Wireless Sensor Networks Security Enhancement Approach Based on Single Path Secure Routing Algorithm

Xiaoyan Luo

Academic Affairs Office, Hunan University of Arts and Science, Changde, 415000, China
E-mail: xiaoXyanYluoL@outlook.com

Received 20 December 2023; Accepted 07 June 2024

Abstract

To improve the security of wireless sensor networks, the experiment proposes a network security improvement method based on multi-objective ant colony optimization and single-path secure routing protocol. First, LEAP is used to improve the single-path secure routing algorithm to enhance the security of data during transmission; then, a multi-objective ant colony optimization algorithm is introduced to find the optimal network parameter path. The detection accuracy shows that when the time reaches 62.23 ms, the method proposed in the study has a maximum detection accuracy of 99.89%; at this time, the detection accuracy of the other three schemes is significantly less than 95.00%. When the system running time is 57.41 ms, the detection accuracy of wormhole attacks by this method begins to reach a stable state, and the detection accuracy has been infinitely close to 100% in the future. This method is applied to the Internet of Vehicles and the Enterprise Office Network respectively. When the number of intrusion nodes is 1,780 and 2,000

Journal of Cyber Security and Mobility, Vol. 13_5, 1085–1104.
doi: 10.13052/jcsm2245-1439.13512

respectively, external intrusion can damage the key space and steal secrets. The above results show that the proposed method can not only improve network security and ensure energy efficiency, but also optimize network performance.

Keywords: Wireless sensors, network security, single path secure routing, key pre-distribution.

1 Introduction

Wireless Sensor Networks (WSN) are composed of numerous sensor nodes that can sense the environment, process data and transmit wirelessly, ultimately forming a self-organized multi-hop network [1]. In WSN, routing technology plays a crucial role, which ensures that data transmission from source to destination can follow established protocols and paths. However, since the transmission of the network relies heavily on the transmission of wireless signals and lacks physical protection measures, the WSN network is very vulnerable to attacks [2]. During the attack, the attacker may destroy the routing process, cause network failures, or even issue false instructions, posing a serious threat to network security. In practical applications, the security of critical infrastructure such as chemical facilities and power systems is frequently compromised by malicious incidents, which not only poses a threat to public safety, but also poses a challenge to the security of national assets. At the same time, WSN plays an important role in many fields such as military, environmental monitoring, and health monitoring. With the development of technology, WSN has become more and more widely used. However, network security issues have also increased. Especially during the data transmission process, the effectiveness of the secure routing algorithm is directly related to the security of the entire network. and stability [3]. At the same time, due to limited energy supply, computing power and storage resources, as well as an open communication environment, WSN faces serious security threats. Traditional secure routing algorithms often face problems such as high computational complexity, poor adaptability, and vulnerability to attacks, which limits the application of WSN in some key areas. Some scholars believe that Ant Colony Optimization (ACO) is a path selection mechanism that can effectively solve complex optimization problems [4]. In WSN, this algorithm is often used to find the optimal data transmission path, thereby improving the security and efficiency of the network. At the same time, by combining the single-path secure routing algorithm, the security and reliability during data

transmission are further ensured [5]. In view of this, the experiment proposes a new WSN network security improvement technology that integrates an improved multi-ant colony target optimization algorithm and a single-path secure routing algorithm. It is expected that through intelligent path selection and optimization algorithms, WSN can improve its performance in the face of different security threats. robustness and adaptive capabilities.

The study includes four parts. The first part summarizes the current research status of wireless sensors both domestically and internationally. The second part is the combination and design of single path secure routing and multi-objective ant colony optimization algorithm. The third part is an actual performance analysis of the design scheme. The fourth part is a results summary and specific future prospects.

The innovation of the article can be divided into two points. First, starting from the aspects of WSN network security and energy efficiency, we focused on the routing protocol issues. The comprehensive trust value is calculated and used as the heuristic factor of the ant colony algorithm. Various factors and energy are added to the pheromone update to obtain an energy-saving and efficient secure routing algorithm. Second, an ant colony secure routing algorithm is constructed based on the node trusted secure routing protocol and combined with multi-objective optimization. Utilize the concept of multi-target to achieve multi-target ant colony secure routing to reduce energy consumption.

2 Related Works

Scholars have conducted extensive research on exploring the security enhancement of WSN. These studies mainly focus on developing efficient and reliable routing algorithms to ensure secure transmission of data in insecure environments. Raja Basha proposed a feasible security aware routing scheme to cope with external attacks on the network during WSN operation. This scheme introduced the optimal trust inference model of conditional tug of war optimization algorithm to calculate numerical values. The results showed that the trust factor introduced in this scheme helped the system identify network attacks and block foreign intrusions [6]. Yuan E and Wang L, two scholars, proposed a digital signature technology based on identity encryption and elliptic curve cryptography to improve the security performance of WSN. During the process, a dual encryption method was used to protect the privacy of network locations. The results showed that the constructed scheme occupied less key storage space and consumed less energy to protect the

specific location information of nodes [7]. Kumar CP and Selvakumar R, two scholars, constructed a decentralized erasure code from the optimal code and introduced a key pre-distribution protocol to reduce the number of nodes required for reconstructing data from internal faulty nodes in WSN. The results showed that the scheme ensured efficient communication capabilities between nodes in the network during operation [8]. Prakash G and other researchers proposed an energy source based resource key distribution algorithm to improve communication services between vehicular organizational networks. This protocol generated a throughput of up to 86% and significantly reduced the probability of routing delay by 13%, ultimately enhancing the lifespan of WSN [9]. Ramesh S and Yaashuwanth C, two scholars, proposed a secure routing framework based on improved lightweight trust decision-making to improve the resolution and security of image sensors during transmission. This protocol was widely used in forming groups, exchanging trust values between master nodes, member nodes, and base stations. Compared to traditional network security models, this model had higher reliability and occupies less memory [10].

