Hindawi
Mobile Information Systems
Volume 2022, Article ID 2067628, 11 pages
https://doi.org/10.1155/2022/2067628

Research Article

A Data Symmetry Algorithm-Based Security Awareness Model for Emergency Wireless Communication under Multisensor Fusion

Ye Liang and Nan Gao

School of Electronic Engineering, Lanzhou City University, Lanzhou, Gansu 730070, China

Correspondence should be addressed to Ye Liang; liangye@lzcu.edu.cn

Received 27 January 2022; Revised 21 February 2022; Accepted 22 February 2022; Published 31 March 2022

Academic Editor: Hye-jin Kim

Due to the characteristics of sensor networks, wireless sensor networks (WSN) have a series of security threats in their applications. For example, wireless sensor networks are vulnerable to attacks such as eavesdropping, data tampering, and jamming. The processing capacity of sensor nodes is limited, and its integrity and confidentiality are greatly threatened. Nodes are easily captured or counterfeited; control of the energy of nodes; encryption and decryption of data depends on the distribution and management of keys; how to ensure the legal networking and access of nodes, etc. With the deepening and gradual promotion of WSN research, these security threats have become an urgent problem to be solved. In the context of multisensor fusion, this research realized the construction of a security perception model of emergency wireless communication based on the Bicycle data symmetric encryption algorithm and the use of secret sharing technology. The 16 bit Bicycle encryption and decryption time is about 1/40 of the encryption time, and the 32 bit Bicycle decryption time is about 1/30 of the encryption time, 16 bit encryption is slower than 32 bit encryption and faster decryption.

1. Introduction

The small size of nodes in wireless sensor networks, low power consumption, easy deployment, and the functions of information collection, data processing and wireless communication make it popular among researchers at home and abroad. In recent years, with the research and development of sensor network technology, wireless sensor networks have very broad application prospects both in national security and in various aspects of the national economy [1]. And in the future, it is possible to realize the development of a comprehensive sensor network that integrates sea, land and air, realize the interface between the real world and the digital world, and penetrate into all aspects of life. Its role will be no less than that of the Internet, and it will be one of the three high-tech industries in the world in the future. With the development of technology, it will play an increasingly important role in people's lives, and its safety performance will be valued by more and more researchers along with its application and development [2, 3].

Wireless sensor network is a network system formed by a large number of sensor nodes deployed in the monitoring area through wireless self-organization. Because of its convenient deployment and high security features, it has attracted great attention from domestic and foreign research fields, and was once rated as the top ten emerging technologies that will deeply affect human life in the future. In wireless sensor networks, nodes have the characteristics of limited energy and easy capture. Therefore, wireless sensor networks will be subject to some new attacks in addition to traditional attacks. For example, the captured node generates and transmits legal malicious data, causing the loss of the key, or the node's own failure to generate erroneous data. Relying solely on encryption and authentication technology cannot solve these new security problems encountered by wireless sensor networks.

The innovation of this research lies in: the use of secret sharing technology to realize the security perception model, which protects the master key well. At the same time, the concept of domain is proposed to better subdivide the network structure to ensure the safe storage and transmission of data. And the introduction of the Bicycle algorithm, which can double the amount of information transfer, and can selectively provide plaintext, which is innovative in preventing attackers from exhausting keys, and the algorithm is simple, fast, and efficient in encryption [4]. At the same time, the introduction of the hash algorithm can not only guarantee the integrity of the data, but also provide an antitampering and inspection mechanism, which guarantees security and has good technical advantages.

2. Related Work

Many scholars at home and abroad have done a lot of research on multi-sensor fusion, data symmetry algorithm, wireless communication and security perception model. Wang developed a simple model to solve the interaction between the securities lending market and the securities trading market [5–7]. When securities are easy to borrow, short selling will result in lower spot prices. When securities are difficult to borrow, any short-selling supply and demand changes should be absorbed by the lending market to a large extent, so the impact on spot prices is small [8]. Positive borrowing costs means that the negative views of short sellers are offset by the opposite views of securities lenders, so that the equilibrium securities prices only reflect the views of people who neither lend nor short [9]. Fagan specifically investigated users' motivations for following or not following computer security recommendations through a survey distributed by MechanicalTurk ($N = 290$). Fagan uses the rational decision model to guide research design and current thinking about human motivation [10]. The data shows the main cognitive gap between those who follow tested recommendations (ie update software, use password managers, use 2FA, change passwords) and those who do not, and it also helped explain the motivation behind the participant's decision. It is worth noting that Fagan found that social considerations are widely overwhelmed by individualized reasons [11]. Chen proposed a model that combines the limited attention or bounded rational nature of IoT participants [12]. In addition, Chen established an in-game game framework and proposed the Gestanash equilibrium (GNE) solution concept to characterize the agent's decision-making and quantify the limited perceived risk due to limited attention. Chen designed an iterative algorithm based on the near-end to calculate GNE [13, 14]. Through the case study of the intelligent community, the designed algorithm can successfully identify the key users who need other users to consider their decisions during the security management process [15]. Rahman developed a community-based model that defines the main responsibilities of stakeholders, including local and central governments, nongovernmental organizations, and community people working in a well-coordinated manner, which will effectively reduce the shortage of safe drinking water [16]. In order to analyze the evolution trend of cyber threats and explore the self-awareness and control of security situation, Huang incorporates a dynamic wavelet neural network model into the model design, which is a network security situation awareness based on network security situation awareness. An optimized dynamic wavelet neural network is proposed to enhance the interaction and cognitive capabilities between the various layers of the network security system [17]. Sreedharan proposed a multi-hop clustering algorithm that considers spatial correlation between nodes to form clusters and implements an energy-efficient routing scheme that selects multi-hop paths in the network in a dynamic manner [18]. Dai proposed a visible/infrared image weighted average fusion algorithm. It first requires a visible/infrared device to capture the target perimeter information, perform feature analysis, and complete antifog denoising preprocessing. These operations aim to improve the accuracy of image segmentation. Secondly, feature extraction is performed on the visible and infrared target images respectively to further complete the recognition of the target images. Finally, image fusion is performed by weighted averaging of the targets detected in the visible and infrared images. The fusion uses a matching matrix to represent the similarity of the two images [19]. The data of these studies is not comprehensive, and the results of the research are still to be discussed, so they cannot be recognized by the public, and thus cannot be popularized and applied.

