WSN Secure Routing Planning Algorithm Based on MOACO

Qian Mei[1,*], Jie Li[2] and Zhiyong Si[1]

[1]*Information Office (Big Data Management Center), Zhengzhou Railway Vocational and Technical College, Zhengzhou 450000, China*
[2]*School of Intelligent Engineering, Henan Mechanical and Electrical Vocational College, Zhengzhou 450000, China*
E-mail: Meiqian1212026@outlook.com; lijie_hpu@126.com; sizhiyong@zzrvtc.edu.cn
[*]*Corresponding Author*

Received 21 January 2026; Accepted 13 April 2026

Abstract

This study proposes a secure routing planning algorithm that integrates an improved Dempster-Shafer Evidence Theory (D-S ET) and enhanced Multi-Objective Ant Colony Optimization (MOACO) to balance security protection and Energy Consumption (EC) in Wireless Sensor Networks (WSN). For the D-S ET, we correct third-party recommendation bias by calculating evidence distance and introducing discount coefficients, thereby optimizing its conflict handling mechanism, solving the problem of node credibility misjudgment caused by traditional evidence fusion, and achieving accurate Node Trust Evaluation (NTE) through a direct and indirect dual trust mechanism. For MOACO, we integrated elite retention strategy, improved crowding distance, and mutation convergence operation to optimize the Pareto optimal solution set, improving the search accuracy and stability of the algorithm, and achieving multi-objective routing optimization with node trust value and remaining energy as the core objectives. Based on a 100 node WSN simulation environment, the algorithm was compared with typical baseline methods under

Journal of Cyber Security and Mobility, Vol. 15_3, 683–708.
doi: 10.13052/jcsm2245-1439.1537

consistent initial parameter settings. The experimental results show that when the proportion of Malicious Nodes (MN) is 25%, the detection rate of MN in this algorithm is 84.5%, and the false positive rate is 9.2%, which is better than the comparative methods. In terms of routing performance, it extends the lifecycle of WSN to 937 rounds, maintaining a stable throughput of 4344 bps and a minimum average delay of 33 ms. Without black hole attacks, the MN is only 37.5 J. Faced with 10 single type black hole attack nodes, its MN decreases by 4.8%, and the packet loss rate is controlled at 9.9%, demonstrating excellent anti-attack performance. This algorithm effectively balances the security and energy efficiency of WSN, and innovative improvements to the core algorithm provide reliable technical support for the efficient and stable operation of WSN, with significant practical application value.

Keywords: Wireless sensor network, secure routing, D-S evidence theory, MOACO.

1 Overview

Wireless Sensor Network (WSN), as the core perception layer technology of the IoT, has been widely used in key fields like environmental monitoring, industrial control, and intelligent security due to its advantages of flexible deployment and low cost. However, WSN nodes are usually deployed in open and unattended complex environments. In addition, the nodes themselves have limited energy and weak computing and storage resources, making them extremely vulnerable to security threats such as Malicious Node (MN) attacks and data tampering [1–4]. At the same time, excessive pursuit of security protection will increase Energy Consumption (EC), shorten the network lifecycle, and form a "security-EC" contradictory dilemma [5, 6]. Currently, WSN secure routing research mostly focuses on single-objective optimization. Some algorithms identify MNs through trust mechanisms but ignore the need for efficient energy utilization. Another part of the energy-saving routing algorithms lacks effective consideration of security protection and is difficult to resist malicious behaviors such as black hole attacks [7, 8]. In addition, traditional trust evaluation models often lead to misjudgments of node credibility due to evidence conflicts, and it is difficult for single-objective optimization algorithms to balance multi-dimensional performance indicators.

Saravanaselvan and Paramasivan proposed a feedforward-backpropagation neural network optimized based on the woodpecker mating algorithm

for secure routing and data encryption problems in WSN. The method was divided into three stages. Stage 1 was based on FFBPNN to form a dynamic clustering sensor network. Stage 2 used elliptic curve-based Hill cipher for key generation for data encryption and decryption. Stage 3 used a homomorphic encryption scheme for timely delivery of aggregated data. Compared with existing models, this method reduced latency by 99.01%, 98.34%, 95.23%, and 97.45% [9]. Kumar et al. proposed an energy-saving optimal routing framework based on Bayesian networks and heuristic genetic algorithms to address issues such as service quality, energy dissipation, processing overhead, and link failures in WSNs. The framework derived disjoint paths by learning node/network connectivity and availability information to alleviate routing issues, improve service quality, and optimize energy efficiency. This framework improved service quality, reduced EC, and ensured the applicability of real-time applications [10]. Sharma et al. proposed a multi-level hierarchical security and optimal routing protocol to address that WSNs used for environmental monitoring are susceptible to illegal intrusion. The protocol was divided into four stages: registration, clustering, authentication, and optimal routing, conducted multi-level trust assessment to detect MNs, and used the chimpanzee optimization algorithm based on polar learning to select the best data transmission path. The protocol had a packet delivery rate of 99.8%, a throughput of 48,000 bits per second, and a detection rate of 95% [11].

Multi-Objective Ant Colony Optimization (MOACO) is a Multi-Objective Optimization (MOO) algorithm built on ant colony behavior and is taken to deal with complex optimization issues. MOACO can optimize multiple objective functions and evaluate the quality of the solution by maintaining the Pareto front. Meanwhile, it has the advantages of fewer parameters and strong robustness. Nasouri and Delgarm proposed a simulation-oriented Pareto optimization method for building energy efficiency in response to the problems of high EC intensity, lack of optimal design, and excessive release of toxic gases in the building industry. This method combined EnergyPlus with the MOACO algorithm to help engineers in optimizing in the early stages of building design. Compared with single-objective optimization, the optimal solution provided by Pareto optimization was more reliable, and the optimized building configuration significantly improved the efficiency of solar collectors with a slight increase in building EC [12]. Amir Prasad et al. designed a hybrid framework fusing Non-Dominated Sorting Genetic Algorithm-III (NSGA-III) and MOACO to address the growing demand for sustainable practices in the construction industry while maintaining

efficiency and cost-effectiveness. Compared with independent NSGA-III, MOACO, teaching-based MOO, and multi-objective Particle Swarm Optimization (PSO), the hybrid framework had superior performance. Trade-off analysis provided actionable insights, revealed connections between goals, and enable informed decision [13]. Hou et al. proposed a MOACO algorithm built on a dynamic constraint evaluation strategy to address small and discontinuous feasible regions in highly constrained optimization problems. The algorithm proposed a dynamic constraint violation metric to evaluate the degree of constraint violation of a solution. Furthermore, for subpopulations with evolutionary advantages, an evolutionary strategy based on dynamic transition probability was proposed to improve evolutionary efficiency, and a Gaussian mutation evolution strategy was proposed to increase the diversity of subpopulations with higher constraint violations. Compared with other constrained MOO algorithms, this algorithm could achieve more satisfactory performance in highly constrained optimization [14].

