2+\left|1+w_1\right|\ldots\left|1-w_n\right|^2} \tag{10}$$

where $dis(w)$ represents the maximum distance where the privacy node is marginalised, and w_n represents the weighted Euclidean distance.

In the calculation and summary of the edge distance of the above privacy nodes, it is also necessary to consider unifying the distribution distance of the privacy nodes and calculating the attribute weight of the privacy nodes to obtain:

$$\rho_i = \varepsilon w_i + \beta w_i \tag{11}$$

Among them, ρ_i represents the attribute data node weight of the custom privacy nodes, and ε represents the privacy degree of the nodes' standard attributes, and β represents the proportion. The calculation w_i results are:

$$w_i = \sum_{i=1}^{n}\frac{w_{all}}{w_i} \tag{12}$$

where n represents the total number of privacy node markers, and w_{all} represents the weight value of the standard attributes.

After marginalisation the privacy node, the identity of the privacy node is set to τ_{id} through the edge computing device, and the length of each node is C. At this case, the terminal identity expression of the privacy node is:

$$\tau_{id} = \left\{\tau_{id_1}, \tau_{id_2}, \ldots, \tau_{id_N}\right\} \tag{13}$$

Then select a random key for each privacy node in the terminal identity of its privacy node $\aleph_i$, and assign these keys to each privacy node to complete the study of the privacy node encryption of the wireless sensor network, obtaining:

$$q_i = \sigma^{\aleph_i} \bmod \omega \tag{14}$$

$$q_i' = \tau_{id} \times P\forall_s \aleph_{i \bmod \omega} \tag{15}$$

where σ represents the matching coefficient, ω represents the error value in the key assignment, and $\forall_s$ represents the order of encryption.

Privacy in wireless sensor network node in the encryption, with the aid of random algorithm to determine the difference of privacy node degree of privacy, privacy and calculate the node of global and local sensitivity, introducing edge calculation method, the edge will privacy node quantity and divided privacy through the calculation of edge node datasets, then will be assigned to different edge privacy node, Terminal encryption key is set for privacy node to realise privacy node encryption in wireless sensor network.

4 Experimental analysis

4.1 Experimental scheme

In order to fully verify the real effect of the private node encryption method in this paper and improve the accuracy of the simulation experiments, this research is based on the MATLAB platform, and 1,000 sensor nodes are randomly deployed in a 150 × 150 plane area, and the number of private nodes in these nodes is set to 600. The number of anchor nodes is 10, and the rest are ordinary nodes. The generated sensor nodes are used as the experimental sample dataset, and the noise between –1 dB and 1 dB is added to the node dataset for the convenience of real scene simulation. The specific experimental parameters are shown in Table 1.

Table 1 Design of simulation experimental parameters

Parameter	*Content*
Number of sample nodes/individual	1,000
Number of privacy nodes/number	600
Number of anchor nodes/individual	10
Node communication radius/m	50
Encryption key generation quantity/individual	600
Encryption interval/s	0.5
Noise range/dB	[–1–1]

4.2 Experimental index design

According to the design of the above experimental protocol, the experiment was conducted by comparing the present method, Lv's (2021) method and Jiang et al.'s (2021) method. The main indicators set in the experiment are the error degree of privacy node positioning, and the accuracy of key matching in privacy node encryption are the experimental indicators. The calculation formula of the privacy node location error is as follows:

$$e_i = \left\| \breve{X} - X \right\| / n \tag{16}$$

where e_i represents the location error results of the privacy node, the actual position coordinates of the privacy node is $\breve{X}$, the coordinate positions of the predicted privacy nodes is X, and n is the number of locations.

4.3 Analysis of experimental results

4.3.1 Location error analysis of private nodes in wireless sensor networks

In the experiment, the location error of privacy node in wireless sensor network is analysed firstly. The location error of privacy node is the key of encryption and the key to measure the designed encryption algorithm. The method in this paper, the method in Lv (2021) and the method in Jiang et al. (2021) are used to locate 600 privacy nodes in the sample of 1000 nodes, and the comparative results of positioning errors are obtained, as shown in Figure 4.

As can be seen from the experimental results in Figure 4, the positioning errors of the three methods are different with the continuous changes of wireless sensor node data. As can be seen from the data in the figure, the positioning error range of the method in Lv (2021) is between 0.9% and 1.7%, while that of the method in Jiang et al. (2021) is between 1.4% and 2.2%. However, the positioning error of the method in this paper is small, with a maximum of 0.9%, and presents a downward trend with the increase of data. From the trend of the overall view, using the method for privacy node localisation error is lower, this is because the algorithm in this paper, the refining visit all nodes, determine the neighbour node set of privacy nodes, through the node entropy calculation of degree of node information loss, and privacy node sensitivity is obtained by adjacency matrix, In the undirected graph, the privacy node location is realised by using the three-side location method, which reduces the location error.