3. Emergency Wireless Communication Security Perception Model

3.1. Domain-Based Network Model. Combining traditional network models and secret sharing technologies, a domain-based wireless sensor network model is proposed after research. In the model, this paper puts forward the concept of domain (as shown in Figure 1 domain P and domain Q) to better subdivide the network structure and ensure the safe storage and transmission of data [20].

In this model (Figure 1), this paper divides the entire network into a domain structure, and each domain structure includes ordinary nodes, council nodes, key nodes, and dynamic gateway nodes. Ordinary nodes are nodes that complete the collection and processing of data in the domain, and have no other functions. The council node is a network node that has the master key in the domain, and plays the role of protecting the master key. In addition, it also has the function of key distribution to the nodes in the domain. The role of key nodes is to preserve the routing relationships between nodes in the domain and adjacent domains, process and forward network data, and select the role of dynamic gateway nodes. The dynamic gateway node only plays a role in the process of network communication. This model combines a flat network structure with a hierarchical network structure and a clustering routing protocol. The key node in the model is the upper node of the network, and other nodes belong to the lower layer of the network. In the communication process, the key node selects the dynamic gateway node in the domain, and after the dynamic gateway node processes the message, it is forwarded to the gateway node in the adjacent domain. Since the dynamic gateway node belongs to the lower node, it is beneficial to protect the internal network node [21].

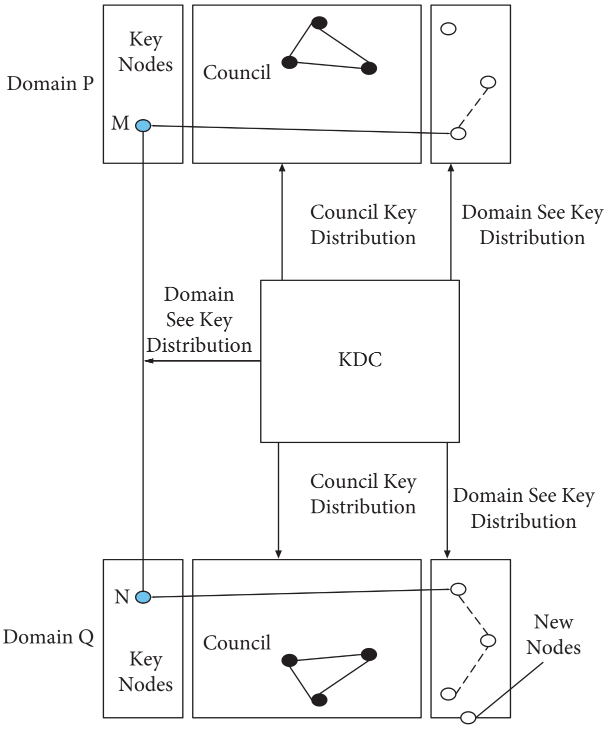


Figure 1: Intradomain structure.

3.2. Initialization of the Network Protocol

(1) A member node in the domain is dead. If the key node does not receive a data packet from a member in the domain within a certain period of time, the node is considered dead. Although in the entire WSN, the death of a cluster member will not have much impact on the entire network, in order to prevent node impersonation, we will destroy the shared key between this node and the key node to ensure the source of data security.

(2) The death of key nodes. This situation often occurs in the later stages of the network life cycle and abnormal situations, such as large energy consumption of key nodes, loss of function or key nodes are captured by the enemy, etc. In this case, we will use the council node to periodically check the network. In a certain period of time, there is no reply or the reply information is fake. At this time, the council node will re-elect a new node as a key node to ensure the reliability of network communication.

(3) The council node fails. In the sensor network, the council node may also be unexpected for some reason. In this case, let the council node periodically check and find that there is a council node less than a certain value, and it is considered that there is a node failure. At this time, the council can select a new council node and assign it to its child master key to ensure the security of the council.

(4) New nodes are added. In the network, once a new node is found to enter, the new node will send a request to the key node, after identity verification, the key node will send a request to the council, and the council will distribute the shared key within the domain to ensure secure communication.

3.3. Domain-Based Secure Communication Protocol. On the basis of the foregoing, this article further forms a secure communication protocol based on the security model of the wireless sensor network in the domain, and establishes the communication process as shown in Figure 2 to illustrate the communication protocol proposed in this article. In the communication process, unicast communication is realized between nodes and key nodes, broadcast communication is realized between key nodes and dynamic gateway nodes, and broadcast communication is realized between dynamic gateway nodes.

3.4. Routing Processing. The routing protocol is responsible for forwarding data from the source node to the destination node through the communication network. It mainly includes two aspects: finding the optimized path between the source node and the destination node, and forwarding the data packets correctly along the optimized path.

In the clustered network routing protocol, the cluster head node controls the routing information of each node in the domain, as well as the routing information between cluster heads. In this case, the failure of the cluster head node will also have a great impact on the communication between the networks, and the inaccurate selection of intercluster and intracluster routes will cause the performance of the network to decrease [22].

In the domain-based WSN secure communication model, we use the secret sharing mechanism on the basis of the clustering routing protocol and join the council structure to make the network more secure. In the process of query routing, the council node not only saves the routing information of the nodes in the domain, but also saves the routing information between adjacent domains. In this way, when a key node in the domain fails, the council node can redistribute routing information for it, which prevents the loss of routing information and can quickly find the next path for the node.

3.5. Security Analysis. In the network model of wireless sensor designed in this paper, we use the secret sharing mechanism to achieve the protection of the master key, and divide the master key into different subkeys distributed to different nodes to form the council nodes. Dynamic gateway nodes are used to achieve data forwarding in the communication process.

(1) Data integrity: in this paper, we take a secure communication method to realize the communication between domain nodes in the communication process, we forward the message through the key node and calculate the MIC check value of the message at the receiving node to verify whether the MIC is equal or not, which ensures the integrity of the message.