In summary, although the current secure routing model for WSN can significantly improve its security, it is still difficult to effectively solve the "security-EC" problem. Most trust routing algorithms only achieve MN identification through simple evidence fusion, without designing dynamic correction mechanisms for evidence conflicts, which can easily lead to trust misjudgments, and do not incorporate Node Trust Values (NTV) and remaining energy into a unified MOO framework. Although mainstream multi-objective routing algorithms consider energy optimization, they lack accurate Node Trust Evaluation (NTE) models, making it difficult to effectively avoid MN. When facing malicious behaviors such as black hole attacks, network performance drops sharply. In view of this, this study proposes a WSN-Secure Routing Planning (SRP) algorithm that integrates improved Dempster-Shafer Evidence Theory (D-S ET) and MOACO. It aims to realize the collaborative optimization of WSN security, energy efficiency, and transmission performance, and enhance the network's resistance to malicious behaviors such as black hole attacks. The innovation lies in, first, by optimizing the conflict handling mechanism of D-S ET, an accurate NTE model is constructed and, second, MOACO is improved by combining the elite retention strategy and mutation close operation to achieve multi-objective collaborative optimization of trust value and EC.

The research on the improvement of D-S ET and MOACO is based on the practical requirements of WSN secure routing, and the core technical logic is designed. For D-S ET, the similarity of third-party recommendation trust vectors is quantified by calculating the evidence distance, and the weight of

conflicting evidence is dynamically modified by introducing discount coefficients, replacing the traditional fixed weight fusion method. This resolves trust misjudgments caused by evidence conflicts from the root, making the fusion of direct and indirect trust more in line with the actual behavior of nodes. For MOACO, on the basis of elite retention and crowding distance, a mutation convergence operation is added to achieve precise convergence of the solution through random mutation of individual positions combined with Hamming distance multi-point intersection. At the same time, the crowding distance sorting rule is optimized to solve the problem of uneven distribution of the Pareto solution set in traditional algorithms, making MOO more suitable for the collaborative optimization needs of WSN trust and MN.

The research contribution lies in proposing an improved NTE model based on D-S ET, which optimizes the conflict handling mechanism through evidence distance calculation and discount coefficient, integrates direct indirect dual trust mechanisms, and effectively solves the problem of node reliability misjudgment caused by evidence conflicts. Simultaneously improving the MOACO algorithm, introducing elite retention strategy, optimizing crowding distance, and mutation convergence operation, to achieve collaborative multi-objective routing optimization of NTV and remaining energy. Through multidimensional experimental verification from a single black hole attack to a combination attack scenario, sensitivity analysis of core parameters has been completed, verifying the robustness, resistance to attacks, and engineering feasibility of the algorithm, providing a new solution for WSN secure routing design.

Section 2 elaborates on the methods and principles of algorithm design, including the construction of an improved D-S ET NTE model and an improved MOACO secure routing model. Section 3 verifies the trust evaluation performance, routing optimization performance, and anti-attack performance of the model through simulation experiments, and conducts parameter sensitivity analysis. Section 4 discusses the experimental results and analyzes the advantages of the algorithm and the limitations of existing research. Section 5 summarizes the research results of the entire text and looks forward to future research directions.

2 Methods and Materials

To reduce EC while ensuring network security, this study proposes a WSN-SRP model based on D-S ET and MOACO. This study first uses the optimized

D-S ET to assess the NTV, and then implements a secure routing protocol through MOACO to avoid MNs with the lowest EC.

2.1 NTE Model Based on Conflict Handling Mechanism and D-S ET

To standardize the symbols, this article adopts a consistent symbol system for trust vectors, time indexes, and node indexes: i and j are used to represent any node index, and t is the time index. The direct/indirect trust vector of node i towards j at time t is denoted as $T_{ij}(t)$, and the comprehensive trust vector is denoted as $T^*_{ij}(t)$. All vector dimensions and element definitions are kept consistent, and the index symbols are reused without ambiguity throughout the process, ensuring the consistency of formula derivation and model description. The NTE model is a key component to achieve secure routing, which improves the overall security and reliability of the network by evaluating the credibility of nodes. Establishing a trust assessment model requires accurate and reasonable trust measurement. D-S ET solves the problems of subjective uncertainty and evidence conflict by combining evidence from various sources and improves the accuracy of trust assessment. The NTE model based on D-S ET is shown in Figure 1.

In Figure 1, the model calculates the direct trust value by comprehensively considering key indicators such as the reception rate, forwarding rate, and consistency of data packets to evaluate the direct credibility of the node. In addition, the model also introduces third-party evidence sources to evaluate the indirect trust of nodes to comprehensively evaluate the reliability of nodes from different perspectives. Direct trust and indirect trust are synthesized through D-S ET to derive a comprehensive trust value, which is then used to evaluate the node's overall trust level to ensure the reliability of the evaluation process [15, 16]. Assuming that there are several mutually exclusive and exhaustive evidence under the recognition framework, according to the D-S

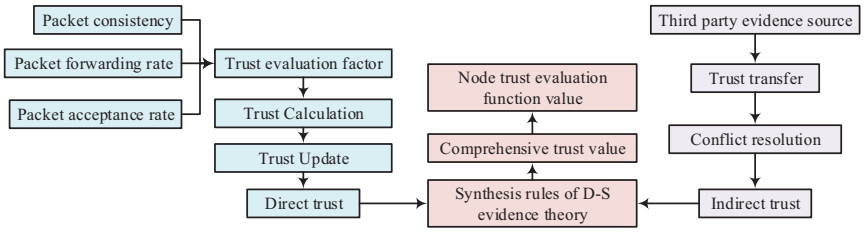


Figure 1 NTE model based on D-S ET.

synthesis rule, its credibility function is as shown in Equation (1).

$$\begin{aligned} c(A) &= (c_1 \oplus c_2 \oplus \cdots \oplus c_n)(A) \\ &= \begin{cases} (1-C)^{-1} \sum\limits_{\cap A_i = A} \bigcap\limits_{1 \le i \le n} c_i(A_i), & A \neq \Phi, \quad A \subset \Omega \\ 0, & A = \Phi \end{cases} \end{aligned} \tag{1}$$

In Equation (1), $c(A)$ is the credibility function of proposition A. c_n is the credibility function of the n-th evidence. C is the conflict factor. Φ is the empty set. Ω is the recognition frame. At the same time, by processing the trust function and likelihood function of D-S ET, the evaluation function can be obtained, as shown in Equation (2).

$$E(A) = t(A) + \frac{|A|}{|\Omega|} \times \ [l(A) - t(A)] \tag{2}$$

In Equation (2), $E(A)$ is the evaluation function. $t(A)$ is the trust function. $|A|$ and $|\Omega|$ are proposition A and the number of elements of the recognition frame. $l(A)$ is the likelihood function. For node credibility assessment, if it has direct knowledge of node behavior, the direct trust model can be used for assessment. The direct trust model mainly relies on direct evidence or information to evaluate the trustworthiness of a node [17, 18]. In this model, trust measures are based on evidence obtained directly from nodes rather than through recommendations or ratings from other nodes. The direct trust vector calculation formula is shown in Equation (3).

$$\begin{aligned} \vec{T}_d(t) &= \begin{bmatrix} Vt_{i,j}(t) \\ Vn_{i,j}(t) \\ Vu_{i,j}(t) \end{bmatrix} = \begin{bmatrix} c(\{T\}) \\ c(\{-T\}) \\ c(\{T,-T\}) \end{bmatrix} \\ &= \begin{bmatrix} \omega_1 S_{R,ij}(t) + \omega_2 S_{T,ij}(t) + \omega_3 S_{C,ij}(t) \\ \omega_1 R_{R,ij}(t) + \omega_2 R_{T,ij}(t) + \omega_3 R_{C,ij}(t) \\ 1 - Vt_{i,j}(t) - Vn_{i,j}(t) \end{bmatrix} \end{aligned} \tag{3}$$