On the other hand, scholars also conducted extensive research on WSN's application. Ahlawat P and Dave M, two scholars, proposed a WSN design method based on secure mixed key pre-distribution to effectively address the problem of network node capture attacks. This method combined the robustness and threshold resistance polynomial schemes of multiple different methods to address network vulnerabilities with fewer nodes. It was found that the constructed method effectively defended against attacks on network nodes. Compared to other schemes, the scheme constructed by the research institute reduced the probability of key leakage, and had lower communication and storage costs [11]. Xiong P and Su Q, two scholars, proposed a random key pre-distribution scheme with an improved hash chain to improve the connection and survival capabilities of network security. The results showed that the constructed scheme was highly effective and had a certain degree of scalability [12]. Mitchell CJ proposed a polynomial based group key pre-distribution scheme to address node computation in WSN and improve sensor storage capacity. The proposed scheme enabled WSN to construct shared keys between networks without any communication overhead. It was found that the security proof of the constructed scheme was not very strict, but it was able to correctly analyze the issues involved in the pre-distribution scheme [13]. To effectively reduce the probability of security vulnerabilities in WSN and improve the security of data transmission, researchers such as Rajasoundaran S proposed a watchdog network product.

The superiority of the proposed technology was verified through performance testing and application effects [14]. Krishnapriya M's team proposed a rank-based energy-saving key management protocol to limit energy utilization. This protocol can quickly transmit sensor data to the base station to achieve effective control of the base station. The results showed that this scheme effectively reduced the probability of nodes being attacked and successfully intercepted foreign intrusions with minimal power consumption, throughput, and packet loss rate [15].

Overall, a large number of scholars have conducted extensive research on WSN related routing protocols and achieved good results. However, there is still relatively little research on combining multi-objective ant colonies with single path secure routing protocols to enhance WSN security. To address this issue, this study will integrate the two to control network security, exploring how to further optimize the energy efficiency and data processing capabilities of the network while ensuring security. This will open up new avenues for the development and application of WSN, especially in critical application areas that require high security and reliability.

3 Improved WSN Network Security Enhancement Technology

This part mainly adopts an improved single path secure routing protocol, which aims to enhance the robustness and adaptability of WSN in the face of different security threats through intelligent path selection and optimization algorithms. Then, an improved multi-ant colony algorithm is introduced for path selection process optimization, thereby improving the efficiency and security of routing. Through this research, it is expected to provide more reliable and effective technical solutions for the security and stable operation of WSN.

3.1 WSN Security Technology Based on Single Path Secure Routing Protocol

The nodes of WSN have the characteristics of high capacity, wide distribution, and strong deployment ability, thus showing great research potential in various application scenarios such as smart city construction, battlefield environment monitoring, and object detection. However, due to the fact that WSN is often deployed in harsh and complex environments, developing routing algorithms suitable for these special scenarios has become the

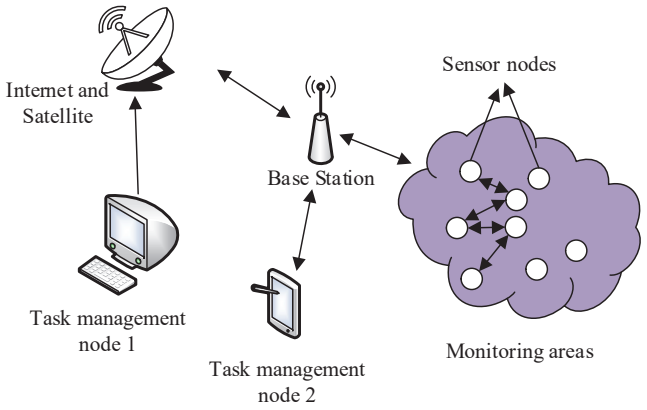

Figure 1 Specific structural model of WSN.

key to improving the transmission efficiency of WSN. In WSN, all nodes communicate and interact through a multi hop, self-organizing distributed mode [16]. These systems include low-cost sensor nodes, base stations, and task management nodes distributed in monitoring areas, equipped with wireless communication and sensing functions, as well as information processing capabilities. The detailed structural model of WSN can refer to Figure 1.

Compared with traditional networks, WSN is more susceptible to attacks from intruders due to its completely open wireless communication channel and typically operating in harsh environments, making it a challenge to establish a secure routing mechanism for WSN. In view of this, an improved secure routing protocol for single path WSN is proposed in the experiment, which is based on the key management mechanism in the Localized Encryption and Authentication Protocol (LEAP) [17]. LEAP creates 5 different types of keys for each different node in WSN, including initial keys, individual node keys, paired keys, cluster keys, and group keys. Figure 2 shows the steps required to add a new node to WSN in LEAP.