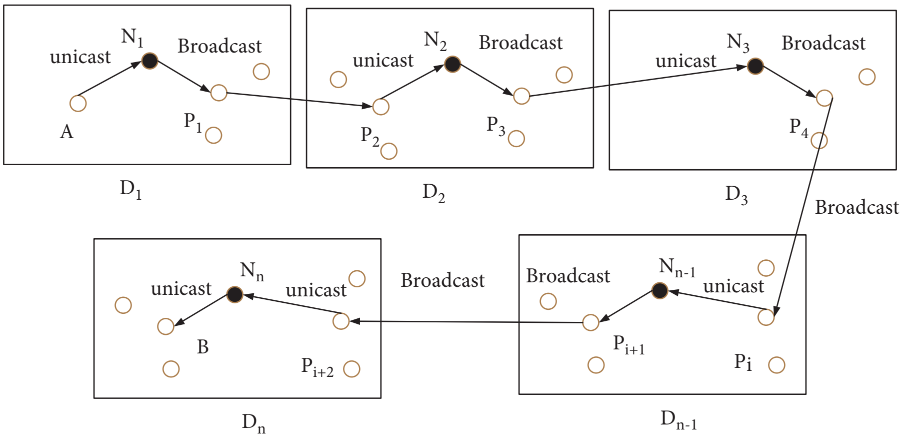


Figure 2: Secure communication process for domain-based wireless sensor networks.

(2) Data confidentiality: in the process of message transmission, we use the hash function to process the shared key between nodes to get the encryption key and the check key. In this link, we can ensure the security and confidentiality of the message by ensuring that the shared key between nodes is not disclosed.

(3) Key point attack: in this wireless sensor network, as the key nodes are in the network, they frequently communicate with different domains, which makes the nodes easy to be discovered or captured by the adversary. In this model, it proposed council node periodically detects and assigns keys to the key nodes, and once a node is found to be failed or captured, the council node re-elects a new node to ensure the continuity of the network and reassigns a new key to the node.

(4) Dynamic gateway nodes: in the designed model, dynamic gateway nodes are used to implement the forwarding of data, so that the structure of the network is shielded and the structure within the network cannot be derived from outside the domain.

(5) Protection of master key: in a hierarchical network protocol, the master key is held in the cluster head node, which manages the nodes within the cluster. The role of the cluster head node becomes important in the cluster and the master key is exposed once the node has an accident or is captured. The council nodes come to jointly manage the master keys and jointly manage the keys for the nodes in the domain; in this way, even if the key nodes fail, new key nodes can be re-elected by the council nodes to ensure the secure transmission of data.

Compared with the existing wireless sensor network secure communication model, this scheme has the following advantages.

(1) Secure communication: communication between nodes is encrypted using node-domain, domain-domain keys to ensure the security of communication.

(2) No fixed gateway: in this scheme, the gateways are dynamically selected so that the path of message transmission is not easily exposed.

(3) Reliability: secret sharing scheme is adopted, and the inter-domain key, intra-domain key and routing information are managed by the council, and when the key node fails, a new key node can be reselected by the council to ensure the continuous reliability of network communication.

In the network model designed in this paper, we use the threshold secret sharing mechanism to form a council structure to achieve the protection of the master key and to the key nodes. In this scheme, it is important to determine the appropriate threshold value to achieve the security of the network. In this paper, the relationship between the probability of node failure and the number of nodes and the threshold value is used to determine the threshold value.

3.6. Emergency Wireless Communication Model. The situational awareness model of emergency wireless communication is shown in Figure 3. The model includes multiple functional modules such as information collection, multisource fusion, and situation understanding to complete the extraction of emergency wireless communication security elements, state perception and trend prediction.

The framework of emergency wireless communication security situation integration is shown in Figure 4. In this framework model, the multisource fusion is more accurate and effective than the single-source fusion.

The data preprocessing framework model is shown in Figure 5, which mainly includes three major parts: one-time classification processing of each sensor data in the network, information fusion processing of multiple sensors, and classification correction of evidence conflict data.

4. Experimental Analysis

In this experiment, the bicycle algorithm is used to realize the symmetric encryption of data. The mathematical principle on

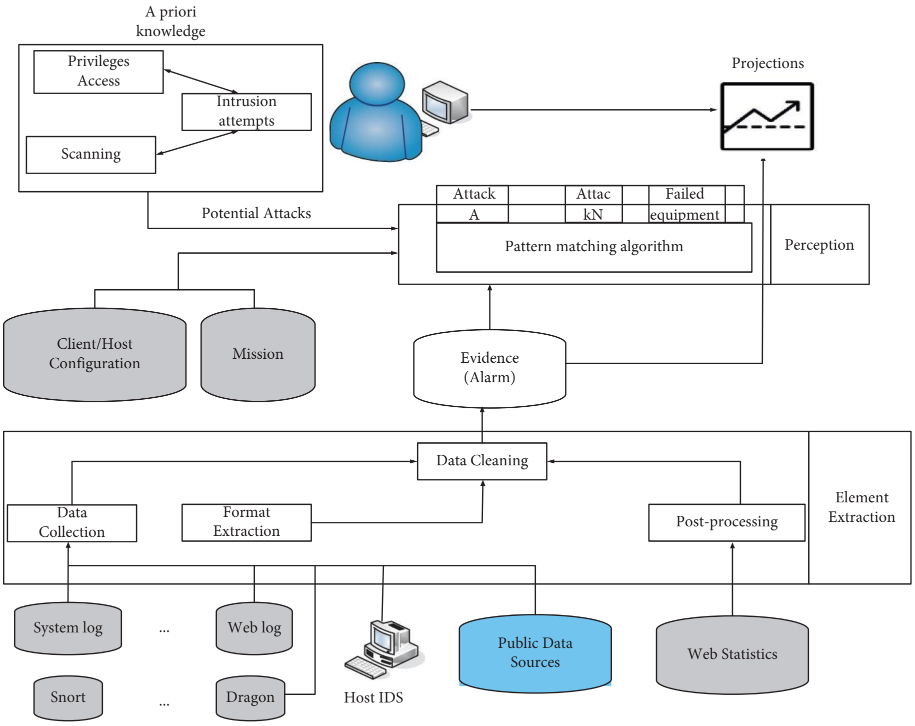


Figure 3: Network situational awareness model.

