Hindawi
Journal of Sensors
Volume 2021, Article ID 7886639, 11 pages
https://doi.org/10.1155/2021/7886639

Research Article

Optimization of Wireless Sensor Network Architecture with Security System

Shanshan Wang[1,2] **and Yun Chen**[2]

[1]*School of Information Management and Engineering, Shanghai University of Finance and Economics, Shanghai 200433, China*
[2]*Shanghai Key Laboratory of Financial Information Technology, Shanghai University of Finance and Economics, Shanghai 200433, China*

Correspondence should be addressed to Shanshan Wang; wss@sufe.edu.cn

Received 28 September 2021; Revised 12 October 2021; Accepted 15 October 2021; Published 8 November 2021

Academic Editor: Guolong Shi

Wireless sensor network (WSN) is a new type of wireless network. It has many advantages, but there are some problems. These problems make it easier for attackers to analyze network security holes and attack and destroy entire networks. This article designs a security wireless sensor network model. It can resist most known network attacks without significantly reducing the energy power of sensor nodes. First, we cluster the network organization to reduce energy consumption. It also protects the network based on the calculation of trust levels and the establishment of trust relationships between trusted nodes and operates the trust management system based on a centralized method, secondly, on the basis of LEACH agreement, draws lessons from the principle of biological immune system, optimizes the wireless sensor network, and further proposes a new immune system structure suitable for wireless sensor networks. The experimental results show that the wireless sensor network model designed in this paper solves the high-efficiency and energy-saving design task, and the trust management system has satisfactory results in defending against attacks.

1. Introduction

After four generations of development, wireless sensor network integrates communication technology, embedded computing technology, distributed information processing technology, and sensor technology, so that people can obtain detailed and reliable information and realize the dream of "ubiquitous computing" [1, 2]. It has huge vitality in the fields of national defence and military, environmental monitoring, medical, and health [3]. Wireless sensor network (WSN) is a basic new type of wireless network, which is based on an infinite number of microsensors powered by a limited amount of batteries, designed to collect information and monitor objects [4, 5]. WSN has many advantages, such as wireless communication channels and dynamically changing topological structures. But there are also shortcomings, such as insufficient infrastructure, big data flow and unlimited nodes, limited battery power supply, and node mobility. These problems allow attackers to more easily analyze network security vulnerabilities to attack and destroy the entire network or a certain controlled object [6].

Generally speaking, the vast majority of attacks focus on disabling sensor nodes, routing protocol disorientation, and destroying the entire network. At present, there are generally two methods to prevent attacks—encrypted measures and nonencrypted measures [7]. The main purpose of encryption measures is to defend against external intrusions and prevent intruders from infiltrating the network. In this case, if a node is broken or captured by an attacker, as a whole network, other nodes will also be threatened. Encryption measures require a large amount of memory and high power consumption in processing and communication, which makes it unsuitable for WSN with limited resources. Therefore, it is necessary to use other security measures. The purpose of the nonencrypted method is to protect the network from internal attacks. Attack analysis shows that most attacks can be called active attacks [8]. In WSN, active attacks present different methods, and data packets can freely enter the wireless channel through internal attackers.

Since the application-oriented domain is one of the main characteristics of wireless sensor networks, it is difficult to have a general specific reference structure to follow [9]. The lack of a unified architecture standard will increase the difficulty of coordination between different systems, cause a waste of research resources, and even restrict the further development of wireless sensor networks. Therefore, this paper proposes an optimized WSN architecture and strives to integrate the advantages of various architectures to improve the module reusability and overall performance of wireless sensor networks. This article first clusters network organizations to reduce energy consumption. It also protects the network based on the calculation of trust levels and the establishment of trust relationships between trusted nodes and operates the trust management system based on a centralized method. Secondly, on the basis of the LEACH protocol, drawing on the basic ideas of biological immunity, a new immune system structure suitable for wireless sensor networks is proposed. The immune response strategy effectively resists attacks from malicious nodes and reduces and eliminates the impact of malicious data, thereby ensuring data security.

The structure of the paper is as follows: Section 2 provides related works. Section 3 discusses our approach. Results are presented in Sections 4. Section 5 concludes the paper.

2. Related Knowledge

2.1. The Development Status of Wireless Sensor Networks. Research on wireless sensor networks began in the late 1990s. Since the 21st century, sensor networks have attracted great attention from academia, military, and industry. The United States and Europe have successively launched many research projects on sensor networks [10, 11]. In particular, the United States has invested heavily in support of sensor network technology research through various channels such as the National Natural Science Foundation of China and the Department of Defence. In 1995, the US Department of Transportation proposed the “National Intelligent Transportation System Project Plan,” which is expected to be fully operational by 2025 [12, 13]. The plan attempts to effectively integrate advanced information technology, data communication technology, sensor technology, control technology, and computer processing technology for the entire ground transportation management and establish a real-time, accurate, and efficient integrated transportation management system. This new system will effectively use the sensor network for traffic management. It can not only make the car drive at a certain speed and automatically maintain a certain distance between the front and rear cars, but it can also provide the latest news about road congestion and recommend the best driving route and remind the driver to avoid traffic accidents, etc. [14]. Because the system will use a large number of sensors to keep in touch with various vehicles, people can use computers to monitor the operating conditions of each car. According to the specific situation, the computer can automatically adjust to keep the vehicle in the best operating state with high efficiency and low consumption and issue warnings about potential failures or directly contact the accident rescue centre [15].

Due to the great application value of wireless sensor networks, it has attracted great attention from the industrial, military, and academic circles in many countries around the world [16]. Information industry giants have also begun research on sensor networks. The technologically developed countries in Japan, Britain, Germany, and Italy have also shown great interest in wireless sensor network technology and have launched research in this field. However, most of the work is still in its infancy. The few commercial products put into use are still far from actual demand. There is very little research work on wireless sensor networks in our country. At present, some domestic colleges and universities and scientific research institutions have actively carried out relevant research work on wireless sensor networks.

At present, domestic research hotspots are mainly concentrated in areas such as wearable computing, context-aware environments, and smart classrooms. The application of wireless sensor network technology in environmental safety monitoring is still rare. Generally speaking, domestic research on sensor networks is still in its infancy. However, because sensor network is an emerging technology, the gap between domestic and international levels is not very large. Promptly carrying out research on this cutting-edge technology that has a far-reaching impact on the future life of mankind will have great strategic significance for the society and economy of the entire country [17–19].