Figure 4 Analysis of privacy node localisation error in wireless sensor networks

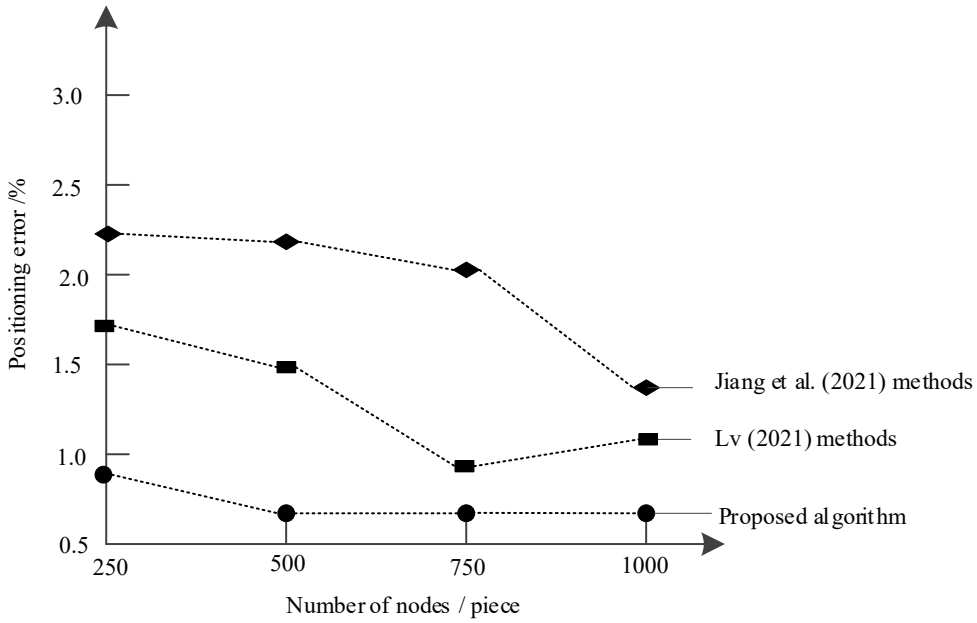


Figure 5 Private node key matching accuracy analysis of different methods

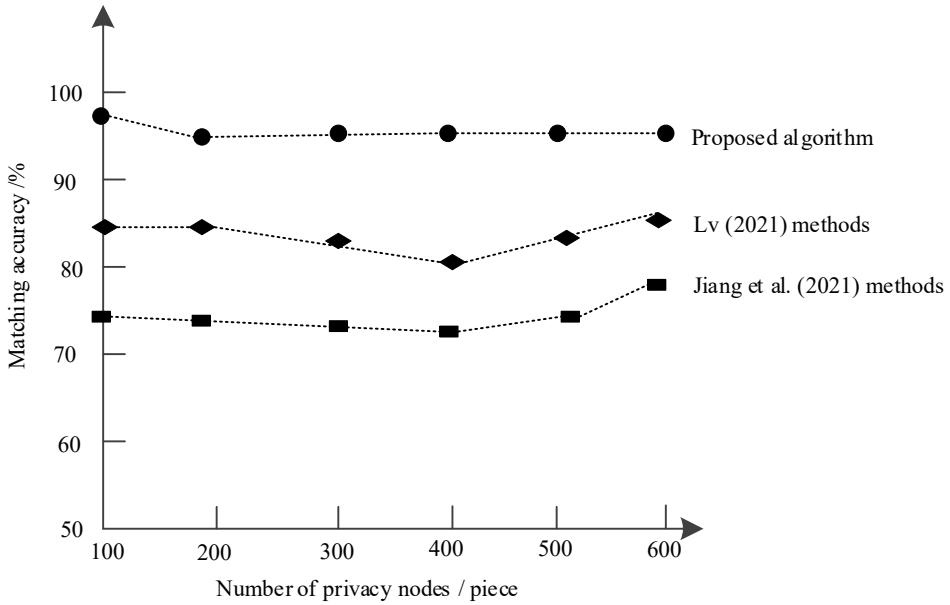


Figure 5 shows the comparison results of matching accuracy of the privacy node key by the three methods.

As can be seen from the experimental results in Figure 5, there are certain differences in the key matching accuracy of the three methods. Among them, the method proposed in this paper has the highest matching accuracy, always higher than 90%, while the matching accuracy of the method in Lv (2021) is lower than 86%, the matching error of the method in Jiang et al. (2021) is lower than 78%, and the matching accuracy of the other two methods is lower than the method proposed in this paper. In comparison, the method presented in this paper has better matching accuracy. This is because the method in this paper introduced the edge computing method to aggregate the number of edge nodes of privacy nodes, divided the dataset of privacy nodes by edge computing, and then allocated the privacy nodes to different edge nodes, and set terminal encryption keys for the privacy nodes, which improved the effectiveness of the proposed method.