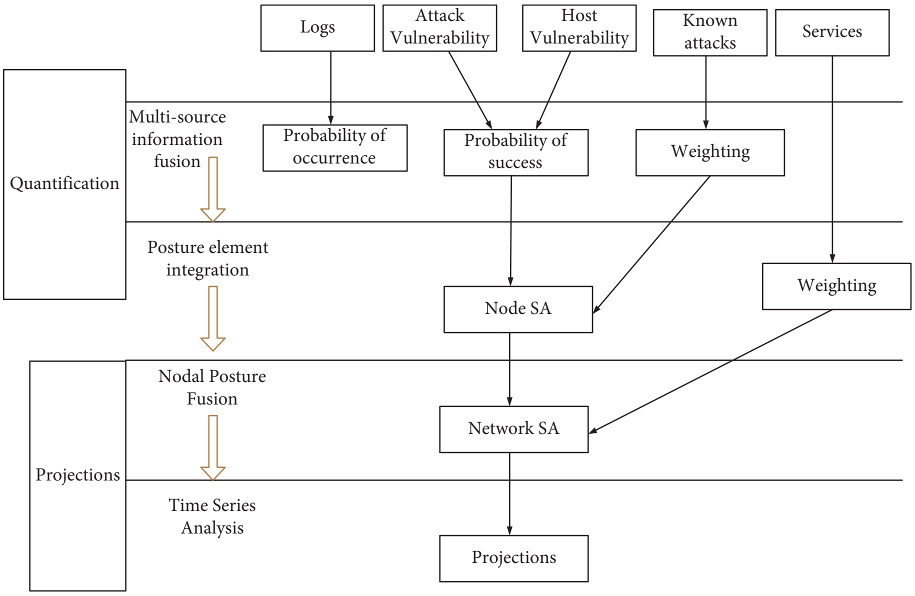


Figure 4: Cybersecurity posture fusion framework.

which the bicycle algorithm is based is in a two-dimensional rectangular coordinate system, a straight line can be determined by knowing the coordinates of two points. For this certain straight line, there is a certain slope and intercept. For this line of known slope and intercept, give the abscissa arbitrarily, and then the corresponding ordinate can be obtained.

Given two sets of keys and plaintext (key g_1, plaintext j_1) and (key g_2, plaintext j_2):

$$\begin{cases} j_1 = g_1 A + B, \\ j_2 = g_2 A + B. \end{cases} \tag{1}$$

The ciphertext s is composed of A and B together.

The communication model of the Bicycle algorithm is shown in Figure 6.

The complete structure of the Bicycle algorithm is shown in Figure 7.

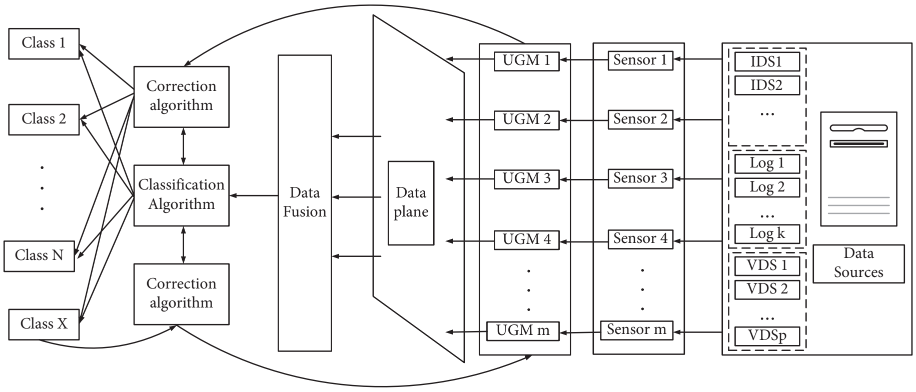


Figure 5: Cybersecurity situational awareness data preprocessing framework.

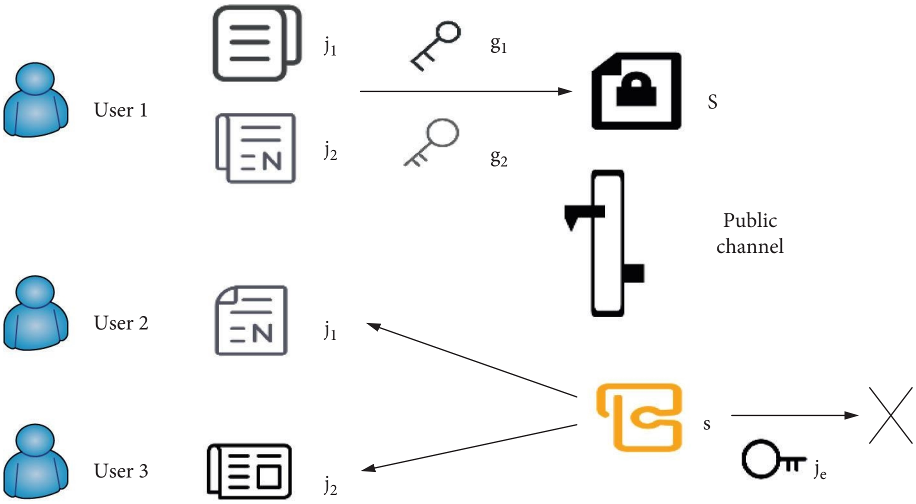


Figure 6: Communication model of the Bicycle algorithm.

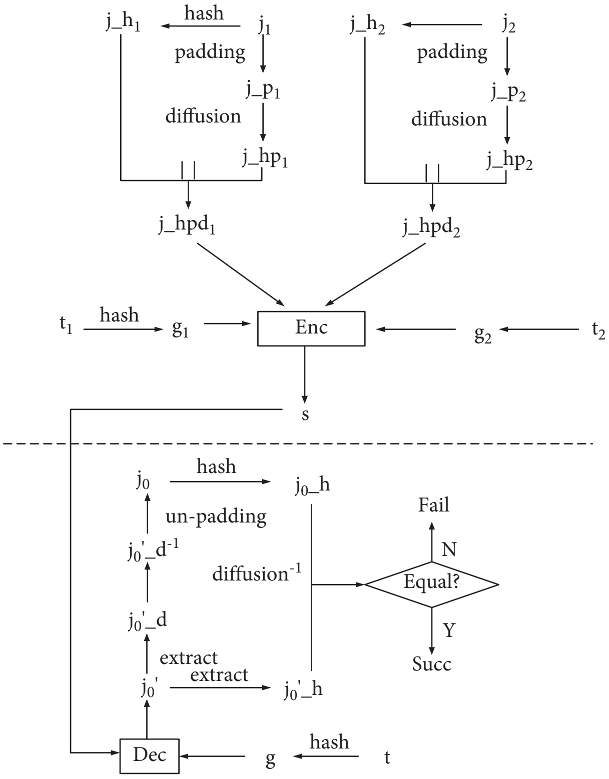


Figure 7: The complete structure of the Bicycle algorithm.

