Multi-hop Network Security Strategy Integrating ACO Algorithm and PSO Algorithm

Qian Hao*, Haixin Huang
Electronic Information Engineering College, Henan Polytechnic Institute, Nanyang, 473000, China
E-mail: haoqian_hao@outlook.com
*Corresponding author

Keywords: multi-hop network, particle swarm optimization algorithm, ant colony abnormal data detection, punishment factor

Received: November 5, 2024

Multi-hop networks are widely used due to their wide coverage and strong adaptability. However, multi-hop networks are prone to attacks and user privacy breaches when transmitting data between nodes. Therefore, a multi-hop network security protection strategy binding particle swarm optimization algorithm and ant colony algorithm was proposed. Support vector machine was utilized for data sorting, and the particle swarm algorithm was improved using inertia weight coefficients. The heuristic function and pheromone update strategy of ant colony algorithm was optimized, and the penalty factor and kernel function of support vector machine were optimized using fusion algorithm. The experimental results showed that the information exposure probability of the fusion algorithm decreased from the initial 0.35% to 0.10%, the detection accuracy was 2.9% higher than that of the second-best method, respectively, and the hazardous response time, disposal time, and root-mean-square error were faster than that of the second-best method by 19.9ms, 22.7ms, and -2.3ms. The running cost of the fusion algorithm was 210 datasets lower than that of the second-best method, and the average computation time was only 27.2ms higher than the normal support vector machine, and the time complexity was lower for all of them. From this, it can be concluded that fusion algorithms can effectively enhance the detection capability of abnormal data, reduce the probability of user privacy data exposure, decrease algorithm operating costs, and improve the response and handling speed of multi-hop networks when facing attacks.

Povzetek: Predlagana je strategija varovanja večskokovnih omrežij, ki združuje algoritma optimizacije roja delcev (PSO) in kolonije mravelj (ACO), izboljšuje zaznavo anomalij ter zmanjšuje stroške in tveganja izpostavljenosti podatkov.

1 Introduction

Multi-hop relay technology is a wireless communication technology proposed by the United States in the 1970s, which forms a self-organizing network through mobile nodes and relay nodes. It has been widely used in communication systems such as satellite relay, microwave relay, and battlefield communication [1]. As mobile communication technology advances, multi-hop networks, which offer benefits like swift long-distance transmission speeds and extensive coverage, are gaining widespread adoption [2]. Multi-hop networks transmit data through multiple intermediate nodes, each of which can be a sender or receiver. Communication tasks can be completed between any two nodes, and even if a node or link fails, other paths can be used to complete data transmission [3-4]. Multi-hop networks can also communicate with distant nodes by changing the data transmission range of individual nodes [5-6]. However, due to the large number of nodes, multi-hop networks are vulnerable to attacks and can lead to the leakage of user privacy data. Existing multi-hop network security protection strategies have problems such as low accuracy in detecting irregular data, insufficient detection precision, and high operating costs. To address the security issues of multi-hop networks, Singh et al. proposed a new quantum atomic search optimization combined with blockchain to solve problems such as collusion attacks, latency, and lifecycle extension in wireless self-organizing networks. This scheme adopted quantum atomic search to choose the optimal relay point for complex multi-hop transmission, and performed data transmission on the blockchain to ensure system security. Experiments showed that the throughput of this method reached 91.5%, energy consumption was reduced to 40%, end-to-end latency was reduced by 20.6%, and security performance was significantly improved [7]. Ezzati Khatab et al. proposed a machine learning relay assisted authentication method for dual hop multi-input multi-output systems to solve the authentication problem in wireless networks. This method used channel characteristics for end-to-end authentication, and to simulate actual situations, defective hardware was used for channel estimation. Experiments showed that this method significantly improved authentication performance, with authentication accuracy exceeding 90% in both single hop and multi-hop scenarios [8].

Mahapatra et al. raised a novel bidirectional butterfly optimization algorithm grounded on clustering tree enhancement to solve the security matters of underwater wireless ad hoc networks. The algorithm designed clusters based on data routing protocols in the first stage, evaluated the trust value of each node using fusion rules in the second stage, and allocated secure channels for data transmission in the third stage. The test reflected that the packet delivery rate of this algorithm reached 90%, the energy consumption was reduced to 0.14J, the network lifetime of 200 rounds was 732s, and the end-to-end delay was 0.12 s, which was significantly better than other algorithms [9]. Pattanayak et al. proposed a new decoding and forwarding protocol grounded on multi-hop hybrid radio frequency and free space optics for the data confidentiality capability of multi-hop networks. This protocol selected a received signal with high confidentiality capability at each hop, and each node in the system was attached to its subsequent nodes through parallel radio frequency and wireless optical communication connections. The experiment showed that the confidentiality interruption probability of this protocol was low, the strict positive confidentiality ability was high, and the confidentiality performance was better than other methods [10]. Altuwairiqi proposed a new multi-hop routing optimization scheme based on improved honey badger algorithm in order to solve the security and energy problems of multi-hop networks. The scheme used the Improved Honey Badger algorithm to select the optimal number of hops and utilized a trust model incorporating indirect and direct trust, data, integrity, and forwarding rate to achieve security-conscious multi-hop routing. Experiments showed that the total number of data received by this scheme under the same conditions was much larger than other methods and the information exposure probability was on average 3.47% lower than other methods [11]. Altowaijri et al. proposed an efficient multi-hop routing protocol in order to ensure the transmission efficiency and security of wireless sensor networks. This protocol considered rank-based next hop selection mechanism, selected the appropriate route for data exchange based on residual energy, extracted residual energy of all nodes and evaluated it based on connectivity. Experiments showed that this protocol outperformed the existing methods in terms of production time, time slot, communication loss, first node failure, and residual energy [12].