In Equation (3), $\vec{T}_d(t)$ is the direct trust vector. $Vt_{i,j}(t)$ is a trusted value. $Vn_{i,j}(t)$ is an untrusted value. $Vt_{i,j}(t)$ is an uncertain value. $c(\{T\})$, $c(\{-T\})$, and $c(\{T,-T\})$ are the basic credibility functions of trusted values, untrustworthy values, and uncertain values. ω_1, ω_2, and ω_3 are the weights of different evidence sources. $S_{R,ij}$, $S_{T,ij}$, and $S_{C,ij}$ are the reception success rate, forwarding success rate and packet consistency between nodes i

and j. $R_{R,ij}$, $R_{T,ij}$, and $R_{C,ij}$ are the rejection rate, rejection forwarding rate and packet inconsistency between i and j. To avoid increasing the trust value of MNs, this study uses historical interactions during consecutive cycles to update the trust value. In the absence of direct evidence, the indirect trust model is utilized to evaluate the node. In the node trust model, when there is no direct interaction record between nodes a and b, a will query other nodes for their trust in b. By combining the direct and the indirect trust models, a more comprehensive NTE system can be formed. At the same time, to solve the one-vote veto problem of D-S ET, this study improves the combination rules, that is, adjusts the weight according to the similarity. The essence of D-S ET conflict resolution strategy is dynamic weight correction based on evidence distance, which introduces discount coefficients by calculating the similarity of recommendation trust vectors, corrects third-party evidence bias, breaks through the limitations of traditional fixed weight fusion, and resolves trust misjudgments caused by evidence conflicts from the root. The calculation of the evidence distance of the node recommendation trust vector is shown in Equation (4).

$$D_{u,v} = \sqrt{\frac{1}{2}(\vec{T}_{s,ij}^{k_v^2} + \vec{T}_{s,ij}^{k_u^2} - 2\vec{T}_{s,ij}^{k_v}, \vec{T}_{s,ij}^{k_u})}, \quad \mathrm{v} = 1, 2 \ldots, \mathrm{s}; \quad \mathrm{u} =, 2 \ldots, \mathrm{s} \tag{4}$$

In Equation (4), $D_{u,v}$ is the evidence distance. $\vec{T}_{s,ij}^{k_v}$ is the indirect trust vector of node k_v. At this time, the similarity formula between recommended trust vectors is shown in Equation (5).

$$S_{u,v} = 1 - D_{u,v} \tag{5}$$

In Equation (5), $S_{u,v}$ is the similarity between recommended trust vectors. Since the evidence difference degree is inversely proportional to the accuracy of the recommended trust value, to avoid the impact of evidence conflict on trust synthesis, this study introduces a discount coefficient to correct the indirect trust vector. The discount coefficient is shown in Equation (6).

$$\eta_u = \varphi_u / \varphi_{\max} \tag{6}$$

In Equation (6), η_u is the discount factor. φ_u and $\varphi_{\max}$ are the standard weight and the maximum weight. At this time, the comprehensive trust degree and comprehensive evaluation function are as shown in Equation (7).

$$\begin{cases} \vec{C}_{t,ij}(t) = (\vec{T}_{s,ij}^{k_1}(t) \oplus \vec{T}_{s,ij}^{k_2}(t) \oplus \ldots \oplus \vec{T}_{s,ij}^{k_i}(t)) \oplus T_{d,ij}(t) \\ \mathrm{E}_{c,j}(t) = \dfrac{1}{2}\left[l_{i,j}(\{T\}) - t_{i,j}(\{T\})\right] + t_{i,j}(\{T\}) \end{cases} \tag{7}$$

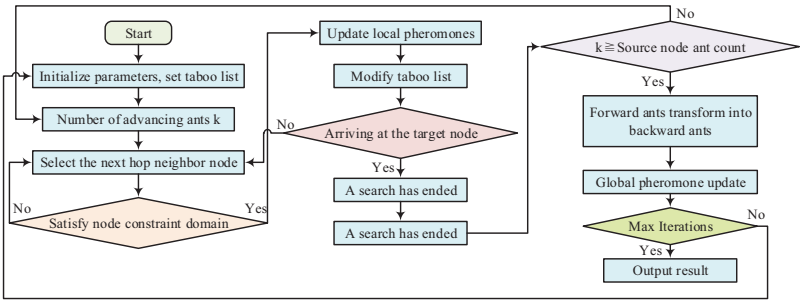


Figure 2 Trusted ant colony routing algorithm.

In Equation (7), $\vec{C}_{t,ij}(t)$ is the comprehensive trust vector. $E_{c,j}(t)$ is the comprehensive evaluation function. $l_{i,j}(\cdot)$ and $t_{i,j}$ are the likelihood function and trust function between nodes i and j. After introducing Ant Colony Optimization (ACO) into the above NTE model, the trusted ant colony routing algorithm can be obtained, as shown in Figure 2.

In Figure 3, the first step is to initialize the parameters, set the taboo table, and start forward ant search. The next step is to select the next hop node, determine whether the constraints are met and update the pheromone, and modify the taboo table at the same time. The next step is to check whether the target node is reached. If it is reached, the ant search will be ended; otherwise, the next search will be continued. If all ant searches are completed, the global pheromone will be updated to check whether the maximum iterations have been reached: if so, the result will be output, otherwise the taboo list will be reset.

2.2 WSN-SRP Model Based on MOACO

After the NTE model is built, the SRP model can be built based on it. Due to the limited resources of WSN, the unilateral pursuit of security will lead to the degradation of other network performance. Therefore, to achieve a balance between energy and security, this study proposes a WSN-SRP model based on MOACO. MOACO is an extended algorithm based on ACO, which is used to solve MOO problems. MOACO aims to optimize multiple conflicting objective functions simultaneously, finding a set of Pareto Optimal Solutions (POSs) that provide different trade-offs between multiple objectives. The process of MOACO is shown in Figure 3.

In Figure 3, Step 1 is parameter initialization and to place a group of ants at the initial point of the current period. The ant with the earliest departure

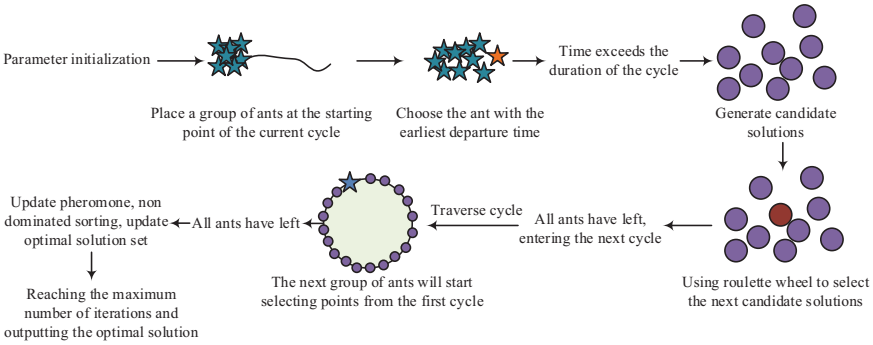


Figure 3 Process of MOACO

time is selected and judged whether it times out. If it does not time out, candidate points will be generated based on constraints and the next point will be selected based on probability. If all the ants in the group have finished walking, it will enter the next cycle, otherwise it will continue [19, 20]. When all cycles are traversed, and if all groups of ants are completed, the pheromone, fast non-dominated sorting and POS sets will be updated. If the maximum iteration is not reached, iteration will continue; otherwise, the optimal solution will be output and ended [21]. The mathematical model of the MOO problem is given by Equation (8).