Segmentation of the algorithm:

$$\begin{aligned}
g_1 &= g_{1,1} g_{1,2} \cdots g_{1,\left(\frac{G}{L}\right)},\\
g_2 &= g_{2,1} g_{2,2} \cdots g_{2,\left(\frac{G}{L}\right)},\\
j\_hpd_1 &= j\_hpd_{1,1}\, j\_hpd_{1,2} \ldots j\_hpd_{1,i},\\
j\_hpd_2 &= j\_hpd_{2,1}\, j\_hpd_{2,2} \ldots j\_hpd_{2,i},\\
j\_hp_1 &= j\_p_1 \,\mathrm{XOR}\, j\_h_1,\\
j\_hp_2 &= j\_p_2 \,\mathrm{XOR}\, j\_h_2.
\end{aligned} \tag{2}$$

Among them, K is the key length, $i = 1, 2, 3, \ldots, n$, $\|$ means connection.

Key distribution rules:

$$g_{1,i} = \begin{cases} g_{1,1} & i \bmod \left(\frac{G}{L}\right) = 1 \\ g_{1,2} & i \bmod \left(\frac{G}{L}\right) = 2 \\ g_{1,3} & i \bmod \left(\frac{G}{L}\right) = 3 \\ \cdots & \cdots \\ g_{1,\left(\frac{G}{L}\right)} & i \bmod \left(\frac{G}{L}\right) = 0, \end{cases},$$

$$g_{2,i} = \begin{cases} g_{2,1} & i \bmod \left(\frac{G}{L}\right) = 1, \\ g_{2,2} & i \bmod \left(\frac{G}{L}\right) = 2, \\ g_{2,3} & i \bmod \left(\frac{G}{L}\right) = 3, \\ \cdots & \cdots \\ g_{2,\left(\frac{G}{L}\right)} & i \bmod \left(\frac{G}{L}\right) = 0. \end{cases} \tag{3}$$

Encryption function:

$$\begin{aligned}
s_i &= Enc\left(g_{1,i}, g_{2,i}, j_{hpd1,i}, j_{hpd2,i}, \mathrm{offset}_i\right)\\
&= \frac{j_{hpd2,i} + offset_i}{\left(g_{2,i} - g_{1,i}\right) offset_i} + \frac{j_{hpd1,i} + \mathrm{offset}_i}{\left(g_{1,i} - g_{2,i}\right)\mathrm{offset}_i}\\
&\cdot \left\| \left(-\left(\frac{j_{hpd2,i} + offset_i}{\left(g_{2,i} - g_{1,i}\right) offset_i} \right) g_{1,i} + \frac{j_{hpd1,i} + \mathrm{offset}_i}{\left(g_{1,i} - g_{2,i}\right)\mathrm{offset}_i} g_{2,i} \right) \right\| \mathrm{offset}_i\\
&= A_i \| B_i \| \mathrm{offset}_i.
\end{aligned} \tag{4}$$

Making

$$\begin{aligned}
j_1 &= j\_hpd_{1,i},\\
j_2 &= j\_hpd_{2,i},\\
\mathrm{offset} &= \mathrm{offset}_i,
\end{aligned} \tag{5}$$

we get the expressions of A and B:

$$\begin{aligned}
A &= \frac{\Delta j}{\Delta g}\\
&= \frac{j_1 - j_2}{g_1 - g_2}\\
&= \frac{(j_1 - j_2)\mathrm{offset}}{(g_1 - g_2)\mathrm{offset}}\\
&= \frac{j_1 \mathrm{offset}}{(g_1 - g_2)\mathrm{offset}} + \frac{j_2 \mathrm{offset}}{(g_2 - g_1)\mathrm{offset}}\\
&= \mathrm{offset}\left[\frac{j_1}{(g_1 - g_2)\mathrm{offset}} + \frac{j_2}{(g_2 - g_1)\mathrm{offset}}\right]\\
&= \mathrm{offset}\left[\frac{j_1 + \mathrm{offset}}{(g_1 - g_2)\mathrm{offset}} + \frac{j_2 + \mathrm{offset}}{(g_2 - g_1)\mathrm{offset}}\right]\\
&= \frac{j_1 + \mathrm{offset}}{(g_1 - g_2)\mathrm{offset}} + \frac{j_2 + \mathrm{offset}}{(g_2 - g_1)\mathrm{offset}},\\
B &= j_1 - A g_1\\
&= j_2 - A g_2\\
&= j_1 - g_1 \mathrm{offset}\left[\frac{j_1 + \mathrm{offset}}{(g_1 - g_2)\mathrm{offset}} + \frac{j_2 + \mathrm{offset}}{(g_2 - g_1)\mathrm{offset}}\right]\\
&= j_2 - g_2 \mathrm{offset}\left[\frac{j_1 + \mathrm{offset}}{(g_1 - g_2)\mathrm{offset}} + \frac{j_2 + offset}{(g_2 - g_1)\mathrm{offset}}\right].
\end{aligned} \tag{6}$$

The ciphertext group s_i is connected according to the ECB mode, and the ciphertext s can be obtained:

$$s = s_1 s_2 \ldots s_i. \tag{7}$$

Abstract the encryption process as a function:

$$s = Enc\left(g_1, g_2, j\_hpd_1, j\_hpd_2, \mathrm{offset}\right) = A \| B \| \mathrm{offset}. \tag{8}$$

Decryption function:

$$\begin{aligned}
j_{0,i} &= \mathrm{Dec}\left(g_i, s_i\right)\\
&= \mathrm{Dec}\left(g_i, A_i \| B_i \| \mathrm{offset}\right)\\
&= \left(A_i g_i + B_i\right) - \mathrm{offset}.
\end{aligned} \tag{9}$$