2.2. Protocols in Wireless Sensor Networks. There are many routing protocols in wireless sensor networks, which can be mainly divided into three categories. They are data-centric routing protocols represented by directed diffusion [20], hierarchical routing protocols represented by LEACH [21], and location-based routing protocol represented by GEAR [22].

However, these routing algorithms proposed for wireless sensor networks only improve the application of the network as much as possible but do not fully consider security issues. In recent years, the academic community has conducted research on the security of wireless sensor networks from different levels and angles. Literature [23] and literature [24] research on routing security in wireless sensor networks. The work in this area mainly uses encryption and authentication technology; the purpose is to establish a reliable and energy-efficient multihop routing path for data transmission. Literature [25] and literature [26], respectively, proposed new broadcast authentication protocols based on the μTESLA protocol. Literature [27] proposed a sensor network security protocol SPIN to solve the problems of sensor network node key agreement, point-to-point authentication, and data freshness. Literature [28, 29] proposed a secure LEACH protocol (SecLEACH) on the basis of random key distribution, SPIN, and μTESLA. Literature [30] introduces a security authentication scheme between nodes and proposes a secure LEACH protocol to contain abnormal nodes, namely, SLEACH.

Although many results have been achieved, there are still many security issues and security protocols that need to be further studied.

The use of encryption and authentication technology can effectively resist external forged routing information and improve the security of the routing protocol. But it affects the efficiency of the system. In wireless sensor networks, public key cryptography cannot be used. Therefore, the μTESLA mechanism is less efficient when the number of sensor nodes is large.

Biological immune system is a highly distributed, parallel, and adaptive system. The system has good robustness and high complexity. This provides important clues to building a robust computer security system. The wireless sensor network is a typical distributed, self-organizing environment, which can learn from the working principle of the biological immune system. Literature [31] first proposed a wireless sensor network security architecture based on biological immunity, mainly using the idea of an intrusion detection system, but did not give a specific implementation plan. The processing of malicious nodes is only a kind of simple intrusion isolation.

3. Method

3.1. Wireless Communication Network Hierarchical Trust Management Model. Although in the literature [32], a wireless communication network hierarchical trust management model is proposed. However, the network model does not consider the decision-making role of the base station (BS). In addition, it does not provide a security protocol to implement network security mechanisms and related algorithms. The cluster head of this model is relatively fixed. The cluster heads in our system are dynamic and changeable. For this reason, we designed an algorithm for cluster head reselection. In this way, our system is abler to adapt to the complexity and variability of the real environment.

Our main purpose of designing the trust management system is to protect WSN from malicious actions of attackers. We combine reliability with the ability to resist attacks for as long as possible. Energy efficiency refers to the ability to maintain the operability of the network for as long as possible using less energy. To reduce energy consumption, we adopt the following measures:

(1) One way to reduce the power consumption of a sensor is to change it from an active state to a "sleep" state to minimize its energy consumption. This can be achieved by reducing packet forwarding between nodes. Under this model, WSN is divided into multiple clusters

(2) Reduce the amount of calculation of sensor node (SN)

(3) Use the method of data aggregation to minimize the energy consumption in WSN

(4) The aggregator is used to collect information from other nodes, calculate the aggregation function, and transmit its value to the network coordinator. Compared with the situation without aggregator, the total cost of information transmission is significantly reduced

The architecture of this model is shown in Figure 1. The information collection module obtains information from the SN and uses it to calculate the trust level. Then, according to the node type, the results are analyzed. SN does not trust the connection management module. This module processes information about node N. If node N successfully passes the test, the data associated with N goes into the trusted node table. Therefore, all nodes in the same cluster will receive messages about node N. If node p detects that there is an abnormality in node q, node p will send a message to CH, and CH will make a decision about node q.

(1) Information collection module

Two nodes in the same wireless transmission and reception range are called neighbours. Due to the broadcast characteristics of the wireless medium, a given node can collect first-hand information about data packets. By listening to all frames received by the MAC layer and recording the transmission data of the data packet, the behavior of its neighbouring nodes is forwarded. If it is a cluster-based WSN, a condition must be added. The condition is that the nodes must be in the same cluster.

(2) Trust level calculation module

We have given a formula for calculating the trust level.

$$A_{pq} = \frac{i_1 X_{pq} - i_2 Y_{pq}}{i_3 X_{pq} - i_4 Y_{pq}}. \tag{1}$$

Here, A_{pq} is the trust value of node p with respect to node q, X_{pq} is the number of successful events of q measured by p, and Y_{pq} is the number of failed events of q measured by p. And i_1, i_2, i_3, and i_4 represent the weight/importance of successful events relative to the weight/importance of failure events. Each network event will calculate the trustworthiness value. The trust values associated with these behaviors are then multiplied by the weight factor X to reflect their importance in the security level. Add them together to get the reliability of the entire node. The specific calculation formula is shown in formula (2). Further, we can obtain the level of stability.

$$G_{pq} = \sum_{i=1}^{m} x_i * A_{pq}, \tag{2}$$

$$\mathrm{Le} = \frac{x_1 * E + x_2 * d * G_{pq}}{x_3 * L}. \tag{3}$$

Among them, E refers to the remaining energy level; L refers to the mobility level of the node; d refers to the distance from the base station; Le refers to the stability level;