$$\begin{cases} \min y = f(x) = (f_1(x), f_2(x), \ldots, f_n(x)), & n = (1, 2, \ldots, N) \\ s.t. g_i(x) \leq 0, & i = 1, 2, \ldots, p \\ h_j(x) = 0, & j = 1, 2, \ldots, q \end{cases} \tag{8}$$

In Equation (8), y is the target vector. $f(x)$ denotes the objective function. $f_n(x)$ means the n-th $f(x)$. x is the decision variable. N is the target quantity. $g_i(x)$ and $h_j(x)$ are the i-th and j-th inequality and equality constraints. p is the constraint quantity. q is the equality constraint quantity. To ensure network security and lower network EC at the same time, this study builds a secure routing model with the trust value and node residual energy as the goals, as given by Equation (9).

$$\begin{aligned} &\max f(t) = (f_1(t), f_2(t)) \\ &s.t. \begin{cases} E_i(t) \geq 0 \\ DR_{i,j}(t), DT_{i,j}(t) > 0 \\ 0 \leq t \leq t_{\max} \end{cases} \end{aligned} \tag{9}$$

In Equation (9), $f(t)$ is the secure routing model. $f_1(t)$ and $f_2(t)$ are the objective functions of residual energy and trust value. $E_i(t)$ is the remaining energy of node i at time t. $DR_{i,j}(t)$ and $DT_{i,j}(t)$ are the number of packets received by the node and forwarded by the node. $t_{\max}$ is the maximum simulation time. WSN-SRP aims to achieve efficient energy utilization under security and EC constraints. Security constraints require that the NTV in the path is $\geq$0.23, and MNs are excluded. The EC constraint limits the total EC of the path to no more than 15% of the remaining energy of the network. In the priority rules, security is the primary consideration. After security is met, the remaining energy and transmission delay are optimized through MOACO to extend the network life cycle. The expressions of $f_1(t)$ and $f_2(t)$ are calculated as Equation (10).

$$\begin{cases} f_1(t) = \sum_{j=1}^{N} E_j(t)/N \\ f_2(t) = \sum_{j=1}^{N} T_j(t)/N \end{cases} \tag{10}$$

In Equation (10), $T_j(T)$ is the trust value. By using MOACO to solve the above model, MOO of WSN secure routing can be achieved. The state transition probability $P_{i,j}^k(t)$ of MOACO is shown in Equation (11).

$$P_{i,j}^k(t) = \begin{cases} \dfrac{\begin{array}{c}\tau_{i,j}^{\lambda\alpha}(t)\cdot\mu_{i,j}^{(1-\lambda)\alpha}(t) \\ \cdot\eta_{i,j}^{\lambda\beta}(t)\cdot\vartheta_{i,j}^{(1-\lambda)\beta}(t)\end{array}}{\sum_{l\in \text{alloweal}_k\cap \text{Area}(i)}\tau_{i,j}^{\lambda\alpha}(t)}, & if\ j\in allowed\cap Area(i) \\ \begin{array}{c}\cdot\mu_{ij}^{(1-\lambda)\alpha}(t)\cdot\vartheta_{i,j}^{(1-\lambda)\beta}(t)\end{array} & \\ 0, & other \end{cases} \tag{11}$$

In Equation (11), $\tau_{i,j}$ and $\mu_{i,j}$ are the pheromone concentrations of $f_1(t)$ and $f_2(t)$. Both α and β are weight parameters. λ is the weight value of ants for different goals. $\eta_{i,j}$ and $\vartheta_{i,j}$ are the inspiration pheromones for $f_1(t)$ and $f_2(t)$. The pheromone update formula is shown in Equation (12).

$$\tau_{i,j}^n(t+1) = (1-\rho)\tau_{i,j}^n(t) + \rho\Delta\tau_{i,j}^n(t), \forall(i,j)\in T, n=1,2 \tag{12}$$

In Equation (12), $\tau_{i,j}^n(t+1)$ is the pheromone concentration at time $t+1$. ρ is the pheromone volatility coefficient. $\Delta\tau_{i,j}^n(t)$ is the initial pheromone

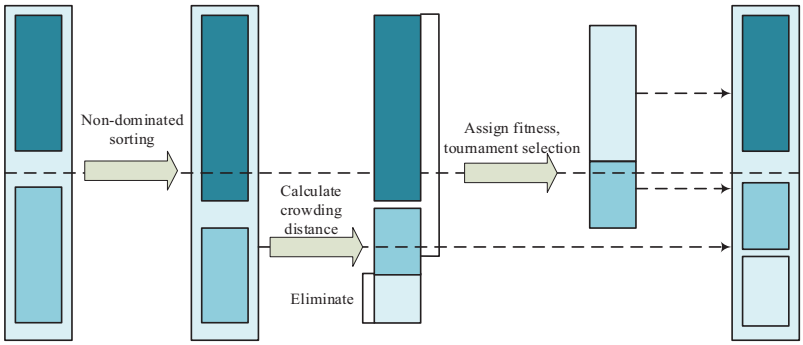


Figure 4 Elite retention strategy.

concentration of the n-th optimization objective. Since the POS set contains a large number of non-inferior solutions, the efficiency of the algorithm is seriously affected. In view of this, this study introduces elite retention strategy and crowding distance to improve algorithm efficiency. MOACO adds mutation convergence dual operations on the basis of elite retention and crowding distance, combining random mutation individual positions with Hamming distance multi-point cross convergence to improve the search accuracy of Pareto solutions. At the same time, it optimizes the crowding distance sorting rules to avoid uneven distribution of solutions and enhance the algorithm's optimization ability and stability. The elite retention strategy is shown in Figure 4.

In Figure 4, during the population update process of each generation, by comparing the newly generated population with the non-dominated layer of the parent population, the optimal individuals are selected to enter the next generation. An elitist strategy selects which individuals should be retained to the next generation based on these layers and crowding distance. In addition, due to sorting according to the crowding distance from small to large and eliminating small solutions, the distribution of Pareto solutions will be uneven [22, 23]. The crowding distance d_c is put into calculation as shown in Equation (13).

$$d_c = \sum_{n=1}^{2} (f_n^{r+1} - f_n^{r-1})/(f_n^{\max} - f_n^{\min}), \quad 1 < r < l \tag{13}$$

In Equation (13), f_n^r denotes the function value of the r-th optima on the objective n. $f_n^{\max}$ and $f_n^{\min}$ are the maximum and minimum function values of the target n. To enhance the search accuracy of the algorithm, this study

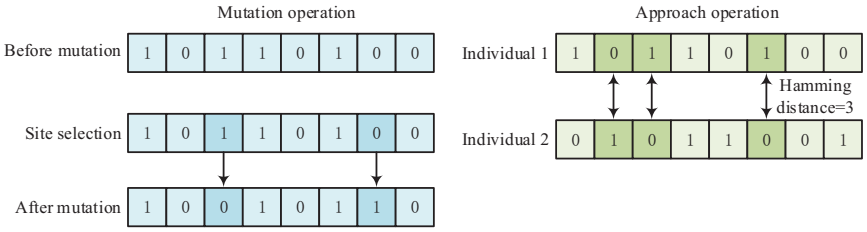


Figure 5 Mutation and convergence operation.