In Figure 2, it can be observed that adding a new node to the WSN requires a total of 4 steps. After this process, the node will establish paired shared keys with adjacent neighbors. After the initial key is eliminated, the node will not be able to establish paired keys with any nodes between the already eliminated initial keys. Meanwhile, due to the time required for attackers to invade nodes, all nodes can ensure the elimination of the initial key between intrusions. Without knowing the initial key, attackers are also unable to establish paired keys with any node other than the neighbors of the compromised node. Through this process, routing protocols can effectively

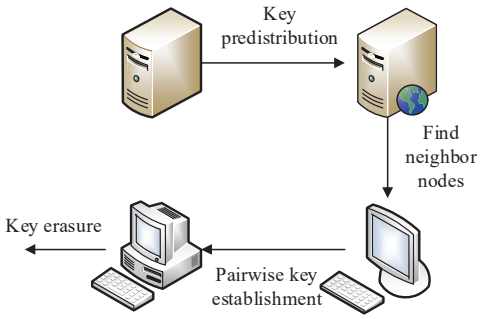

Figure 2 The specific process of adding new nodes to WSN.

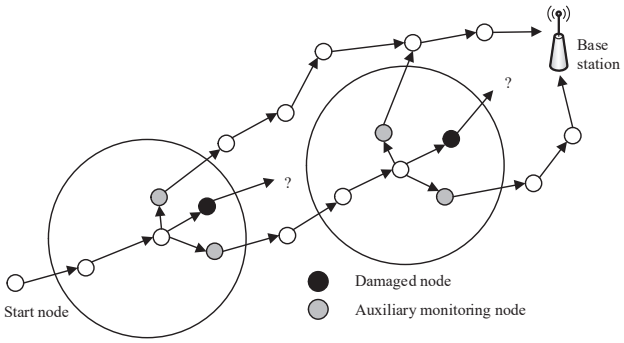

Figure 3 The data packet bypasses the damaged node and continues to be forwarded along a single path.

evade attacks within a certain range. The LEAP protocol can ensure that WSN is not attacked by replay routing information and selectively forwards attacks, with good security. In WSN, nodes can listen to the communication of neighboring nodes through wireless channels, but they cannot effectively monitor all malicious node attacks in the network. To address this issue, a secure single path routing protocol based on Neighbor Watch System (NWS) has been proposed. In this protocol, system packets will bypass damaged nodes and start forwarding nodes along a single path secure route. The specific process is shown in Figure 3.

3.2 Design of WSN Secure Routing Scheme Using Multi-objective Ant Colony Optimization Algorithm

Due to WSN being often deployed in unattended areas, sensor nodes are vulnerable to attacks. Additionally, using a single path secure routing protocol

can only improve network security to a certain extent, but it inevitably leads to a decrease in other metrics. Therefore, while strengthening network security, it is also necessary to consider the energy consumption of sensors. However, the objective optimization method cannot fully meet these requirements. Therefore, a multi-objective ant colony optimization secure routing protocol using single path secure routing protocol is proposed [18]. This protocol adopts an improved D-S theory to evaluate node trust, and optimizes the objective functions of path average energy and trust value. At the same time, network constraints and node behavior are used as constraints, and these two optimization objectives are integrated into the ant colony routing algorithm to effectively avoid malicious nodes and improve network security.

Multi-objective optimization is about finding a set of non-inferior solutions that can comprehensively consider all objectives. The specific model of this type of multi-objective combination is shown in Equation (1).

$$\begin{cases} \min y = f(x) = (f_1(x), f_2(x), \ldots, f_n(x)) & (n = 1, 2, \ldots, N) \\ s.t.\ (x) \leq 0 & (i = 1, 2, \ldots, p) \\ \quad h_j(x) = 0 & (j = 1, 2, \ldots, q) \end{cases} \tag{1}$$

In Equation (1), $x = (x_1, x_2, \ldots, x_m)$ represents the decision variables on the m dimension. $y = (y_1, y_2, \ldots, y_m)$ represents the objective vector on the n dimension. $g_i(x)$ and $h_j(x)$ represent the constraints of the i-th and j-th inequalities, respectively. $f(x)$ represents the objective function. $f_n(x)$ represents the n-th objective function.

In the routing problem of WSN, improving network security usually means higher energy consumption. To solve this problem, a multi-objective optimization strategy is introduced on the basis of existing single objective ant colony optimization algorithms, and node residual energy and trust value are designed to determine the optimal routing path. A Security routing protocol using objective ant colony optimization (SRMOACO) is obtained, the corresponding mathematical model is shown in Equation (2).

$$\begin{cases} Max\ f(t) = (f_1(t), f_2(t)) \\ s.t. \begin{cases} E_i(t) \geq 0 \\ RP_{i,j}(t),\ TP_{i,j}(t) > 0 \\ 0 \leq t \leq t_{\max} \end{cases} \end{cases} \tag{2}$$

In Equation (2), $RP_{i,j}(t)$ and $TP_{i,j}(t)$ respectively represent the total energy of data packets received and forwarded by the node i. $E_i(t)$ represents

the remaining energy of a node i over time t. N represents the number of path nodes. $t_{\max}$ represents the maximum simulation time. $f_1(t)$ and $f_2(t)$ represent the average remaining energy and trust value, respectively. The first objective function f_1 is set based on the node energy value. Equation (3) shows an energy model that takes into account the sending and receiving states of data packets.

$$E_j(t) = E_j(t-1) - RP_{i,j}(t) * E_R - TP_{i,j}(t) * E_T - E_e(t) \tag{3}$$

In Equation (3), E_R and E_T respectively represent the energy consumed by receiving and forwarding a data packet. $E_e(t)$ represents the other energy consumption.