We define

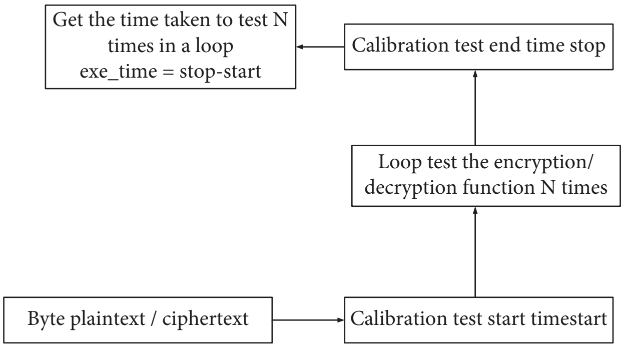

Get the time taken to test N times in a loop exe_time = stop-start
Calibration test end time stop
Loop test the encryption/ decryption function N times
Byte plaintext / ciphertext
Calibration test start timestart

FIGURE 8: Speed testing process of Bicycle algorithm.

$$\begin{aligned} j_0' &= j_0 \\ &= \mathrm{Deck}(g, s) \\ &= \mathrm{Deck}(g, A\|B\|\mathrm{offset}). \end{aligned} \tag{10}$$

We verify

$$\text{boolean} \quad \text{if Succ} = \left(j_0\_h = j_0'\_h?\text{true: false}\right). \tag{11}$$

The speed test process of Bicycle algorithm is shown in Figure 8.

The time taken for the 16 bit bicycle algorithm to execute 100 times is shown in Figure 9.

From Figure 9, it can be shown that the average time taken to encrypt 100 times by the 16 bit bicycle algorithm is 2.472 s, and the decryption time is 0.058 s.

Figure 10 shows the time it takes for the 32 bit bicycle algorithm to execute 100 times.

From Figure 10, it is clear that the 32 bit bicycle algorithm takes an average time of 2.188 s to encrypt 100 times and 0.073 s to decrypt. 16 bit encryption is slower than 32 bit encryption and faster decryption.

When the number of nodes in the domain is 6, the comparison of error correction rate is shown in Table 1.

Table 1 shows that when the number of nodes in the domain is 6, as the failure probability of the node increases, the threshold in the domain changes continuously. The comparison of the error correction rate between different threshold networks and the comparison with the error correction rate of the parallel structure is obtained. It can be seen from the comparison that as the threshold increases, the error correction capability of the network is getting lower and lower.

The delays of different thresholds under the layered structure are shown in Figure 11(a). The time delay comparison between the hierarchical structure and the parallel structure is shown in Figure 11(b).

Figure 11(a) shows the comparison of network delays under different thresholds. It can be seen in Figure 11(a) that as the probability of a node increases, as the threshold increases, the network delay is continuously reduced. This is because the larger the threshold value, the greater the possibility of selecting the best path for transmission, and the shorter the detection time of the node, the smaller the waiting time delay. Therefore, as shown in Figure 11, as the threshold value increases, the transmission delay changes gradually, and the larger the threshold value, the smaller the delay. In Figure 11(b), when we select the threshold as (3, 6), the comparison of the two structures shows that the delay of the layered structure is significantly greater than that of the parallel structure.

Table 2 shows the comparison of the transmission rate between the planar structure and the layered structure.

Table 3 shows the time delay under the data packet change under the fixed hierarchical structure threshold.

Figure 12 shows the time delay under the data packet change under the fixed hierarchical structure threshold.

In Figures 12(a) and 12(b), when the thresholds are (2, 6) (3, 6), respectively, as the probability of node failure increases and the data packet changes, the network delay changes. It can be seen from Figure 12 that, with the increase of data packets, the delay of the network gradually becomes larger.

5. Discussion

The security of wireless sensor network is mainly reflected in its secure communication protocol. Based on the research of wireless sensor network structure model, flat routing protocol and layered routing protocol, a domain-based secure communication protocol is proposed. The article mainly explains the proposed communication protocol, analyzes the performance of the network, and explains the initialization of the network. Then, it explains in detail how the nodes of the network communicate and how the nodes are routed. Finally, it analyzes the performance of the established network model and summarizes the advantages of the network model designed in this article compared with the traditional network model.

The data symmetric encryption method based on double plaintext proposed in this paper, on the one hand, uses double keys to return different information without using

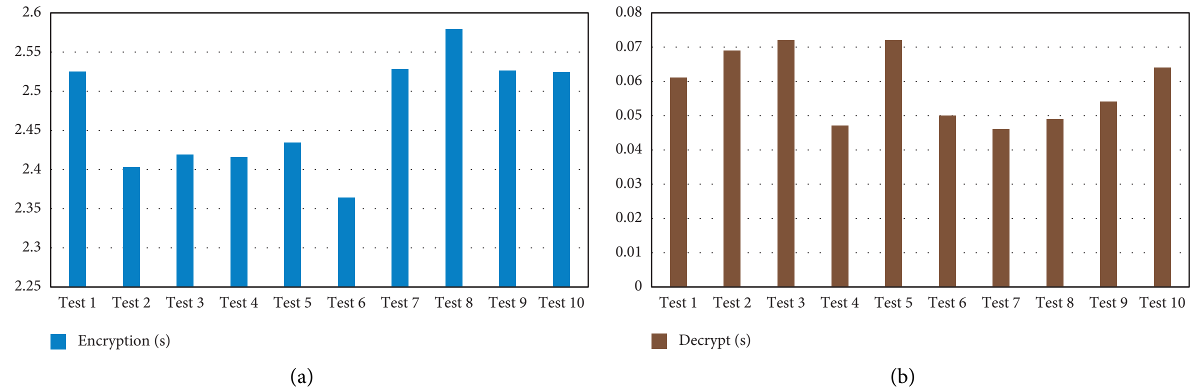


Figure 9: Time taken to execute the 16 bit bicycle algorithm 100 times.