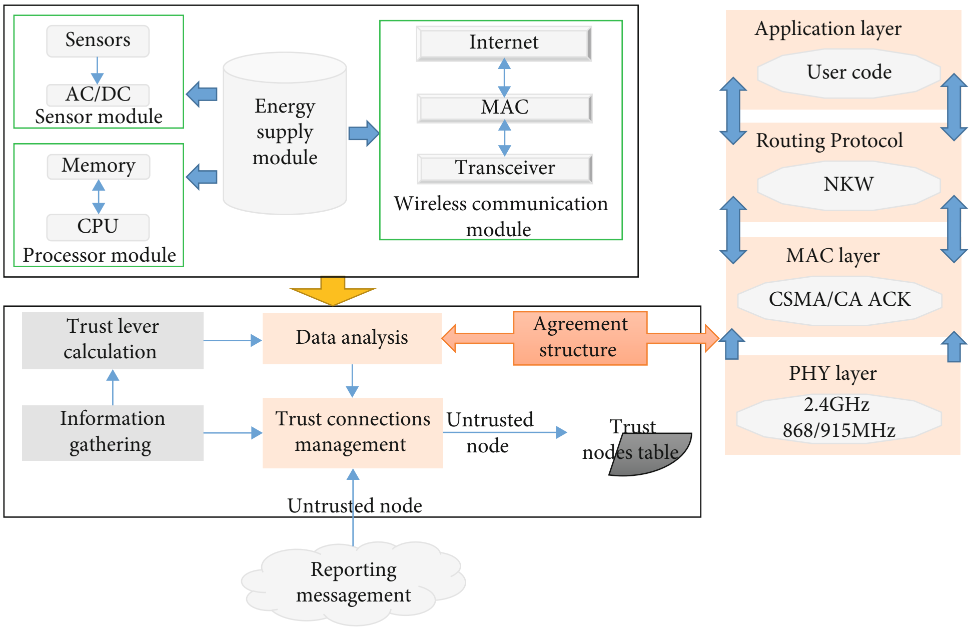

Figure 1: The architecture of the trust management system.

(3) Trusted connection management module

The module works according to the following algorithm to determine the confidence level:

(1) CH gets the parameters from the analyzer

(2) CH requests sensor node a to provide E_a and G_a

(3) CH uses formula (2) to calculate G_b according to the received parameters

(4) CH compares the values: if $G_a = G_b$, continue the algorithm; otherwise, the incorrect value of a will become untrusted

(5) CH compares E with the number of packets sent

The following conditions should be maintained:

$$\begin{aligned} E &= \max\left(0, E_a\right), \\ E &= \min\left(0, E_a\right), \\ E &= \operatorname{avg}(0, E_a), \\ \mathrm{Tp} &= \max\left(\min\left(0, E_a\right)\right), \\ \mathrm{Tp} &= \min\left(\operatorname{avg}(0, E_a)\right), \\ \mathrm{Tp} &= \operatorname{avg}(\max\left(0, E_a\right)). \end{aligned} \tag{4}$$

(6) If these conditions can be maintained, then a is credible; otherwise, it is necessary to analyze the type of data packet sent

If most packets are managed, a is untrusted. If most packets are routed, a is untrusted. If most packets are of data type, then a is indeterminate. So let us do the analysis under this condition.

3.2. Security Protocol for Managing Mobile Clustered Wireless Sensor Network. This article provides a protocol to protect mobile sensor networks from all major types of network attacks, while not significantly reducing the power consumption of nodes and the life expectancy of their networks.

The base station sends the initialization message to all network nodes. All nodes therefore receive the information and send a response message to the BS in the same way according to the timeout definition. The BS receives the information about the node and checks the ratio of serial numbers. The last step in the initialization process is a message from the base station. This message will be sent to all configured nodes, and if any node does not receive the message, the BS will consider it suspicious or malicious. Nodes that have been initialized are marked as trusted.

On the other hand, the BS will also add these nodes to the list of trusted nodes, and future cluster heads will be selected from these nodes. The initialization process has two purposes. First, establish a trusted connection between the base station and the node. Second, the base station can store the preloaded list of trusted nodes in the network and compare the data it obtains with its own dynamic list.

The BS announces the start of CH selection and sends a special message M to each node. The BS executes the node initialization algorithm to determine the confidence level of the network node. If a node has been successfully verified, the base station will indicate that the node can become a CH. BS requests verified nodes to provide E. BS grades the value of E and calculates the average value. If the value of E of a is greater than or equal to the average value, it will be selected as a temporary CH. The base station sends a cluster head election to each node finished message.

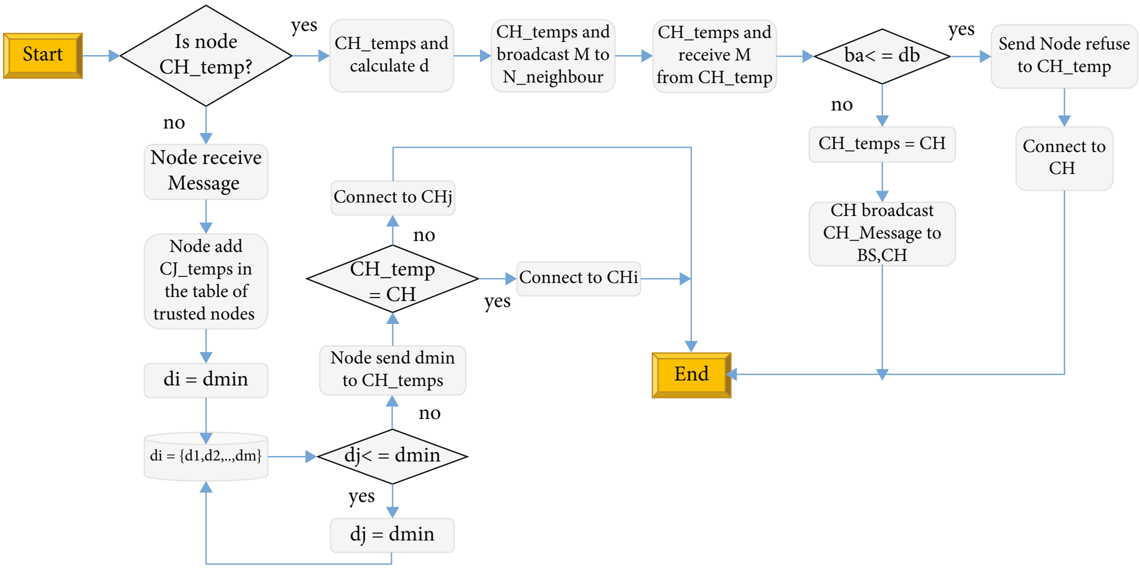

Figure 2: Network clustering algorithm.

In addition, the BS sends a message that it may become a CH to each potential cluster head CH_temp.

When the BS completes the selection of potential cluster heads, it starts the network clustering algorithm. The idea of the algorithm is that each temporary cluster head must calculate the distance d between CH_temp and BS. After that, CH_temp sends the value of d together with the proposal to join the cluster to neighbouring nodes. Next, each node determines the minimum value it receives and confirms the corresponding CH_temp. On the other hand, each CH_temp compares its d value with the neighbour's d value. If its own value is the smallest, CH_temp can be self-styled as a cluster head and notify all its neighbours and BS. Figure 2 shows the network clustering algorithm.