When the routing path length is N, the expression of f_1 of the node is shown in Equation (4).

$$f_1(t) = \sum_{j=1}^{N} E_j(t)/N \tag{4}$$

Then the second f_2 is set with the trust value of network nodes. The trust value $T_j(t)$ is obtained using D-S theory, and the calculation of f_2 is shown in Equation (5).

$$f_2(t) = \sum_{j=1}^{N} T_j(t)/N \tag{5}$$

In Equation (5), $T_j(t)$ represents the value $F_j(t)$ of the node trust evaluation function obtained through the D-S evidence theory comprehensive trust model. The D-S evidence theory comprehensive trust evaluation model is shown in Figure 4.

In order to highlight each objective, the experimental result f_1 will take into account the remaining energy, and the corresponding calculation of heuristic information $\eta_{i,j}(t)$ is shown in Equation (6).

$$\eta_{i,j}(t) = E_j(t)/C \tag{6}$$

Similarly, the calculation of heuristic information $\eta_{i,j}(t)$ corresponding to the objective function f_2 taking into account node trust values is shown in Equation (7).

$$\eta'_{i,j}(t) = T_j(t) \tag{7}$$

Combining Equations (6) and (7), it can be seen that in the ant colony algorithm, when each ant constructs a feasible routing path, it will select

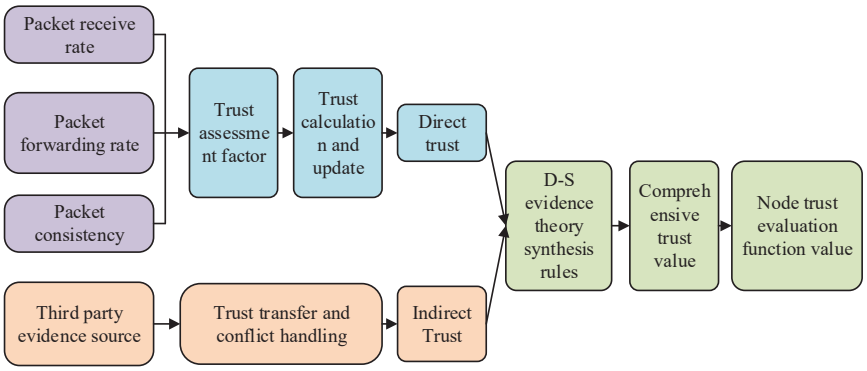

Figure 4 D-S evidence theory comprehensive trust evaluation model.

the next node based on the value of the heuristic function. In this way, the heuristic information provides a priority for each path that the ant may choose, so that the ant tends to choose those paths with higher heuristic values and starts to calculate local pheromones to improve the convergence speed of the algorithm. The calculation of pheromone updates is shown in Equation (8).

$$\Delta\tau_{i,j}^{n}(t+1) = (1-\rho)\tau_{i,j}^{n}(t) + \rho\Delta\tau_{i,j}^{n}(t),\ \forall(i,j) \in T, n = 1,2 \quad (8)$$

In Equation (8), ρ represents the volatility coefficient, with a value range of (0,1). T represents the feasible solution path for local pheromone updates. $\Delta\tau_{i,j}^{n}(t)$ represents the initial pheromone value of the n optimization objective ($n = 1,2$). In order to promote the updating of pheromones, different targets update different pheromone values, and the expression of local pheromone updates is shown in Equation (9).

$$\begin{cases} \Delta\tau_{i,j}^{1}(t) = \dfrac{1}{(f_1/C)} \\ \Delta\tau_{i,j}^{2}(t) = \dfrac{1}{(f_2)} \end{cases} \quad (9)$$

Then the global information degree is updated, and the update rules are shown in Equation (10).

$$\tau_{i,j}^{n}(t+1) = (1-\rho)\tau_{i,j}^{n}(t) + \rho\Delta\tau_{i,j}^{n}(t), \forall(i,j) \in T^{g} \quad (10)$$

In Equation (10), $\Delta\tau_{i,j}^{n}(t)$ represents the increment of global pheromones. T^{g} represents the non dominated solution path for global pheromone updates.

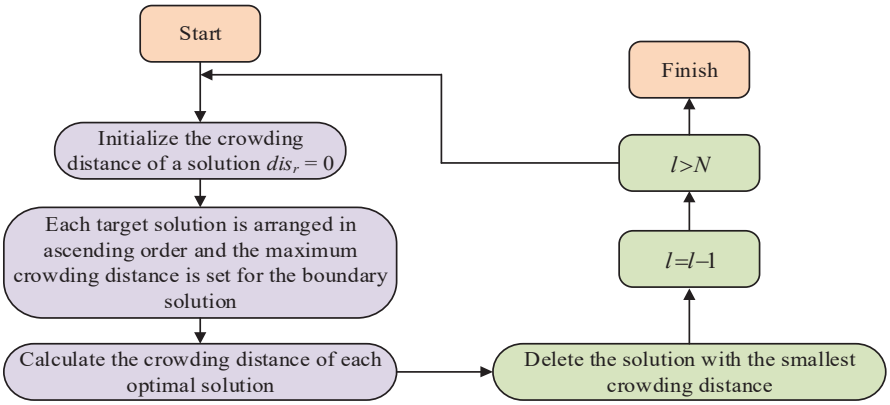

Figure 5 Process of improving crowding distance strategy.