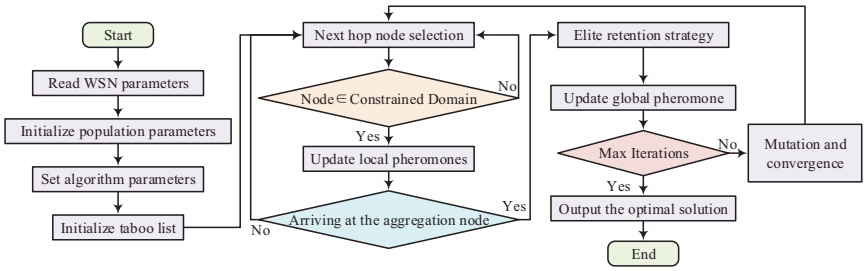


Figure 6 Process for improving MOACO.

also introduces mutation and moving operations to retain the information of excellent individuals in the next generation. The mutation close operation is displayed in Figure 5.

In Figure 5, the operation generates new information individuals by randomly selecting the mutation positions of individuals and replacing them with optional numbers. The moving operation calculates the Hamming distance and uses multi-point cross mutation to move closer to generate new information individuals. At this time, the process of improving MOACO is shown in Figure 6.

In Figure 6, first the WSN and population size are initialized, and the algorithm parameters are set. Next, the taboo list is initialized, and then the next hop node selection is performed. If the node is located within the constraint domain, the local pheromone will be updated; otherwise, the node will be re-selected. At this time, if the ants reach the convergence node, they turn into backward ants. At the same time, each solution is collected and sorted non-dominated, and excellent individuals are retained to screen the Pareto solution set, otherwise the node will be re-selected. Then, the global pheromone is updated. At this time, if the maximum iterations are reached, the optimal solution will be output; otherwise, mutation and close operations will be performed to generate a new population. Here we quantitatively

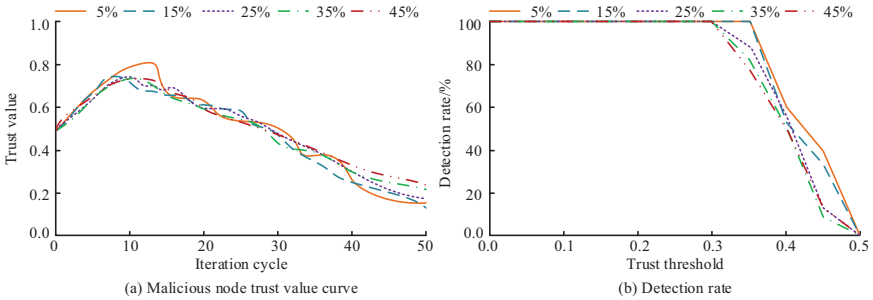
analyze the WSN-SRP algorithm from both time and space complexity perspectives. Let the total number of nodes in WSN be N, The ant population size is M, and the maximum number of iterations for the algorithm is K. In the NTE stage, based on the improved D-S ET trust vector calculation, it is necessary to traverse the interaction information between nodes and third-party recommendation evidence, with a time complexity of $O(N^2)$ and a space complexity of $O(N)$ (storing node trust vectors and evidence matrices). For the MOACO routing optimization stage, the time for a single ant to complete a path search is $O(N)$, the time complexity for population iterative search is $O(M \cdot K \cdot N)$, and the space complexity is $O(M \cdot N)$ (storing ant colony paths and Pareto solution sets). Overall, the algorithm has an overall time complexity of $O(M \cdot K \cdot N + N^2)$ and a space complexity of $O(M \cdot N + N)$. It has excellent computational efficiency in small-scale WSN with N of 100, and the complexity increases polynomial with node size, making it feasible for engineering implementation.

3 Results

To validate the performance of the WSN-SRP, this article tests the NTE model and the secure routing model. The study ensures comparative fairness through unified experimental settings with the same simulation environment, initial parameters, and evaluation indicators. All algorithms are implemented and tested based on the same WSN node size, initial energy, attack scenario, and other basic configurations. The simulations are all implemented on the MATLAB R2023b platform, and are independently repeated 20 times to take the mean to ensure the reliability of the results. WSN nodes are randomly and uniformly deployed in a 100 m $\times$ 100 m monitoring area, using the classic radio MN model (with transmission/reception MN of 50 nJ/bit and 10 nJ/bit, respectively). The traffic model is a Constant Bit Rate (CBR), with continuous and stable data transmission. The network topology is an undirected connected graph, with a communication radius of 50 m. The remaining core simulation parameters are uniformly set and applied to all comparison algorithms.

3.1 Test Results of NTE Model

To verify the performance of the NTE, the article conducts simulation analysis on it and compares it with Dynamic Trust Evaluation based on Multi-Index Fusion (DTEMIF) and Importance Score-Column, Row, and Diagonal



(a) Malicious node trust value curve (b) Detection rate

Figure 7 Trust value curve and detection rate of MNs.

Matrix Decomposition (ISCRUMD). DTEMIF and ISCRUMD were selected as baselines, as they are typical multi-criteria fusion and matrix factorization methods in the current WSN NTE field, widely cited and validated by relevant research. In the experiment, ω_1, ω_2, and ω_3 are 0.04, 0.88, and 0.06, and the constant factors are 0.4–0.6. The initial trust value and initial energy are 0.5 and 2 J, the data forwarding rate of normal nodes is 0.9–1.0, the Packet Loss Rate (PLR) of MNs is 0.1–0.5, the data packet size is 800 bit, and the total amount of nodes is 100. The experiment was independently repeated 20 times, and the mean $\pm$ standard deviation was taken as the final evaluation index to verify the statistical significance of the data. To verify whether the performance difference between the proposed algorithm and the baseline method is statistically significant through independent sample t-test, eliminate the influence of random errors in a single simulation, and ensure the reliability and effectiveness of the experimental conclusions. Under different proportions of MNs, the malicious NTV curve and detection rate are shown in Figure 7.

In Figure 7(a), under different proportions of MNs, as the iteration period grows, the trust value of MNs first increases and then decreases. Taking 15% of MNs as an example, when the iteration period is 8, the trust value of the MN is 0.74, and when the iteration period is 50, its trust value is 0.15. This is because the trust evaluation model may take some time to detect and confirm malicious behavior of nodes. The trust value of the MN may temporarily increase due to the lack of negative feedback. In Figure 7(b), under different proportions of MNs, when the trust threshold reaches 0.3, the detection rate of the model gradually decreases. Taking 45% of MNs as an example, when the trust threshold is less than 0.3, the detection rate is 100%. When the trust threshold is 0.4, its detection rate is 50%. In view of this, after comprehensive consideration, it is more reasonable to set the trust threshold

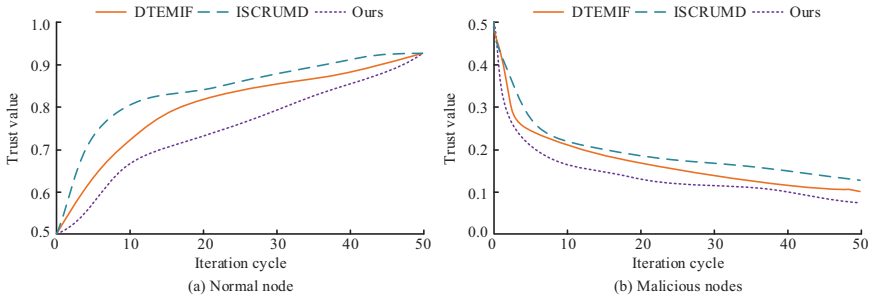


Figure 8 NTVs using different methods.