The BS periodically sends requests to the CH regarding the following:

$$\text{request} = (E, G, L, d). \tag{5}$$

3.3. Based on LEACH Wireless Sensor Network Immune System. There are many architectures of WSN, such as hierarchy architecture and clustering architecture. The protocol of hierarchical architecture consists of three operations, namely, network initialization and maintenance protocol, MAC protocol, and routing protocol. The receiver-oriented distributed time division multiple access (TDMA) channel allocation protocol is adopted in the data transmission phase, and the "hidden" and "exposed" problems can be avoided by appropriate channel allocation algorithm. The clustering architecture consists of clusters of sensor nodes, each of which is controlled by a cluster head. The performance of stability is sacrificed to reduce protocol overhead. The architecture based on LEACH has good stability and cost performance. Therefore, this paper chooses leach-based architecture.

The LEACH protocol divides all nodes into several clusters. Each cluster elects a leader. Cluster leaders can also form higher-level clusters. The cluster leader receives the data sent by the nodes in the cluster, realizes the data fusion function, and sends data to the base station. Since sending data to the base station consumes a lot of power, the leader needs to be reelected at regular intervals to ensure that the power consumption is evenly distributed among all nodes.

The protocol has two operating phases: cluster establishment phase and stable operation phase. In order to reduce the protocol overhead, the duration of the stable operation phase is longer than the cluster establishment phase.

The basic idea of LEACH is to randomly select cluster head nodes in a circular manner and evenly distribute the energy load of the entire network to each sensor node, so as to achieve the purpose of reducing network energy consumption and improving the overall survival time of the network. The protocol defines the concept of "round." Each round can be divided into two phases: the cluster establishment phase and the stable phase of data transmission.

In order to save resource overhead, the duration of the stable phase is greater than the duration of the setup phase. In the cluster establishment stage, the cluster head is selected first, and the selection of the cluster head node is based on the total number of cluster head nodes required in the network and the number of times each node has become a cluster head so far.

The specific selection method is each sensor node selects a value belong to [0, 1]; if the selected value is less than a certain threshold Tre, then this node becomes the cluster head node. The threshold Tre is calculated as formula (6):

$$\text{Tre} = \frac{k}{1 - k(r * \text{mod}\,(1/k))}. \tag{6}$$

Among them, k is the percentage of cluster head nodes to the total number of nodes, r is the current round number, s is the set of nodes that have not acted as cluster heads in the past $1/k$ rounds, and the symbol mod is the modulus operator (as shown in Figure 3).

The immune system of wireless sensor network based on LEACH can be expressed as a 4-tuple $\{S, G, Ag, F\}$.

$$T = \{ S, G, Ag, F \}. \tag{7}$$

Among them, S is the self-individual collection. Ag is the collection of antigens to be detected. F is the set of discriminant functions.

In order to design a data security immune system structure, it is necessary to combine the characteristics of wireless sensor networks and add some new functional nodes. In order to make the wireless sensor network have immune function, a kind of node with immune function will be added, which is called immune node. Consider the possible attacks of wireless sensor networks that cause malicious nodes to become cluster heads. In this case, if it is not stopped, the work of the entire cluster will not be completed normally.

In order to deal with this situation, the article uses a backup cluster head strategy and introduces a fifth type of node, that is, the backup cluster head.

This article puts the immunoassay step in the data fusion process and introduces the self-gene bank G. Since the computing power and energy performance of the base station are much higher than that of ordinary sensor nodes, it can be assumed that the effectiveness of the base station in identifying malicious data is quite high. The majority voting mechanism of immune nodes makes its overall credibility relatively high.

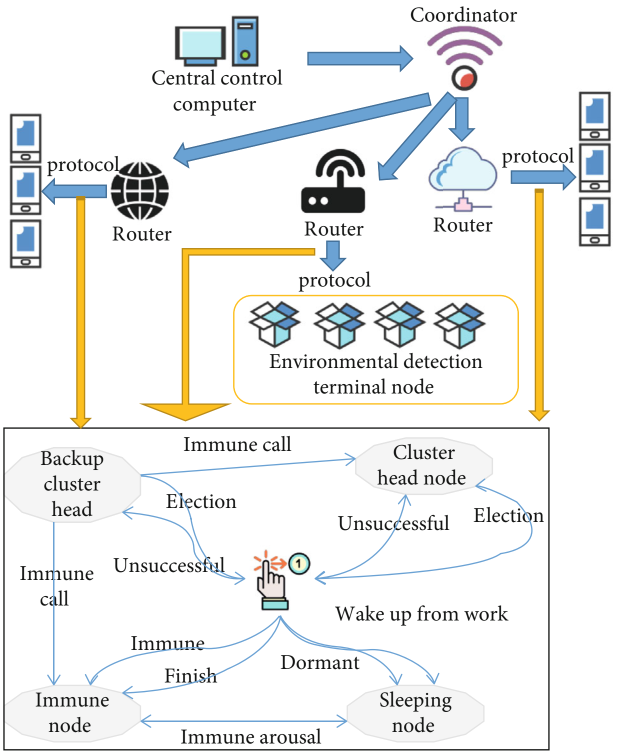

FIGURE 3: The design of the immune system structure based on LEACH.

4. Results and Discussion

4.1. Conspiracy Attack Experiment. Figure 4 shows the accuracy of the wireless communication network hierarchical trust management model and other models designed in this paper under collusion attacks when the percentage of malicious servers in WSNs ranges from 10% to 90%.

As can be seen in the figure, the results of BTRM [33], Eigen [34], and the model in this paper are basically similar; until the percentage of malicious servers is less than 70, the result of BTRM is better. When the percentage of malicious servers is greater than 80, the accuracy of TMS [35] is between 60 and 50%, indicating that there are certain security flaws. But the results of other simulation models are basically the same or worse, and our model can deal with 70% of malicious nodes, which is satisfactory to us.

4.2. Oscillation Attack Experiment. In the oscillatory network, our accuracy is higher. Figure 5 shows that all models except BTRM have an accuracy higher than 50%. Therefore, although the model in this paper does not achieve the best results in the selection percentage of credible servers, despite this, its accuracy is still higher than 70%, and the model in this paper has the lowest energy consumption value in all experiments.

4.3. Collusion and Oscillation Attack Experiment. When conducting collusion and oscillation attacks, the performance of the BTRM model is the least satisfactory. As shown in Figure 6, when the number of malicious servers exceeds 40%, the accuracy of the model is less than 70%. It can be said that the model has some shortcomings, while other models can last up to 60% of malicious servers. When the malicious server exceeds 70%, the accuracy is about 50%; this result is acceptable. After testing, it can be seen that our model performs well, and the energy consumption level is lower than other models.