The expression of the increment of global pheromones is shown in Equation (11).

$$\Delta\tau_{i,j}^{n}(t) = \frac{1}{Bd_k^n} \tag{11}$$

In Equation (11), Bd_k^n represents the number of node hops passed by the backward ant k. The Pareto optimal solution is usually composed of a set of solutions consisting of numerous non-inferior solutions. With the limited storage space of WSN nodes, the increase in external archives of non dominated solutions will affect the algorithm efficiency. Therefore, an improved crowding distance strategy is introduced in the experiment to preprocess the external solution set, ensuring that the non inferior solution set is as close and uniformly distributed as possible at the Pareto front [19]. The process of improving the congestion distance strategy is shown in Figure 5.

The crowding distance calculation for obtaining the optimal solution r through the crowding distance method is shown in Equation (12).

$$dis_r = \sum_{n=1}^{2}(f_n^{r+1}, f_n^{r-1})/(f_n^{\max} - f_n^{\min}), 1 < r < l \tag{12}$$

In Equation (12), l represents the number of solutions. f_n represent the goal. dis_r represents the optimal solution. f_n^r represents the value of r on the objective n. The specific process of obtaining an improved secure routing algorithm is shown in Figure 6.

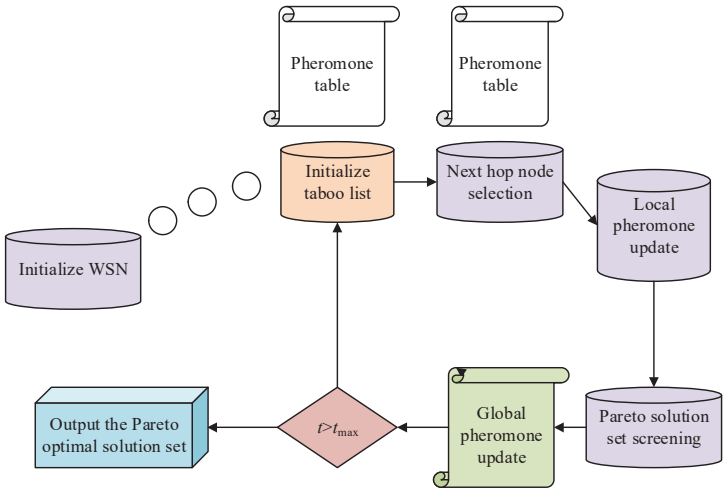

Figure 6 The specific process of improving the multi-target ant colony secure routing algorithm.

4 Performance Analysis of WSN Security Model

The reliability and effectiveness of the WSN security system (IMACO-SSP) constructed by the research institute were verified through experiments. Firstly, WSN based on lightweight key distribution scheme (IPK), WSN path selection and security system based on BAT and firefly algorithm (BAT-FA) were selected Comparison of performance testing between WSN spatial storage system based on Combined Design of Key Pre-distribution Scheme (CD-KPD) and IMACO-SSP scheme [20–22]. Before starting the experiment, the environment and parameters were first set for the simulation experiment, as shown below.

Table 1 Experimental parameters

Parameter Variables	Parameter Selection
Modeling Platform	SIMULINK
simulation software	Matlab
System PC side memory	36G
Data storage	Sheepdog
Simulation experimental environment	MRDS
Operating system	Microsoft Windows 10
CPU model	i7-9800X
Data regression analysis platform	SPSS, Excel

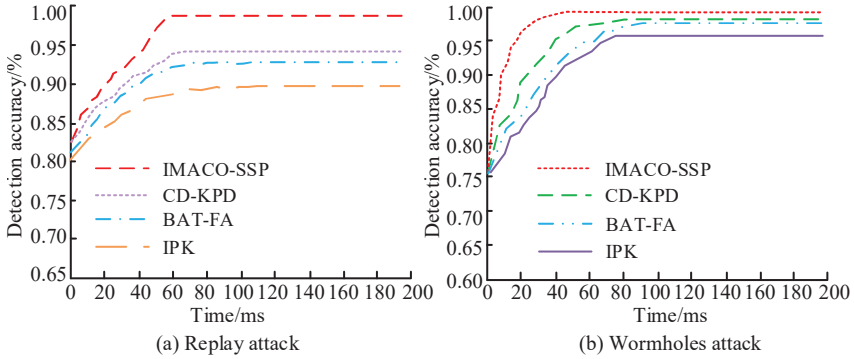

Figure 7 Comparison of detection accuracy of different schemes against node attacks.

In order to compare the accuracy of four methods for detecting different types of intrusion methods, the experiment first compared the detection accuracy of replay attack and Wormholes wormhole attack as the research object. The specific results are shown in Figure 7.