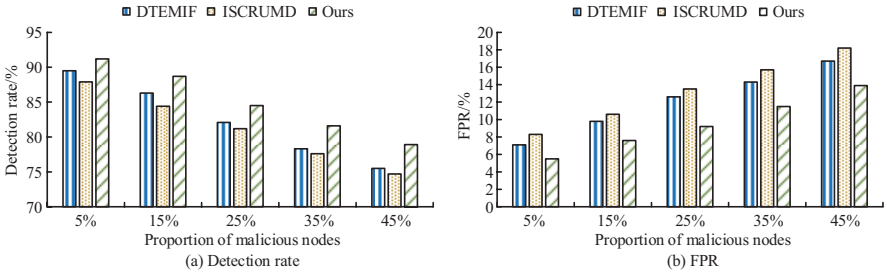


Figure 9 Detection rate and false detection rate of different methods.

to 0.23. This shows that the proposed NTE model is more sensitive to MNs. The NTVs of different methods are shown in Figure 8.

In Figure 8(a), compared with other methods, the normal NTV of the research method increases more slowly, which can effectively increase the trust value quickly in a short period of time. When the iteration period is 20, the normal NTVs of DTEMIF, ISCRUMD, and the research method are 0.82, 0.84, and 0.73. In Figure 8(b), for MNs, the trust value of the research method is smaller. When the iteration period is 20, the malicious NTVs of DTEMIF, ISCRUMD, and the research method are 0.17, 0.19, and 0.13. The research method can more accurately evaluate the trust between WSN nodes. Figure 9 shows the detection rates and False Positive Rates (FPRs) of different methods.

In Figure 9(a), the MN detection rate of the research method is always higher. Taking 25% of MNs as an example, the detection rates of DTEMIF, ISCRUMD, and the research method are 82.1%, 81.2%, and 84.5% (p <0.05). In Figure 9(b), as the proportion of MNs rises, the FPR of each method gradually increases, but the FPR of the research method is always lower than other methods. Taking 25% of MNs as an example, the FPRs of

DTEMIF, ISCRUMD, and the research method are 12.6%, 13.5%, and 9.2% (p <0.05). The research method can more accurately identify MNs in WSN.

3.2 WSN Secure Routing Model Test Results

To validate the performance of the research method, it is tested and compared with Secure Routing Model based on Multi-Factor Trust Mechanism (SRMMFTM) and Non-dominated Sorting Multi-Objective Hiking Optimization Algorithm (NSMOHOA). SRMMFTM and NSMOHOA were selected as baselines, as they are respectively classic multi-factor trust routing models and mainstream MOO routing algorithms, which are highly consistent with the research direction of this paper and have comparative reference value. In the experiment, the initial energy of WSN is 0.5 J, the length of the data packet sent and the length of control information are 4000 bit and 200 bit, the maximum amount of hops is 10, and the nodes are 100. The Number of Surviving Nodes (NoSNs), remaining energy, throughput and delay of different methods are shown in Figure 10.

In Figure 10(a), the NoSNs of SRMMFTM and NSMOHOA begins to decrease after iterations of 646 and 753 rounds, while the NoSNs of the research method begins to decrease after iteration of 892 rounds. In

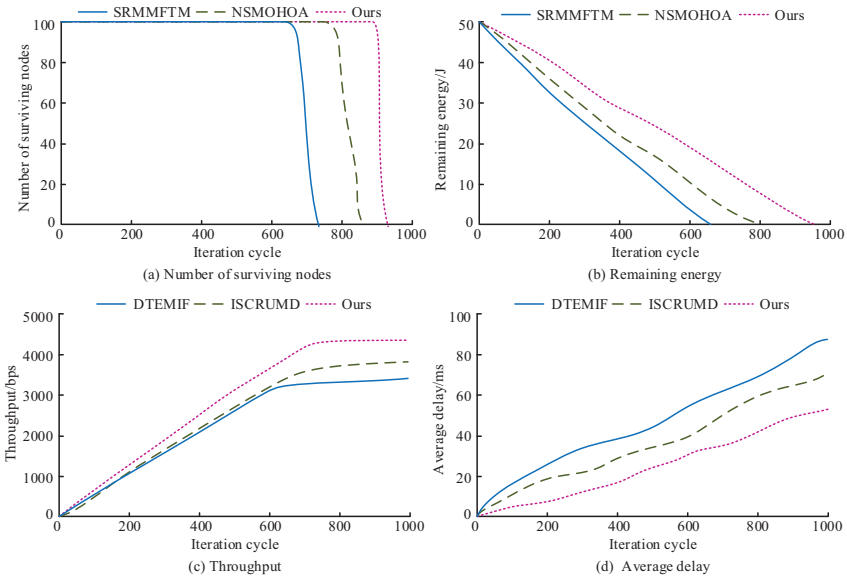


Figure 10 NoSNs, remaining energy, throughput, and time delay.

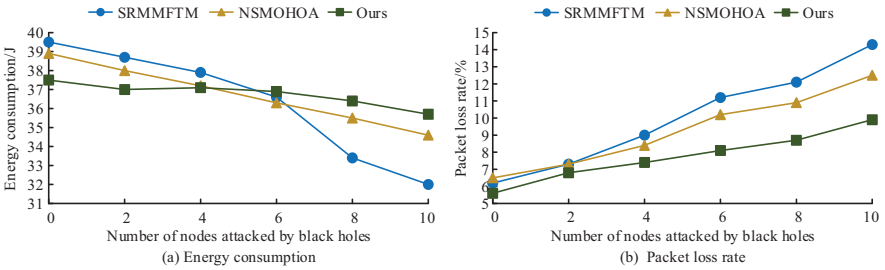


Figure 11 EC and PLR of different methods.

Figure 10(b), SRMMFTM and NSMOHOA consume the energy of all nodes after iterations of 638 and 800 rounds, while the research method only consumes the energy of all nodes after iteration of 937 rounds. Research methods can effectively extend the life cycle of WSN. In Figure 10(c), the throughput of SRMMFTM and NSMOHOA is stable at 3468 bps and 3921 bps, while the research method is stable at 4344 bps. In Figure 10(d), at 600 rounds of iteration, the average delays of SRMMFTM, NSMOHOA, and the research method are 55 ms, 40 ms, and 33 ms. The research method has shorter delay, which can not only effectively ensure the throughput of WSN, but also reduce its delay. The EC and PLR of different methods are shown in Figure 11.

In Figure 11(a), as the number of Black Hole Attack Nodes (BHANs) rises, the EC of each method gradually decreases. When no black hole attack occurs, the EC of the research method is only 37.5J. When the number of NoSNs is 10, the EC of SRMMFTM and NSMOHOA is reduced by 19.0% and 11.1%, while the research method only reduces by 4.8% ($p < 0.05$). MN attacks will not have a large impact on the EC of the research method. In Figure 11(b), when the number of NoSNs is 2, the PLRs of SRMMFTM, NSMOHOA, and the research method are 7.3%, 7.3%, and 6.8%. When the number of NoSNs is 10, the PLRs of the three methods are 14.3%, 12.5%, and 9.9% ($p<0.05$). The research method can effectively resist attacks from MNs. The routing load is shown in Table 1.