4.4. Energy Difference between Nodes. In wireless sensor networks, the energy difference between nodes reflects the balance of energy consumption between nodes. The energy difference is defined as the difference between the maximum residual energy and the minimum residual energy of the nodes in the network. The smaller the energy difference between nodes, the more uniform the energy consumption of the network, and the longer the life of the network. In this experiment, we compare the energy difference between several algorithms.

Figure 7 compares the energy difference of several algorithms. In Figure 7, the abscissa represents the number of nodes in the network, and the ordinate represents the magnitude of the energy difference.

It can be seen from the figure that the energy difference of the L-PEDAP algorithm is the largest. The reason is that in L-PEDAP, each node needs to periodically establish a local minimum spanning tree. Because L-PEDAP has an

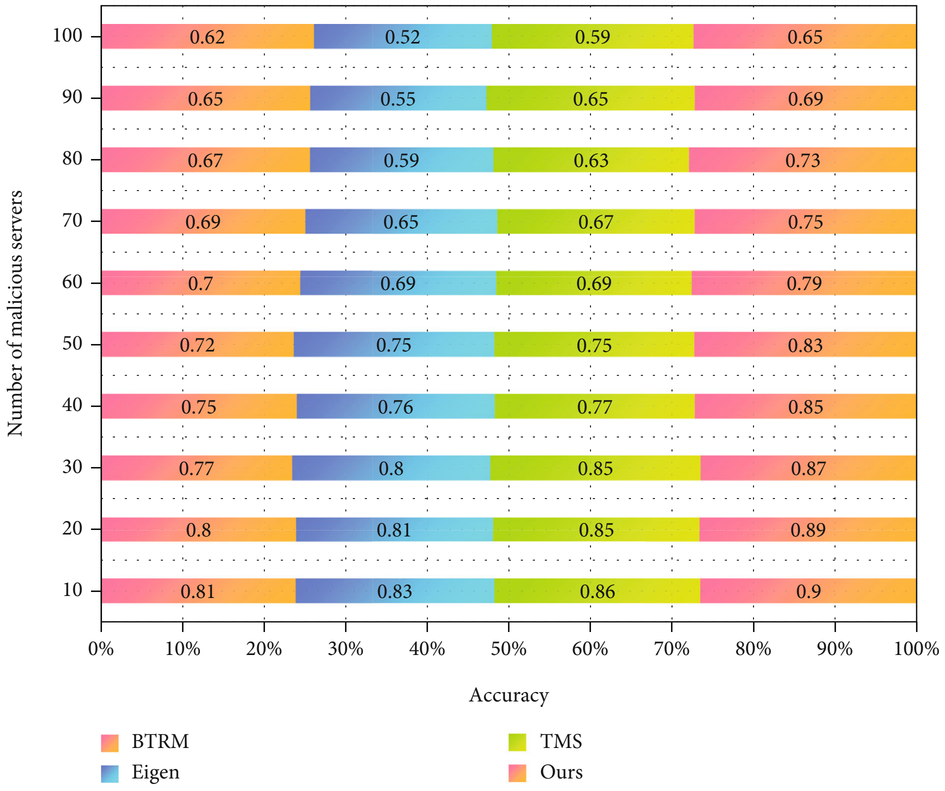

Figure 4: Accuracy of dynamic WSN under collusion attack.

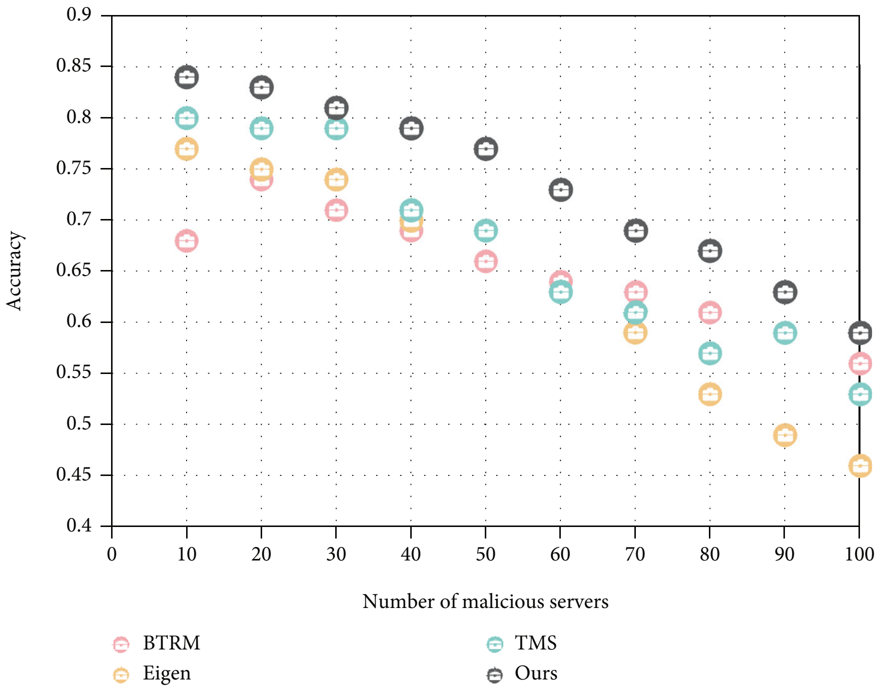

Figure 5: Accuracy of dynamic WSN under oscillation attack.

energy sensing function, the weights of edges in the established network graph are always changing. L-PEDAP can locally balance the energy consumption of nodes, and the more neighbours, the higher the energy consumption of nodes. This is because when the node density is high, when establishing a local minimum spanning tree, each node needs to communicate with neighbour nodes to obtain the remaining energy information of the neighbour nodes.