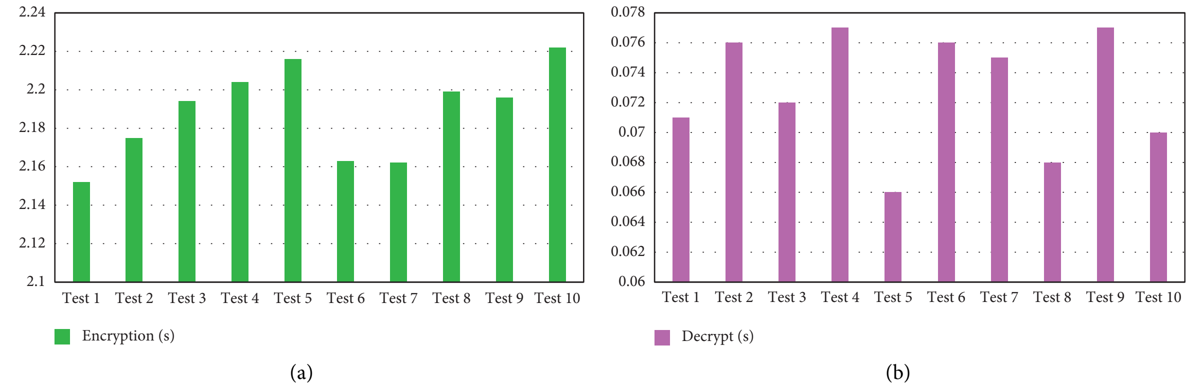
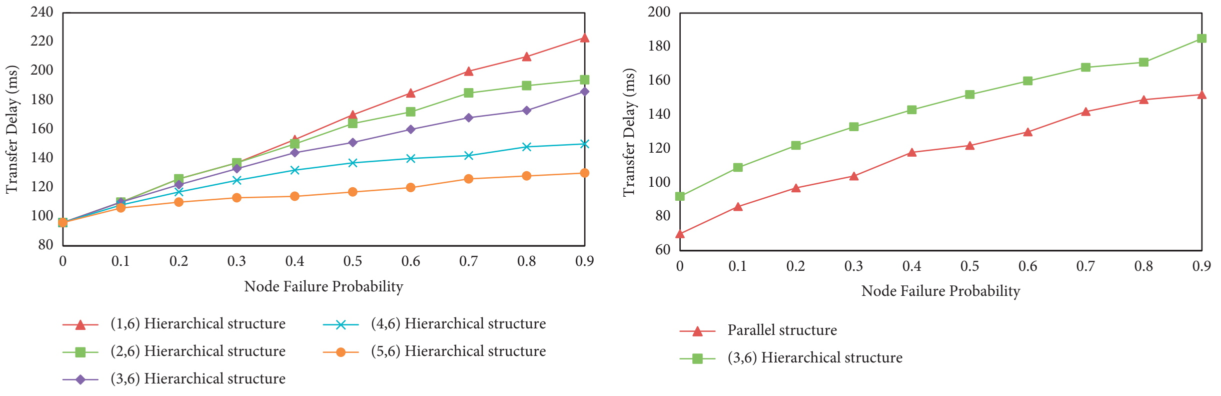


Figure 10: Time taken to execute the 32 bit bicycle algorithm 100 times.

Table 1: Comparison of error correction rate.

	(2, 6) hierarchical structure	(3, 6) hierarchical structure	(4, 6) hierarchical structure	(5, 6) hierarchical structure	Parallel structure
0	1	1	1	1	1
0.1	0.99	0.97	0.92	0.54	0.52
0.2	0.98	0.95	0.72	0.25	0.38
0.3	0.96	0.84	0.48	0.1	0.25
0.4	0.92	0.65	0.25	0.03	0.14
0.5	0.82	0.43	0.1	0.02	0.07
0.6	0.65	0.21	0.04	0.01	0.02
0.7	0.41	0.07	0.03	0.01	0.01
0.8	0.18	0.02	0.01	0	0
0.9	0.04	0.01	0	0	0
1	0	0	0	0	0

judgment sentences, on the other hand, it increases the difficulty of brute force exhaustion. At the same time, the introduction of a hash function supplements the lack of integrity in traditional symmetric cryptographic algorithms, and increases the amount of information contained in the plaintext of the same bit of ciphertext.



(a)

(b)

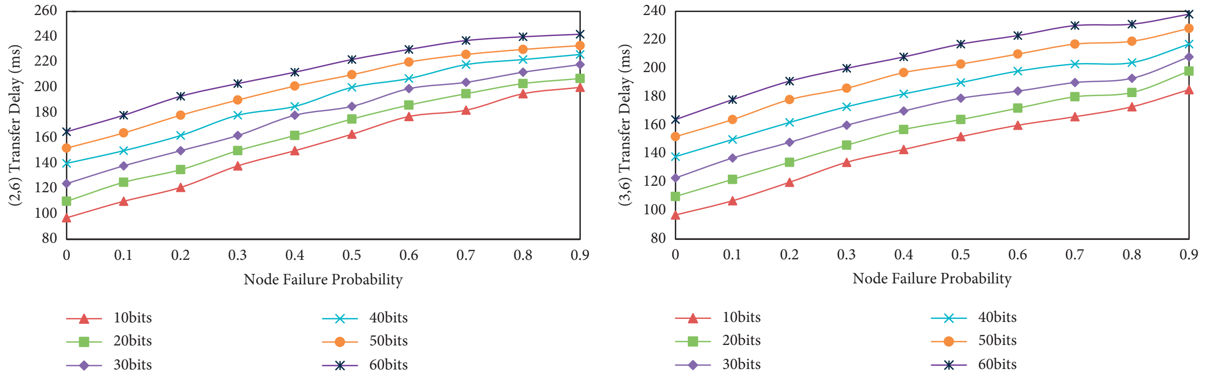
Figure 11: Delay of different thresholds under hierarchical structure and comparison of delay of hierarchical structure and parallel structure.

Table 2: Comparison of transmission rates of flat and hierarchical structures.

	(2, 6) hierarchical structure	(3, 6) hierarchical structure	(4, 6) hierarchical structure	(5, 6) hierarchical structure	Parallel structure
0	1	1	1	1	1
0.1	0.99	0.97	0.95	0.86	0.72
0.2	0.97	0.95	0.78	0.67	0.36
0.3	0.95	0.86	0.52	0.48	0.13
0.4	0.92	0.68	0.28	0.3	0.04
0.5	0.83	0.45	0.1	0.15	0.03
0.6	0.65	0.22	0.04	0.07	0.02
0.7	0.4	0.08	0.02	0.03	0.01
0.8	0.17	0.03	0.02	0.02	0
0.9	0.03	0.01	0	0.01	0
1	0	0	0	0	0

Table 3: Delay under packet variation with fixed threshold of hierarchical structure.

	10 bits	20 bits	30 bits
Transfer Delay (ms)	96.23	110.25	122.35
	40 bits	50 bits	60 bits
Transfer Delay (ms)	137.89	151.36	164.28



(a)

(b)

Figure 12: Delay under packet variation with fixed threshold of hierarchical structure.