In Table 1, when the number of NoSNs does not exceed 3, the routing overhead of the research algorithm is slightly larger than that of others. This is because the research method requires additional routing control packets. When the number of NoSNs is greater than 4, the research algorithm can more effectively avoid MNs and reduce routing overhead through the deepening of the trust model. To verify the robustness and strength of the proposed algorithm, parameter sensitivity analysis is conducted on core parameters

Table 1 Routing load

Number of Nodes Attacked by Black Holes	SRMMFTM	NSMOHOA	Ours
0	0.45	0.44	0.45
1	0.46	0.43	0.46
2	0.46	0.43	0.46
3	0.48	0.45	0.47
4	0.50	0.47	0.48
5	0.51	0.50	0.49
6	0.54	0.54	0.50
7	0.58	0.56	0.49
8	0.59	0.57	0.49
9	0.62	0.59	0.52
10	0.64	0.62	0.54

Table 2 Parameter sensitivity analysis results

Core Parameter	Evidence Discount Coefficient	Pheromone Volatility Coefficient	Mutation Probability
Value range	0.10–0.90	0.01–0.10	0.05–0.20
Detection rate fluctuation range	$\leq$2.1%	$\leq$1.8%	$\leq$1.5%
WSN lifecycle fluctuation range	$\leq$3.5%	$\leq$2.9%	$\leq$2.3%
Optimal value	0.60	0.05	0.11

of the NTE model and improved MOACO, including evidence discount coefficient, pheromone volatility coefficient, and mutation probability. Taking MN detection rate and WSN lifecycle as evaluation indicators, the single-factor variable method is adopted for simulation, with parameters adjusted in their respective reasonable ranges, and the results are shown in Table 2.

As shown in Table 2, the fluctuation ranges of the two key indicators are all less than 3.5% when the core parameters change in the reasonable range, which indicates that the proposed algorithm has low sensitivity to core parameters and strong robustness. The optimal values of each parameter are determined through the analysis, which not only ensures the optimal performance of the algorithm, but also provides a reliable parameter configuration basis for the practical application of the algorithm in different WSN scenarios. To explore the algorithm performance under complex attack scenarios, a combined attack test is conducted, which simulates the coexistence of black hole attack, selective forwarding attack, and data tampering attack in WSN. The number of MN is set to 10, and the attack intensity is consistent with the single attack test. SRMMFTM and NSMOHOA are still used as the

Table 3 Performance comparison under combined attack.

Algorithm	Detection Rate (%)	Packet Loss Rate (%)	Energy Consumption Attenuation Rate (%)
SRMMFTM	62.3	21.5	18.7
NSMOHOA	68.9	17.2	13.5
Ours	76.4	12.8	7.3

comparison methods, with the detection rate, PLR and MN attenuation rate as evaluation indicators. The test results are shown in Table 3.

The results show that the proposed algorithm still maintains a relatively high MN detection rate under combined attacks, and the PLR and MN attenuation rate are significantly lower than the comparison methods. This is due to the accurate NTE of the improved D-S ET and the MOO of the improved MOACO, which enables the algorithm to effectively identify multi-type malicious behaviors and maintain the stable operation of the network under complex attack scenarios. However, the detection rate of the algorithm is reduced by about 8% compared with the single black hole attack, which indicates that the defense capability for combined attacks needs to be further optimized.

4 Discussion and Interpretation

WSN consists of a large number of wireless nodes with low cost, low power consumption, and limited computing power. It can monitor and collect environmental information in real time and transmit the processed information to users. However, since WSN nodes usually have limited computing, storage, and energy resources, it is necessary to design efficient and low-energy routing protocols. The application environment of WSN determines that the network itself is vulnerable to attacks by MNs, so security issues are the primary consideration. To isolate MNs in the network, prevent data from being tampered with, forged, or leaked, and reduce network EC, this study proposes a WSN-SRP that integrates the improved D-S ET and MOACO to balance network security and energy efficiency.

At the NTE level, compared with DTEMIF and ISCRUMD, this study optimizes D-S ET through the conflict handling mechanism and introduces a discount coefficient to correct the third-party recommendation bias, effectively solving the problems of misjudgment of MNs and falsely high trust values of normal nodes in the traditional trust model. Experiments show that the model has a detection rate of up to 84.5% for MNs and an FPR as low as

9.2%. It can avoid MN camouflage behavior by dynamically updating trust values, laying a reliable node selection basis for secure routing. However, the weight setting of trust evaluation factors is based on empirical values. In scenarios where node density changes dynamically, parameter configuration needs to be further optimized through adaptive algorithms.

At the routing optimization level, the MOACO framework achieves a collaborative trade-off between trust value and node remaining energy through MOO. Compared with SRMMFTM and NSMOHOA, the proposed algorithm extends the life cycle of WSN by 18.4∼38.3%, increases the throughput by 10.8∼25.5%, and has better EC stability and anti-packet loss performance under black hole attacks. This is due to the optimization of the Pareto solution set by the elite retention strategy and improved crowding distance, as well as the algorithm search accuracy enhanced by the mutation close operation.

The above results show that the research method can effectively balance EC and security and reduce network EC as much as possible while ensuring WSN security. However, in large-scale networks, the computational overhead of pheromone update and non-dominated sorting will increase significantly. The resistance performance of this algorithm to single type black hole attacks has been experimentally verified to be excellent, but its defense ability against composite network attacks such as collusion attacks, witch attacks, and selective forwarding has not been validated, and it is currently unable to achieve universal attack resistance. In high-density relay node scenarios, the disguise and concealment behavior of MN will reduce the accuracy of algorithm detection, and the generalization of attack defense still needs to be further improved. In the future, the clustering routing mechanism can be combined to simplify the search space and improve the real-time performance of the algorithm. In addition, this study only tests for black hole attack scenarios. Follow-up work needs to be expanded to compound attack scenarios such as Sybil attacks and selective forwarding to further verify the robustness of the algorithm and explore integration paths with lightweight encryption technology to build a more comprehensive WSN security protection system.

5 Summary

To solve the balance problem between security protection and EC in WSN, this study proposed an SRP algorithm that integrates improved D-S ET and MOACO. By building an accurate NTE model to identify MNs and combining it with MOACO to achieve multi-objective routing optimization, it ultimately achieved the core goals of ensuring network security, reducing

EC, and improving transmission performance. In experiments, the proposed NTE model performed excellently. When the ratio of MNs was 25%, the detection rate of MNs reached 84.5%, and the FPR was 9.2%. Compared with DTEMIF and ISCRUMD, it could more accurately distinguish between normal nodes and MNs. The trust value of normal nodes increased more slowly, while the trust value of MNs was lower. At the same time, the research model significantly improved the overall network performance. The lifecycle of WSN was extended to 937 rounds, which was 43.7% and 17.1% higher than SRMMFTM and NSMOHOA. The throughput was stable at 4344 bps, the latency was as low as 33 ms, and the EC was 37.5 J. In the scenario of 10 NoSNs, the EC dropped by only 4.8%, and the PLR was controlled at 9.9%, demonstrating stronger attack resistance and stability. The research algorithm effectively balances the security and energy efficiency of WSN, improves network transmission quality and anti-interference capabilities, provides a reliable routing solution for the safe and efficient operation of WSN, and has important practical application value.

References

[1] Luqman M, Faridi A R. Secure data transmission in wireless networking through node deployment and Artificial Bird optimized deep learning network. Telecommunication Systems, 2024, 87(4):1067–1086. DOI: 10.1007/s11235-024-01225-3.

[2] Jadidoleslamy H. A Secure, Hierarchical and Clustered Multipath Routing Protocol for Homogenous Wireless Sensor Networks: Based on the Numerical Taxonomy Technique. International Journal of Computer Science and Network Security, 2025, 23(8):121–136. DOI: 10.22937/IJCSNS.2023.23.8.16.

[3] Wang J. Identification of SQL Injection Security Vulnerabilities in Web Applications Based on Binary Code Similarity. Journal of Cyber Security and Mobility, 2024, 13(6):1239–1262. DOI: 10.13052/jcsm2245-1439.1361.