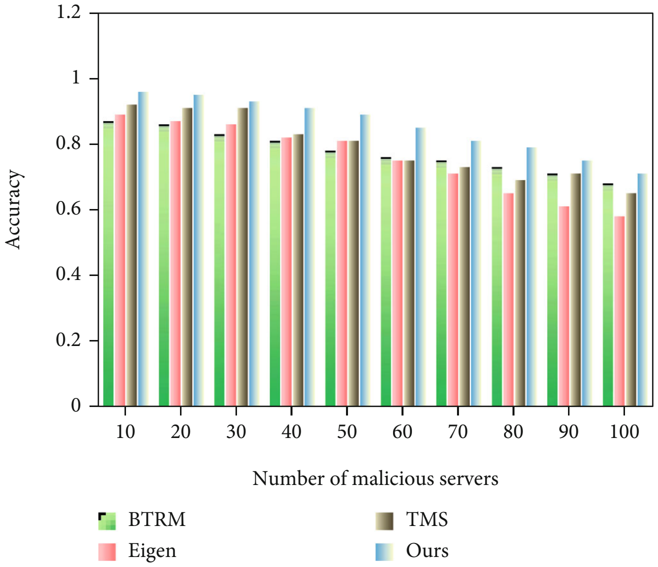

Figure 6: Accuracy of dynamic WSN under collusion and oscillation attacks.

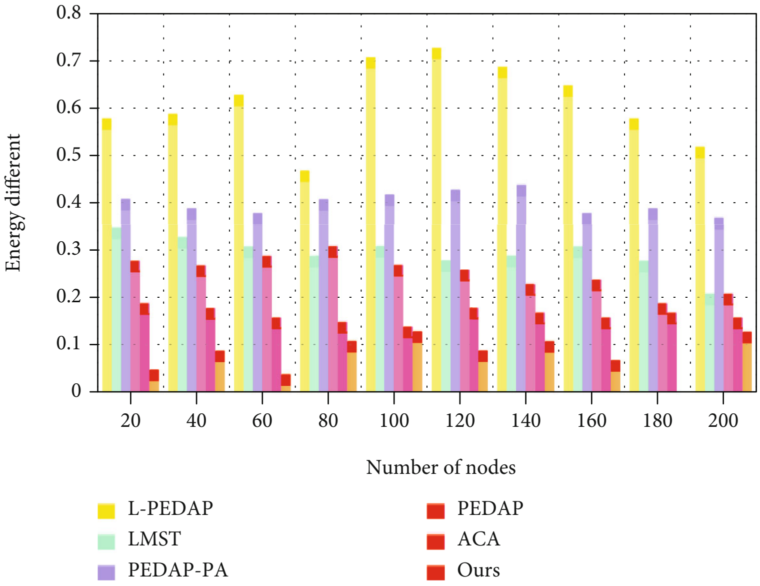

Figure 7: Energy difference after transmitting 200 packets.

Therefore, nodes with many neighbours will consume a lot of energy when building a local minimum spanning tree. Conversely, nodes with fewer neighbours will not consume much energy. Due to the random distribution of the network and the unevenness of the node density, both types of nodes will exist in the network. Therefore, there will be a large energy difference in L-PEDAP. The energy difference of this system is the smallest. The more uniform the energy consumption of the network, the longer the life of the network.

4.5. Immune Function. In the case of not being attacked, the network architecture system after the immune function is added in the life cycle and the number of data packets received by the BS; the simulation results are shown in Figure 8. The result proves that after adding immune function, it has little effect on LEACH performance.

Corresponding to the network life cycle, it can be seen that in the four methods in Figure 8, the data packets received by the base station show a linear upward trend during their respective life cycles. The three security policies and LEACH without security policies are received at the base station. There is not much difference in the number of data packets received. However, due to the different network life cycles, the final received data packets are also quite different.

Because the immune system proposed in this article is embedded with digital genes. Therefore, when a malicious node sends malicious data to the cluster head, in the data fusion stage, the cluster head can find the malicious node and invoke an immune response to it. After that, the

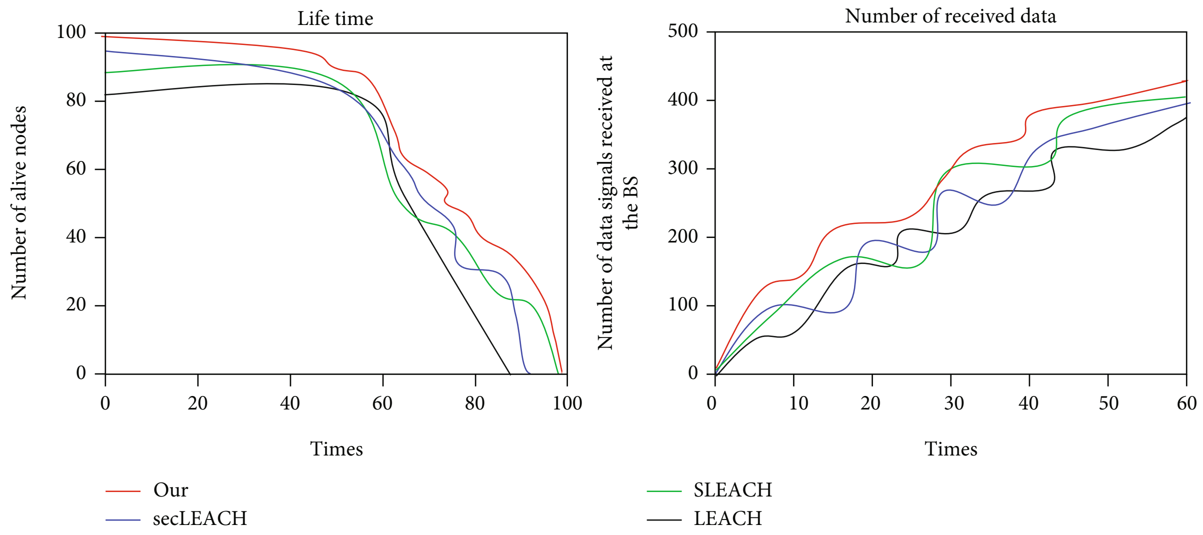

Figure 8: The life cycle of the network architecture system and the number of packets received.