Figure 7 compares the detection accuracy of different schemes under different attacks. It can be observed that over time, the detection accuracy of different schemes for attacks showed a significant increase. Figure 7(a) compares the accuracy of replay attack detection among different schemes. When the time reached 62.23 ms, the IMACO-SSP scheme had a maximum detection accuracy of 99.89%. At this time, the detection accuracy of the other three schemes was significantly less than 95.00%. When the time reached 70.12 ms, the detection accuracy of the CD-KPD scheme began to reach its maximum, with a value of 94.79%. Figure 7(b) shows the accuracy comparison of different schemes for detecting wormhole attacks. When the running time of the system was 57.41 ms, the detection accuracy of the IMACO-SSP scheme for wormhole attacks began to reach a stable state, and the detection accuracy in the future reaches 99.99%, continuously approaching 100% infinitely. This indicates that under the IMACO-SSP scheme, the system accurately detected the source of the attack and reduced the risk of being attacked. This is mainly because the multi-objective ant colony algorithm in the IMACO-SSP solution can not only pay attention to the security of WSN routing, but also take into account the energy consumption efficiency of network transmission, reducing data loss and other problems caused by the wireless sensing process. false positives and false negatives, ultimately improving detection accuracy. Then, the experiment set up a damaged node with malicious packet loss in the set simulation environment, and operated

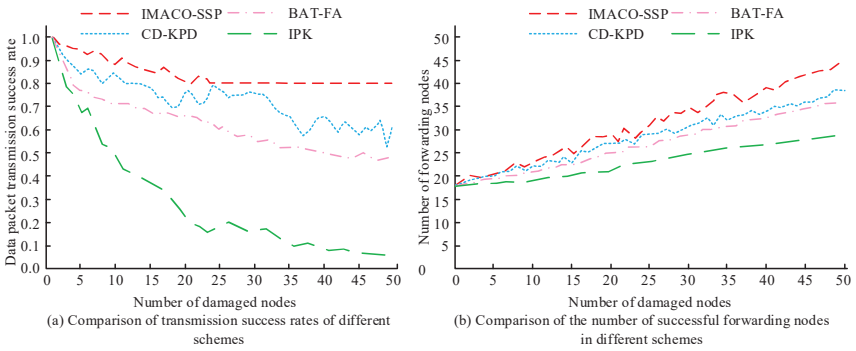

Figure 8 Comparison of transmission power and number of forwarding nodes.

within a 500 m × 500 m area, 300 sensor nodes were randomly and uniformly deployed, each with a constant transmission range of 30 m, corresponding to an average of 10 neighboring nodes. Additionally, the base station and source node were located at two opposite corners of the entire area, with the points located at (50, 50) and (450, 450). There were 18 jumps between two points. The damaged nodes were distributed inside the square area, with a distance of 150 m to 350 m from the side of the target area. During the entire simulation process, damaged nodes maliciously discarded data packets. The comparison of transmission power and number of forwarding nodes for different schemes is shown in Figure 8.

Figure 8(a) shows a comparison of transmission success rates for different schemes. It can be observed that when a damaged node maliciously discarded data packets, the transmission success rates of the four schemes were consistently decreasing. The transmission success rate of the IMACO-SSP scheme decreased slower than other schemes, and when the number of damaged nodes was 25, the transmission success rate remained stable at 80%. The transmission success rate of other schemes was constantly changing and not in a stable state. Figure 8(b) Comparison of successful forwarding node numbers for different schemes. As damaged nodes increased, forwarding nodes for all four schemes began to increase. However, forwarding nodes in the IMACO-SSP scheme were significantly more than other schemes. From this, the IMACO-SSP scheme performed better in terms of energy efficiency than other protocols. It had strong resistance ability and can maintain a high forwarding success rate. Next, the simulation time was set to 1000s (represented by the X-axis) and the energy consumption was compared under different schemes in Figure 9.

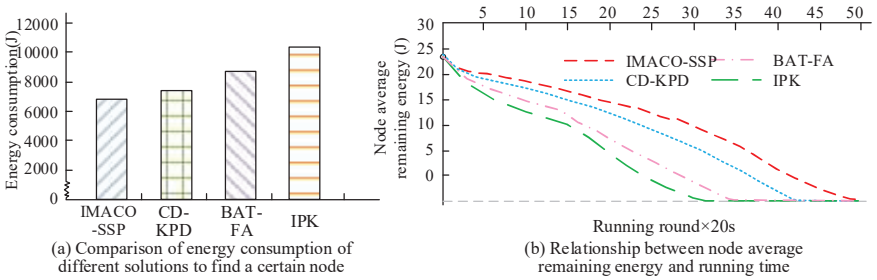

Figure 9 Comparison of energy consumption of different solutions.

Figure 9(a) shows the energy consumption comparison of a key node in the system for different schemes. It can be observed that the energy consumption of the IMACO-SSP scheme was significantly lower than that of the other three schemes. This is because the IMACO-SSP scheme had directionality in packet forwarding, and found the critical node with fewer hops compared to the other three schemes, thus consuming less energy. Figure 9(b) shows the relationship between the remaining energy of a key node and its operating time. Over time, the average node capacity of the IMACO-SSP scheme was consistently higher than the other three schemes. Compared with other models, in the process of constructing the best optimization path, the IMACO-SSP solution can select the optimal path for network transmission signals through the ACO algorithm and perform WSN dynamic energy consumption management to ensure data transmission security while maintaining At the same time, the overall energy consumption of the system is reduced and energy consumption is kept to a minimum. Finally, the four schemes were applied to the factory workshop networking and enterprise office networking systems of a listed company, and the security performance of the four schemes under attack was analyzed. The specific results are shown in Figure 10.

Figure 10(a) shows the security performance comparison of different schemes in workshop networking. As invaded nodes increased, the ability of different schemes to destroy keys also increased. Under the IMACO-SSP scheme, when there were more than 1780 invaded nodes, the intruder caused damage to the key space and steal the key. In addition, during the operation of the other three schemes, when the number of invaded nodes was less than 1500, foreign intrusions began to cause damage to the system key. Figure 10(b) shows the security performance comparison of different schemes in office networking. Under the IMACO-SSP scheme, foreign intrusion required at least 2000 network nodes to steal system secrets.