[4] Deng X, Pan Y, Fang H. Anomaly Detection in Smart Grid Behavior Monitoring via Federated Learning: A Privacy-Preserving Defense Against Cyber-Physical Attacks. Journal of Cyber Security and Mobility, 2025, 14(5): 1151–1172. DOI: 10.13052/jcsm2245-1439.1455.

[5] Chen E. Analysis of E-commerce Security Protection Technology Based on YOLO Algorithm Optimized by Lightweight Neural Network.

Journal of Cyber Security and Mobility, 2025, 14(4): 849–876. DOI: 10.13052/jcsm2245-1439.1444.

[6] Dharma T M, Srinivasan R. Multi-objective Trust-aware Dynamic Weight Pelican Optimization Algorithm for Secure Cluster Head and Routing Selection in WSN. Journal of Electrical Systems, 2024, 20(3):89–102. DOI: 10.52783/jes.1243.

[7] Kumar L, Kumar P. BITA-Based Secure and Energy-Efficient Multi-Hop Routing in IoT-WSN. Cybernetics and Systems, 2023, 54(6):809–835. DOI: 10.1080/01969722.2022.2110683.

[8] Khan A B F. An Enhanced Multi Attribute Based Trusted Attack Resistance (EMBTR) for the Secure Routing of Sensor Nodes in Wireless Sensor Network. Wireless Personal Communications: An International Journal, 2024, 137(4):2397–2407. DOI: 10.1007/s11277-024-11504-6.

[9] Saravanaselvan A, Paramasivan B. FFBP Neural Network Optimized with Woodpecker Mating Algorithm for Dynamic Cluster-based Secure Routing in WSN. IETE Journal of Research, 2024, 70(7):6515–6524. DOI: 10.1080/03772063.2023.2300349.

[10] Kumar A P, Sunitha R, Chaithra M, Dhananjaya S, Kavyasri M N, Nandini G. An Energy-Efficient and Secure WSN Routing Protocol Using Bayesian Networks and Elitist Genetic Algorithms. Journal European des Systemes Automatises, 2024, 57(6):1547–1555. DOI: 10.18280/jesa.570601.

[11] Sharma V, Beniwal R, Kumar V. Multi-level trust-based secure and optimal IoT-WSN routing for environmental monitoring applications. Journal of Supercomputing, 2024, 80(8):11338–11381. DOI: 10.1007/s11227-023-05875-z.

[12] Nasouri M, Delgarm N. Efficiency-based Pareto Optimization of Building Energy Consumption and Thermal Comfort: A Case Study of a Residential Building in Bushehr, Iran. Journal of Thermal Science, 2024, 33(3):1037–1054. DOI: 10.1007/s11630-023-1933-5.

[13] Amir Prasad B, Trupti Ravindra C, T C Manjunath, Shaik C, Chandrakar V K S, Swapnil V. NSGA-III and MOACO-based decision-making framework for optimizing time, cost, quality, and carbon footprint in bridge construction: a hybrid approach. Asian Journal of Civil Engineering, 2025, 26(6):2331–2347. DOI:10.1007/s42107-025-01311-0.

[14] Hou Y, Qin X, Han H, Wang J. Multiobjective Ant Colony Optimization Algorithm Based on Dynamic Constraint Evaluation Strategy for Highly Constrained Optimization. Cybernetics, IEEE Transactions on, 2025, 55(10):4570–4582. DOI: 10.1109/TCYB.2025.3591275.

[15] Agoramoorthy M, Maheswari S, Hemlathadhevi A, Palani H K. Blockchain-empowered secure localisation scheme in WSN using trust assessment and deep adaptive extreme learning. International Journal of Wireless and Mobile Computing, 2025, 29(3):213–231. DOI: 10.1504/IJWMC.2025.148585.

[16] Das R, Dwivedi M. Cluster head selection and malicious node detection using large-scale energy-aware trust optimization algorithm for HWSN. Journal of Reliable Intelligent Environments, 2024, 10(1):55–71. DOI: 10.1007/s40860-022-00200-6.

[17] Wang C, Liu G, Jiang T. Malicious Node Detection in Wireless Weak-Link Sensor Networks Using Dynamic Trust Management. IEEE Transactions on Mobile Computing, 2024, 23(12):12866–12877. DOI: 10.1109/TMC.2024.3418826.

[18] Ahlawat P, Bathla R. A multi-objective optimization modeling in WSN for enhancing the attacking efficiency of node capture attack. International Journal of Systems Assurance Engineering and Management, 2023, 14(6):2187–2207. DOI: 10.1007/s13198-023-02048-2.

[19] Kiran Sree P, Trupti Ravindra C, Víctor Daniel J, Macedo, TC, Manish B, Krushna Chandra S. Opposition-based multi-objective ant colony optimization framework for sustainable retrofitting: time–cost–energy–risk trade-offs. Asian Journal of Civil Engineering, 2025, 26(5):2223–2239. DOI: 10.1007/s42107-025-01309-8.

[20] Poudel Y K, Bhandari P. Control of the BLDC motor using ant colony optimization algorithm for tuning PID parameters. Archives of Advanced Engineering Science, 2024, 2(2): 108–113. DOI: 10.47852/bonviewaaes32021184.

[21] Mrabet N, Benzazah C, El Akkary A, Sefiani N. Multi-Objective Ant Colony Optimization for Enhancing the Maximum Power of Variable-Speed Wind Turbines Based on PMSG. International Journal on Energy Conversion, 2023, 11(5):195–204. DOI: 10.15866/irecon.v11i5.24121.

[22] Xie G, Wei H E, Wangwen H U, Su Y, Shi B. Application of an improved ant colony algorithm based on unevenly distributed pheromone and multi-objective optimization in path planning for unmanned surface vehicles. Chinese Journal of Ship Research, 2025, 20(1):115–124. DOI: 10.19693/j.issn.1673-3185.04207.

[23] Backman J, Uusitalo J, Holmstrm E, Nikander J, Vtinen K, Jylh P. A multi-objective optimization strategy for timber forwarding in cut-to-length harvesting operations. International Journal of Forest Engineering, 2023, 34(2):267–283. DOI: 10.1080/14942119.2022.2149003.

Biographies

Qian Mei received her master's degree from Henan Polytechnic University (2013). Presently, she is working as a Section Chief in the Information Office (Big Data Management Center) of Zhengzhou Railway Vocational and Technical College. Her research focus is computer application technology, and she has conducted in-depth research on wireless sensor network algorithms. She has published two EI-indexed papers, obtained five invention patents and five utility model patents. As the first associate editor, she co-authored a textbook and won seven Innovation and Application Awards granted by the Department of Education of Henan Province.

Jie Li received her master's degree from Henan Polytechnic University. She is currently a full-time faculty member in the Institute of Intelligent Engineering, Henan Mechanical and Electrical Vocational College. Her research focuses on intelligent control technology and industrial automation. She has made outstanding achievements in curriculum development, teaching reform, and skills competitions. She has presided over a number of provincial-level projects, published four papers in core journals, obtained five invention patents and more than 10 utility model patents.

Zhiyong Si received his master's degree from The PLA Information Engineering University in 2005. He currently works in the Information Office (Big Data Management Center) of Zhengzhou Railway Vocational and Technical College. His research interests include network architecture, network attack and defense, multimedia processing, and large model applications. He has participated in many provincial-level projects and won seven Innovation and Application Achievement Awards granted by the Department of Education of Henan Province.