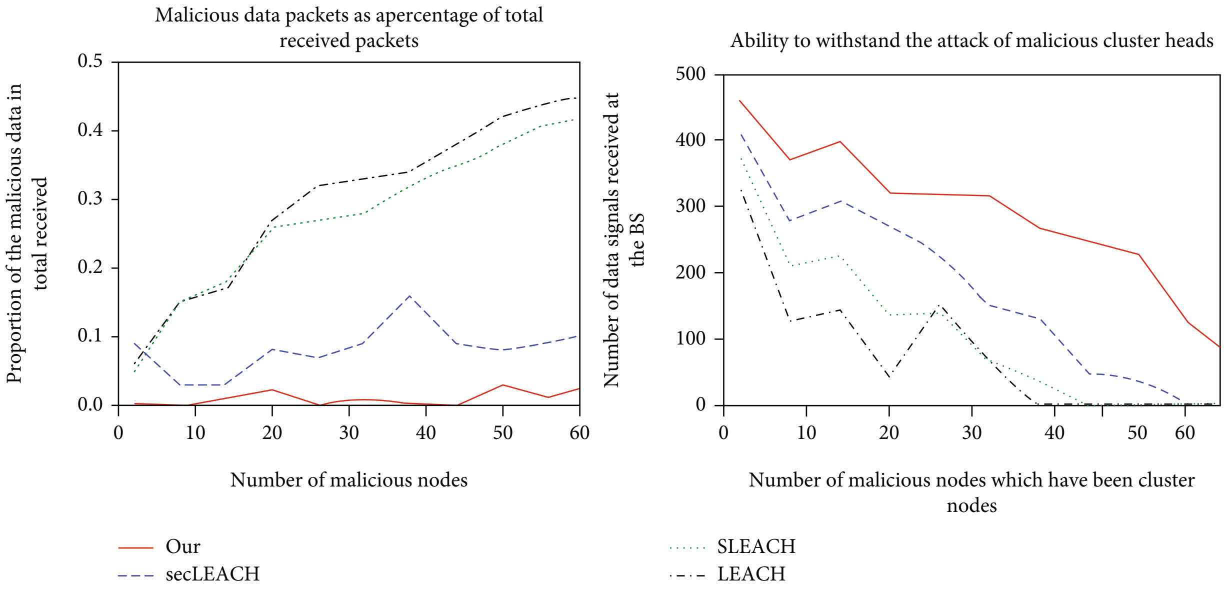

Figure 9: The proportion of malicious data packets in the total received packets and the ability to withstand the attack of malicious cluster heads.

malicious node will not have an impact on the entire network. The simulation results of SecLEACH's and SLEACH's ability to resist malicious nodes joining the cluster are compared with the method in the paper as shown in Figure 9. SecLEACH has poor performance in this respect, almost the same as LEACH without safety functions. This is because it does not solve the authentication problem when the member nodes enter the cluster. Because SLEACH adopts node authentication, its resistance in this respect has the same effect as the method in this paper.

The damage of Hello flooding attack to LEACH is considerable. When a malicious node becomes the cluster head, the function of the entire cluster will be invalid, which is equivalent to false death. A similar Hello flooding attack is used to verify the performance of the algorithm. Here, 60 common malicious nodes that become cluster heads are used to compare the antiattack ability of each scheme. The simulation results are shown in Figure 9. Although the performance of SecLEACH in this respect is slightly higher than the method in the text, but SecLEACH is a centralized strategy, and the validity of the cluster head needs to be verified by the base station. The sensor nodes in the network have no energy consumption in this respect. And as a result, the base station can easily expose its own private data, which creates new problems. The method in this paper does not rely on the distributed strategy of the base station at all.

It can be seen from the above analysis that the performance of the network architecture system designed in this paper is generally optimal. Under the premise of not relying on the base station, the influence of malicious data on the final result is excluded, and the loss of the malicious node as a cluster head is minimized.

5. Conclusion

Under the premise of considering information security, this paper first developed a trust management system based on clustered wireless sensor network. It can resist most known network attacks without significantly reducing the energy power of sensor nodes. And for the efficient and energy-saving operation of the system, on the basis of LEACH protocol, the principle of biological immune system is used for reference to optimize the wireless sensor network and further proposed a new immune system structure suitable for wireless sensor networks. The experimental results show that the wireless sensor network model designed in this paper solves the high-efficiency and energy-saving design task and has ideal robustness on the basis of a small amount of energy overhead, and the system has good practicability.

The research on data security immunity in wireless sensor networks is still a relatively new field. Due to the limitation of network resources, energy consumption, algorithm efficiency, and overall performance need to be considered comprehensively. Further research is needed to design an optimal immune system.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] A. D. Salman, O. I. Khalaf, and G. M. Abdulsaheb, "An adaptive intelligent alarm system for wireless sensor network," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 15, no. 1, pp. 142–147, 2019.

[2] M. Abdulkarem, K. Samsudin, F. Z. Rokhani, and M. F. A Rasid, "Wireless sensor network for structural health monitoring: a contemporary review of technologies, challenges, and future direction," *Structural Health Monitoring*, vol. 19, no. 3, pp. 693–735, 2020.

[3] C. Zhan, Y. Zeng, and R. Zhang, "Energy-efficient data collection in UAV enabled wireless sensor network," *IEEE Wireless Communications Letters*, vol. 7, no. 3, pp. 328–331, 2018.

[4] I. Tomić and J. A. McCann, "A survey of potential security issues in existing wireless sensor network protocols," *IEEE Internet of Things Journal*, vol. 4, no. 6, pp. 1910–1923, 2017.

[5] B. Cao, J. Zhao, Y. Gu, S. Fan, and P. Yang, "Security-aware industrial wireless sensor network deployment optimization," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 8, pp. 5309–5316, 2020.

[6] D. Mohammed, M. Omar, and V. Nguyen, "Wireless sensor network security: approaches to detecting and avoiding wormhole attacks," *Journal of Research in Business, Economics and Management*, vol. 10, no. 2, pp. 1860–1864, 2018.

[7] P. Kumar, S. Kumari, V. Sharma, A. K. Sangaiah, J. Wei, and X. Li, "A certificateless aggregate signature scheme for healthcare wireless sensor network," *Sustainable Computing: Informatics and Systems*, vol. 18, pp. 80–89, 2018.

[8] M. V. Babu, J. A. Alzubi, R. Sekaran, R. Patan, M. Ramachandran, and D. Gupta, "An improved IDAF-FIT clustering based ASLPP-RR routing with secure data aggregation in wireless sensor network," *Mobile Networks and Applications*, vol. 26, no. 3, pp. 1059–1067, 2021.

[9] D. Qin, S. Yang, S. Jia, Y. Zhang, J. Ma, and Q. Ding, "Research on trust sensing based secure routing mechanism for wireless sensor network," *IEEE Access*, vol. 5, pp. 9599–9609, 2017.

[10] R. E. Mohamed, A. I. Saleh, M. Abdelrazzak, and A. S. Samra, "Survey on wireless sensor network applications and energy efficient routing protocols," *Wireless Personal Communications*, vol. 101, no. 2, pp. 1019–1055, 2018.