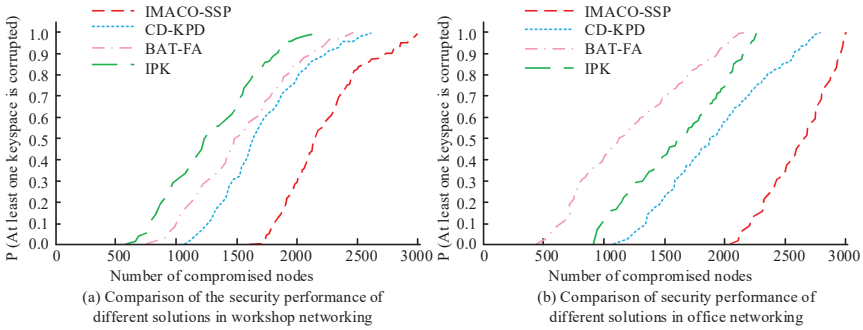

Figure 10 Comparison of security performance of different solutions.

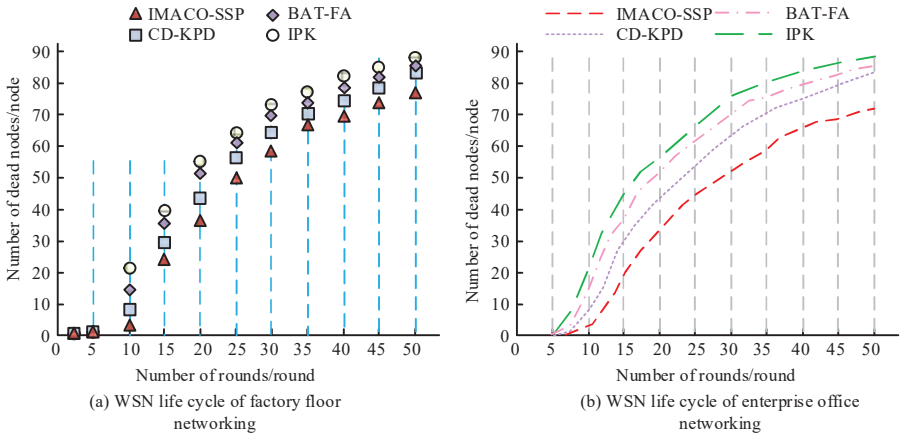

Figure 11 Life cycle of WSN under different solutions.

By comparison, it can be seen that compared to the other three schemes, the IMACO-SSP scheme had a more significant advantage in terms of security. Under the IMACO-SSP scheme, attackers needed to attack massive nodes to disrupt the key space. The IMACO-SSP solution reduces system energy consumption by reducing unnecessary data forwarding and optimizing communication between nodes. WSN systems are generally found in factory floor networking and enterprise office networking systems, and the IMACO-SSP solution is highly flexible and scalable and can be applied to a variety of different wireless sensor network scenarios to maximize energy efficiency. When four schemes were applied to two local area networks, the survival cycle of WSN was analyzed, and the specific results are shown in Figure 11.

Figure 11 reflects the specific situation of the number of node deaths in each round. It can be observed that when using the IMACO-SSP scheme, CD-KPD scheme, BAT-FA scheme, and IPK scheme, the number of WSN dead nodes gradually increased. At the beginning, the IMACO-SSP scheme had the same number of rounds as the other three schemes when the first node died. When the scheme reached 50 rounds, the number of dead nodes in the IMACO-SSP scheme, factory workshop networking, and enterprise office networking was 74 and 71, respectively. At this point, dead nodes in the other three schemes were significantly greater than 70. By comparison, the number of dead nodes in IMACO-SSP scheme was always the smallest, indicating that the IMACO-SSP scheme significantly improved the balance of network energy consumption and had a significant effect.

5 Conclusion

In order to improve the security of WSN, a single path secure routing protocol using multi-objective ant colony optimization algorithm is proposed in the experiment. During the process, the security of data transmission is further enhanced by implementing a single path secure routing protocol. A multi-objective ant colony optimization algorithm is introduced to adjust the algorithm parameters, so that the algorithm can simultaneously consider the energy efficiency and path safety. When the system was subjected to two types of attacks, replay attack and Wormholes wormhole attack, the detection accuracy of the IMACO-SSP scheme was 99.89% and 99.99% respectively when the detection time was 62.23 ms and 57.41 ms, respectively. As damaged nodes increased, forwarding nodes for all four schemes began to increase. However, forwarding nodes in the IMACO-SSP scheme was significantly more than other schemes. When searching for a key point in the system, the energy consumption of the IMACO-SSP scheme was always lower than the other three algorithms. Applying the IMACO-SSP scheme to the vehicle networking and enterprise office networking, when there were 1780 and 2000 intrusion nodes respectively, foreign intrusions caused damage to the key space and steal secrets. When the IMACO-SSP scheme ran for 50 rounds, the number of dead nodes in the factory workshop network and enterprise office network was 74 and 71, respectively. The number of dead nodes in the other three schemes was significantly greater than 70. The above results indicate that the IMACO-SSP scheme can significantly improve the balance of network energy consumption while maintaining high energy efficiency, and significantly affects the availability and reliability of WSN

in resource limited environments. But the experimental simulations are all small-scale WSNs, and in practical applications, the network size may be larger. Therefore, in future research, the feasibility and security of the scheme should be considered when applied to larger networks.