5 Conclusions

In wireless sensor networks, the effectiveness of privacy node encryption affects the security of the entire network. Therefore, this paper designs a privacy node encryption method based on edge computing in wireless sensor networks. This paper first defines the structure of the wireless sensor network to determine the privacy node structure, determine the privacy node neighbour node set. Then, the degree of information loss of nodes is determined by calculating node entropy, the sensitivity of privacy nodes is obtained by adjacency matrix, and the location of privacy nodes in wireless sensor networks is realised by using the three-side location method in undirected graph. Finally, a random algorithm is used to determine the difference privacy degree of privacy nodes, the edge computing method is introduced to collect the number of edge nodes of privacy nodes, and the dataset of privacy nodes is divided by edge computing. Then, privacy nodes are assigned to different edge nodes, and terminal encryption keys are set for privacy nodes to achieve encryption. In order to verify the advance of the proposed method, a comparative experiment is also carried out. Compared with the methods in the literature, this algorithm can effectively reduce the location error of privacy nodes, and the error is always less than 0.9%. It can improve the precision of privacy node key matching and the security of privacy encryption, so it has certain application value. Although the method in this paper has a certain research effect, the response speed is not considered as an indicator in the analysis process, so the speed of encrypted transmission of privacy nodes will be improved through further research in the future.

References

Abbasikesbi, R., Nikfarjam, A. and Nemati, M. (2020) 'Developed wireless sensor network to supervise the essential parameters in greenhouses for internet of things applications', *IET Circuits Devices & Systems*, Vol. 14, No. 8, pp.1258–1264.

Chen, J., Wang, L., Zhong, J., Zhang, Z. and Guo, X. (2021) 'Implementation of improved AES encryption algorithm in wireless sensor networks', *Modern Electronics Technique*, Vol. 44, No. 12, pp.44–48.

Jiang, J-F., Sun, J-X. and You, L-T. (2021) 'Security clustering strategy based on particle swarm optimization algorithm in wireless sensor network', *Computer Science*, Vol. 48, No. 2, pp.452–455, 470.

Juneja, S., Kaur, K. and Singh, H. (2022) 'An intelligent coverage optimization and link-stability routing for energy efficient wireless sensor network', *Wireless Networks*, Vol. 13, No. 35, pp.136–141.

Kanwar, V. and Kumar, A. (2021) 'DV-hop localization methods for displaced sensor nodes in wireless sensor network using PSO', *Wireless Networks*, Vol. 27, No. 1, pp.91–102.

Karimi-Bidhendi, S., Guo, J. and Jafarkhani, H. (2020) 'Energy-efficient node deployment in heterogeneous two-tier wireless sensor networks with limited communication range', *IEEE Transactions on Wireless Communications*, Vol. 36, No. 19, pp.152–157.

Khan, A.N., Tariq, M.A., Asim, M. et al. (2021) 'Congestion avoidance in wireless sensor network using software defined network', *Computing*, Vol. 103, No. 1, pp.634–639.

Kumar, S. and Agrawal, R. (2021) 'A comprehensive survey on meta-heuristic-based energy minimization routing techniques for wireless sensor network: classification and challenges', *The Journal of Supercomputing*, Vol. 78, No. 5, pp.6612–6663.

Lv, Y-R. (2021) 'Research on the protection of source node's privacy location information in wireless sensor networks', *Computer Simulation*, Vol. 38, No. 10, pp.320–323.

Nancy, P., Muthurajkumar, S., Ganapathy, S. et al. (2020) 'Intrusion detection using dynamic feature selection and fuzzy temporal decision tree classification for wireless sensor networks', *IET Communications*, Vol. 14, No. 5, pp.888–895.

Prateek, A.R. and Verma, A.K. (2021) 'Non-coherent localization with geometric topology of wireless sensor network under target and anchor node perturbations', *Wireless Networks*, Vol. 27, No. 4, pp.457–462.

Qi, N., Yin, Y., Dai, K. et al. (2021) 'Comprehensive optimized hybrid energy storage system for long-life solar-powered wireless sensor network nodes', *Applied Energy*, Vol. 29, No. 2, p.116780.

Vijayalakshmi, P., Selvi, K., Gowsic, K. et al. (2021) 'A misdirected route avoidance using random waypoint mobility model in wireless sensor network', *Wireless Networks*, Vol. 27, No. 6, pp.3845–3856.

Wang, J., Wang, R. and Zeng, X. (2022) 'Short-term passenger flow forecasting using CEEMDAN meshed CNN-STM-attention model under wireless sensor network', *IET Communications*, Vol. 12, No. 3, pp.637–642.

Yilmaz, M., Ozbayoglu, A.M. and Tavli, B. (2021) 'Efficient computation of wireless sensor network lifetime through deep neural networks', *Wireless Networks*, Vol. 36, No. 6, pp.63–71.