[11] J. John and P. Rodrigues, "A survey of energy-aware cluster head selection techniques in wireless sensor network," *Evolutionary Intelligence*, pp. 1–13, 2019.

[12] S. An, B. H. Lee, and D. R. Shin, "A survey of intelligent transportation systems," in *2011 third international conference on computational intelligence, communication systems and networks*, pp. 332–337, Bali, Indonesia, 2011.

[13] D. A. Hahn, A. Munir, and V. Behzadan, "Security and privacy issues in intelligent transportation systems: classification and challenges," *IEEE Intelligent Transportation Systems Magazine*, vol. 13, no. 1, pp. 181–196, 2021.

[14] A. Sedrati and A. Mezrioui, "A survey of security challenges in Internet of Things," *Advances in Science, Technology and Engineering Systems Journal*, vol. 3, no. 1, pp. 274–280, 2018.

[15] S. Khanam, I. B. Ahmedy, M. Y. Idna Idris, M. H. Jaward, and A. Q. Bin Md Sabri, "A survey of security challenges, attacks taxonomy and advanced countermeasures in the Internet of Things," *IEEE Access*, vol. 8, pp. 219709–219743, 2020.

[16] D. Kumar, S. Chand, and B. Kumar, "Cryptanalysis and improvement of an authentication protocol for wireless sensor networks applications like safety monitoring in coal mines," *Journal of Ambient Intelligence and Humanized Computing*, vol. 10, no. 2, pp. 641–660, 2019.

[17] R. Lajara, J. J. Pérez-Solano, and J. Pelegrí-Sebastiá, "Predicting the batteries' state of health in wireless sensor networks applications," *IEEE Transactions on Industrial Electronics*, vol. 65, no. 11, pp. 8936–8945, 2018.

[18] M. E. Haque and U. Baroudi, "Ambient self-powered cluster-based wireless sensor networks for industry 4.0 applications," *Soft Computing*, vol. 25, no. 3, pp. 1859–1884, 2021.

[19] A. Rajput and V. B. Kumaravelu, "FCM clustering and FLS based CH selection to enhance sustainability of wireless sensor networks for environmental monitoring applications," *Journal of Ambient Intelligence and Humanized Computing*, vol. 12, no. 1, pp. 1139–1159, 2021.

[20] J. Mu, X. Yi, X. Liu, and L. Han, "An efficient and reliable directed diffusion routing protocol in wireless body area networks," *IEEE Access*, vol. 7, pp. 58883–58892, 2019.

[21] N. Gharaei, K. A. Bakar, S. Z. M. Hashim, A. H. Pourasl, and S. A. Butt, "Collaborative mobile sink sojourn time optimization scheme for cluster-based wireless sensor networks," *IEEE Sensors Journal*, vol. 18, no. 16, pp. 6669–6676, 2018.

[22] W. Tang, K. Zhang, and D. Jiang, “Physarum-inspired routing protocol for energy harvesting wireless sensor networks,” *Telecommunication Systems*, vol. 67, no. 4, pp. 745–762, 2018.

[23] X. Fu, G. Fortino, P. Pace, G. Aloi, and W. Li, “Environment-fusion multipath routing protocol for wireless sensor networks,” *Information Fusion*, vol. 53, pp. 4–19, 2020.

[24] K. A. Darabkh, M. Z. El-Yabroudi, and A. H. El-Mousa, “BPA-CRP: a balanced power-aware clustering and routing protocol for wireless sensor networks,” *Ad Hoc Networks*, vol. 82, pp. 155–171, 2019.

[25] V. Vijayalakshmi and A. Senthilkumar, “USCDRP: unequal secure cluster-based distributed routing protocol for wireless sensor networks,” *The Journal of Supercomputing*, vol. 76, no. 2, pp. 989–1004, 2020.

[26] T. Khan and K. Singh, “TASRP: a trust aware secure routing protocol for wireless sensor networks,” *International Journal of Innovative Computing and Applications*, vol. 12, no. 2-3, pp. 108–122, 2021.

[27] A. I. Saleh, K. M. Abo-Al-Ez, and A. A. Abdullah, “A Multi-Aware Query Driven (MAQD) routing protocol for mobile wireless sensor networks based on neuro-fuzzy inference,” *Journal of Network and Computer Applications*, vol. 88, pp. 72–98, 2017.

[28] S. Varshney, C. Kumar, and A. Swaroop, “Leach based hierarchical routing protocol for monitoring of over-ground pipelines using linear wireless sensor networks,” *Procedia Computer Science*, vol. 125, pp. 208–214, 2018.

[29] J. Bhola, S. Soni, and G. K. Cheema, “Genetic algorithm based optimized leach protocol for energy efficient wireless sensor networks,” *Journal of Ambient Intelligence and Humanized Computing*, vol. 11, no. 3, pp. 1281–1288, 2020.

[30] J. Zhang and R. Yan, “Centralized energy-efficient clustering routing protocol for mobile nodes in wireless sensor networks,” *IEEE Communications Letters*, vol. 23, no. 7, pp. 1215–1218, 2019.

[31] X. Xiao and R. Zhang, “A danger theory inspired protection approach for hierarchical wireless sensor networks,” *KSII Transactions on Internet and Information Systems (TIIS)*, vol. 13, no. 5, pp. 2732–2753, 2019.

[32] W. Meng, W. Li, C. Su, J. Zhou, and R. Lu, “Enhancing trust management for wireless intrusion detection via traffic sampling in the era of big data,” *IEEE Access*, vol. 6, pp. 7234–7243, 2018.

[33] V. R. S. Dhulipala and N. Karthik, “Trust management technique in wireless sensor networks: challenges and issues for reliable communication: a review,” *CSI Transactions on ICT*, vol. 5, no. 3, pp. 281–294, 2017.

[34] M. Kaushik, S. H. Gupta, and V. Balyan, “Evaluating threshold distance by using eigen values and analyzing its impact on the performance of WBAN,” in *2019 6th international conference on signal processing and integrated networks (SPIN)*, pp. 864–867, Noida, India, 2019.

[35] J. Kim and J. Son, “An establishment of super Wi-Fi environment in ships based on UHF system of TMS,” *KSII Transactions on Internet and Information Systems (TIIS)*, vol. 12, no. 5, pp. 2103–2123, 2018.