Funding

The research is supported by Research on Data Security and Integrity Assurance Technology with a Combination of Digital Forensics and Wireless Sensor Network Security, Initial Achievement of Doctoral Startup Project of Hunan University of Arts and Sciences (No. 24BSQD13).

References

[1] Nwokoye C N H, Madhusudanan V. Epidemic models of malicious-code propagation and control in wireless sensor networks: an indepth review. Wireless Personal Communications, 2022, 125(2): 1827–1856.
[2] Lin H Y. Integrate the hierarchical cluster elliptic curve key agreement with multiple secure data transfer modes into wireless sensor networks. Connection Science, 2022, 34(1): 274–300.
[3] Hasanvand M, Nooshyar M, Moharamkhani E, Selyari A. Machine Learning Methodology for Identifying Vehicles Using Image Processing//Artificial Intelligence and Applications. 2023, 1(3): 170–178.
[4] Mokayed H, Quan T Z, Alkhaled L, Sivakumar V. Real-time human detection and counting system using deep learning computer vision techniques//Artificial Intelligence and Applications. 2023, 1(4): 221–229.
[5] Saraswathi R V, Sree L P, Anuradha K. Dynamic group key management scheme for clustered wireless sensor networks. International Journal of Grid and Utility Computing, 2020, 11(6): 801–814.
[6] Raja Basha A. Energy efficient aggregation technique-based realisable secure aware routing protocol for wireless sensor network. IET Wireless Sensor Systems, 2020, 10(4): 166–174.
[7] Yuan E, Wang L. A key management scheme realising location privacy protection for heterogeneous wireless sensor networks. International Journal of Sensor Networks, 2020, 32(1): 34–41.
[8] Kumar C P, Selvakumar R. Reliable and secure data communication in wireless sensor networks using optimal locally recoverable codes. Peer-to-Peer Networking and Applications, 2020, 13(3): 742–751.

[9] Prakash G, Krishnamoorthy R, Kalaivaani P T. Resource key distribution and allocation based on sensor vehicle nodes for energy harvesting in vehicular ad hoc networks for transport application. The Journal of Supercomputing, 2020, 76(8): 5996–6009.
[10] Ramesh S, Yaashuwanth C. Enhanced approach using trust based decision making for secured wireless streaming video sensor networks. Multimedia tools and applications, 2020, 79(15–16): 10157–10176.
[11] Ahlawat P, Dave M. An attack resistant key predistribution scheme for wireless sensor networks. Journal of King Saud University-Computer and Information Sciences, 2021, 33(3): 268–280.
[12] Xiong P, Su Q. Key distribution strategy of wireless sensor network based on multi-hash chain. Journal of Web Engineering, 2021, 20(3): 713–742.
[13] Mitchell C J. How not to secure wireless sensor networks: a plethora of insecure polynomial-based key pre-distribution schemes. IET Information Security, 2021, 15(3): 223–230.
[14] Rajasoundaran S, Prabu A V, Kumar G S, Malla P P, & Routray S. Secure opportunistic watchdog production in wireless sensor networks: a review. Wireless Personal Communications, 2021, 120(2): 1895–1919.
[15] Krishnapriya M, Angeline Prasanna G, Anbarasu S. Rank-Based Energy-Efficient Key Management Routing for Wireless Sensor Network-Based Iot Medical Sensors. Wireless Personal Communications, 2023, 130(3): 2175–2196.
[16] Wang Y, Liu Y, Feng W, Zeng S. Waste Haven Transfer and Poverty-Environment Trap: Evidence from EU. Green and Low-Carbon Economy, 2023, 1(1): 41–49.
[17] Aryavalli S N G, Kumar G H. Futuristic Vigilance: Empowering Chipko Movement with Cyber-Savvy IoT to Safeguard Forests. Archives of Advanced Engineering Science, 2023, 1(8): 1–16.
[18] Palani U, Amuthavalli G, Alamelumangai V. Secure and load-balanced routing protocol in wireless sensor network or disaster management. IET Information Security, 2020, 14(5): 513–520.
[19] Wang J, Yue K, Duan L. Models and Techniques for Domain Relation Extraction: A Survey. Journal of Data Science and Intelligent Systems, 2023, 3(1): 16–25.
[20] Liu W, Harn L, Weng J. Lightweight key establishment with the assistance of mutually connected sensors in wireless sensor networks (WSNs). IET Communications, 2022, 16(1): 58–66.

[21] Dinesh Kumar P, Valarmathi K. Fuzzy based hybrid BAT and firefly algorithm for optimal path selection and security in wireless sensor network. Automatika, 2023, 64(2): 199–210.
[22] Kittur L J, Pais A R. Combinatorial design based key pre-distribution scheme with high scalability and minimal storage for wireless sensor networks. Wireless Personal Communications, 2023, 128(2): 855–873.

Biography

Xiaoyan Luo received her Bachelor's degree from Hunan Normal University majoring in Computer Science and Technology (2005), her Master's degree from Hunan University majoring in Computer Application Technology (2010), and her Doctoral degree from the Philippines Christian University majoring in Curriculum and Instruction (2023). At present, she holds the position of Deputy Director in the Academic Affairs Office of Hunan University of Arts and Sciences and is engaged in teaching courses such as "University Computer Fundamentals" and "C Language Programming". She has presided over several provincial and ministerial level projects and published articles in several well-known journals, and her research areas include image processing, information security and curriculum pedagogy.