6. Conclusion

In order to solve the problem of wireless sensor network protecting the master key and realizing secure communication. This paper is studying the structure of wireless sensor network, and using the secret sharing mechanism to propose a domain-based wireless sensor secure communication network model. In this model, the node key in the domain is managed by the council node, and the interdomain communication is realized by a dynamic gateway. It can better protect the master key in the domain and the structure of the network, and better solve the problem of the loss of the master key and the failure of key nodes, making the network data transmission more secure and reliable. At the same time, this article also proposes a secure communication protocol. From the results, we can conclude that due to the introduction of the secret sharing mechanism, the delay of the model network is obviously inferior to that of the flat network structure, but the fault tolerance is better than the latter, which can better realize network communication. In network transmission, plaintext appears more frequently at key nodes, which will reduce the security of network communication. Whether to negotiate a key between two communicating nodes first, and then further communicate. How to use the council node for key negotiation and whether the network performance is better than the original one still needs further research and improvement.

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 no conflicts of interest.

References

[1] T. Wang, C. Ma, and Q. Sun, "The interaction between security lending market and security trading market," *Pacific-Basin Finance Journal*, vol. 46, pp. 309–322, 2017.

[2] M. Fagan and M. M. H. Khan, "To follow or not to follow: a study of user motivations around cybersecurity advice," *IEEE Internet Computing*, vol. 22, no. 5, pp. 25–34, 2018.

[3] J. Chen and Q. Zhu, "Interdependent strategic security risk management with bounded rationality in the Internet of things," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 11, pp. 2958–2971, 2019.

[4] M. Tauhid Ur Rahman, M. Rasheduzzaman, M. A. Habib, A. Ahmed, S. M. Tareq, and S. M. Muniruzzaman, "Assessment of fresh water security in coastal Bangladesh: an insight from salinity, community perception and adaptation," *Ocean & Coastal Management*, vol. 137, pp. 68–81, 2017.

[5] C. Huang and C. Wang, "Network security situation awareness based on the optimized dynamic wavelet neural network," *International Journal on Network Security*, vol. 20, no. 3, pp. 593–600, 2018.

[6] P. Susheelkumar Sreedharan and D. Jageshwar Pete, "Spatial correlation based clustering with node energy based multi-hop routing scheme for wireless sensor networks," *Tehnički Glasnik*, vol. 15, no. 1, pp. 25–36, 2021.

[7] K. Alic, M. Mohorcic, and A. Svigelj, "Network and traffic design aspects in network-coding-enabled wireless networks," *International Journal of Computers, Communications & Control*, vol. 14, no. 3, pp. 293–310, 2019.

[8] S. V. Bharathi, "Forewarned is forearmed Assessment of IoT information security risks using analytic hierarchy process," *Benchmarking: An International Journal*, vol. 26, no. 8, pp. 2443–2467, 2019.

[9] A. Alexandrou and L.-C. Chen, "Correction to: a security risk perception model for the adoption of mobile devices in the healthcare industry," *Security Journal*, vol. 34, no. 2, p. 261, 2021.

[10] T. Nordfjærn and T. Rundmo, "Transport risk evaluations associated with past exposure to adverse security events in public transport," *Transportation Research Part F: Traffic Psychology and Behaviour*, vol. 53, pp. 14–23, 2018.

[11] S. Lumba, D. Holbrook-Smith, and P. Mccourt, "The perception of strigolactones in vascular plants," *Nature Chemical Biology*, vol. 13, no. 6, pp. 599–606, 2017.

[12] B. L. Eun, J. S. Lee, C. S. Yun, and C. Yeol, "Analyzing community CPTED perception of local residents in the school areas," *Journal of The Korean Society of Civil Engineers*, vol. 37, no. 5, pp. 891–903, 2017.

[13] A. I. Badiora, C. A. Wojuade, and A. S. Adeyemi, "Personal safety and improvements concerns in public places: an exploration of rail transport users' perception," *Journal of Place Management and Development*, vol. 13, no. 3, pp. 319–346, 2020.

[14] D. J. Parada, A. Flórez, and U. E. Gómez, "Análisis de los Componentes de la Seguridad desde una Perspectiva Sistémica de la Dinámica de Sistemas," *Informacion Tecnologica*, vol. 29, no. 1, pp. 27–38, 2018.

[15] T. Holt, M. S. Helland, K. Gustavson, E. M. Cummings, A. Ha, and E. Røysamb, "Assessing children's responses to interparental conflict: validation and short scale development of SIS and CPIC-properties scales," *Journal of Abnormal Child Psychology*, vol. 48, no. 2, pp. 177–196, 2020.

[16] L. L. Tang, Y. W. Chan, and G. L. Shen, "Investigating radio-frequency identification usage behaviours and organisational performance according to factors of user perception," *International Journal of Services Technology and Management*, vol. 25, no. 3/4, pp. 199–214, 2019.

[17] P. Jung-Hong, "Impact of personal health information security awareness on convenience," *Journal of the Korea Contents Association*, vol. 17, no. 6, pp. 600–612, 2017.

[18] A. Abenavoli, S. Pisa, and A. Maggiani, "A pilot study of jugular compression (queckenstedt maneuver) for cranial movement perception," *Journal of Osteopathic Medicine*, vol. 120, no. 10, pp. 647–654, 2020.

[19] A. K. Tripathi, K. Sharma, and M. Bala, "Parallel hybrid BBO search method for twitter sentiment analysis of large scale datasets using MapReduce," *International Journal of Information Security and Privacy*, vol. 13, no. 3, pp. 106–122, 2019.

[20] J. Dentler, S. Kannan, S. Bezzaoucha, M. A. Olivares-Mendez, and H. Voos, "Model predictive cooperative localization control of multiple UAVs using potential function sensor constraints," *Autonomous Robots*, vol. 43, no. 1, pp. 153–178, 2019.

[21] S. Saha, "Enhancing point symmetry-based distance for data clustering," *Soft Computing*, vol. 22, no. 3, pp. 1–28, 2017.

[22] H. Bayar, U. K. Terzi, and O. Ozgonenel, "PCA-ANN based algorithm for the determination of asymmetrical network failures of network-connected induction generators," *Tehnicki Vjesnik-Technical Gazette*, vol. 26, no. 4, pp. 953–959, 2019.