Tan et al. raised a new fusion way of particle swarm optimization (PSO) algorithm and ant colony optimization (ACO) algorithm for the initial parameter selection problem of ACO algorithm. This method applied PSO algorithm to practice the original parameters of ACO algorithm, and then used ACO algorithm to calculate the optimal path. The experiment indicated that the average route length achieved by this way was 473.25mm lower than traditional algorithms, and the average iteration number of the improved method was 17 times [13]. Zheng et al. proposed a new improved ACO load balancing algorithm to achieve flexible control and management of network traffic. This algorithm designed evaluation methods for server modules and interlinkage modules, using the Kent chaos model to mess with the transition probability of ant colonies. Tests proved that this way could validly prevent the algorithm from falling into local optima, with fast convergence speed and achieving good global load balancing [14].

In summary, existing methods have explored the security protection of multi-hop networks and the integration of PSO and ACO algorithms from various aspects. However, existing methods have problems such as low accuracy in detecting irregular data in multi-hop networks, insufficient detection accuracy, and high operating costs. Therefore, a multi-hop network security protection method combining PSO algorithm and ACO algorithm was proposed. The innovative fusion algorithm optimized the penalty factor (PF) and kernel function (KF) of support vector machine (SVM), improved the PSO algorithm using inertia weight coefficient, and optimized the initiation function and pheromone update strategy of ACO algorithm. The improvement method aims to enhance the accuracy of anomaly data detection in multi-hop networks, reduce the probability of information exposure when nodes are attacked, and decrease operating costs. This research is separated into three sections. The first section combines PSO algorithm and ACO algorithm for multi-hop network anomaly detection. The second part estimates the behaviour of the fusion algorithm. The third part is a generalization of this research and expectations for further exploration targets.

Based on the above relevant studies, Table 1 is summarized, in which the research theme, main index methods, and shortcomings of relevant studies are summarized.

Table 1: Summary of relevant information of relevant studies

Docu	Research theme	Main index	Method	Insufficient
Document [7]	Solve the conspiracy attack	Throughput, power consumption, and latency	Quantum atoms search for relay nodes	High degree of complexity
Document [8]	Multi-hop network authentication	Authentication accuracy	End-to-end verification of channel characteristics	Rising network energy consumption
Document [9]	Wireless AD hoc network security	Transmission efficiency, energy	Two-way butterfly optimization algorithm	The recognition accuracy is low

		consumption and lifetime		
Document [10]	Data privacy capability	Information leakage probability	Multi-hop hybrid RF and free-space optics	The specific attack detection capability is insufficient
Document [11]	Multi-hop network security and energy consumption	Information exposure probability and energy consumption	Improved honey badger algorithm	The calculation time is long
Document [12]	Wireless network transmission efficiency	Power consumption and probability of communication loss	Next hop selection mechanism based on rank	Model running cost is high
Document [13]	ACO algorithm parameter selection	Average path length	The combination of PSO algorithm and ACO algorithm	The improved model is more complex
Document [14]	Flexible control of network traffic	Load balancing	Kent chaos model optimization transition probability	The detection accuracy of the improved method is low
This study	Security of multi-hop networks	Information exposure probability, detection accuracy and response time	Fusion of PSO algorithm and ACO algorithm	/

Based on the above related research, although the current research explores the security protection of multi-hop networks and the fusion of PSO algorithms and ACO algorithms from various aspects, the existing methods have the problems of lower accuracy in detecting anomalous data in multi-hop networks, insufficient detection accuracy, and higher operating costs. Therefore, the research innovatively adopts support vector machine for data classification, uses inertia weight coefficients to improve the PSO algorithm, optimizes the heuristic function and pheromone updating strategy of the ACO algorithm, and adopts the fusion algorithm to find the optimization of the penalty factor and kernel function of the support vector machine. It can reduce the probability of user privacy exposure and improve the response speed.

2 Methods and materials

2.1 Improved PSO algorithm based on SVM for Multi-hop network anomaly detection

When transmitting data in a multi-hop network, it needs to go through multiple intermediate nodes for forwarding, which gives attackers an opportunity. The traffic data passing through a running multi-hop network can be roughly divided into normal traffic data and abnormal behavior traffic data. Multi-hop network security detection essentially classifies the two types of data through a preset system. The research adopts the SVM algorithm, which is computationally simple, has fewer parameters, and has a faster learning speed, for multi-hop network anomaly detection. SVM can process both linear and nonlinear data simultaneously. When processing nonlinear data, high-dimensional mapping is required first to convert nonlinear data into linear data [15]. High dimensional mapping generates two parallel hyperplanes, and the larger the distance between the hyperplanes, the better the classification performance of SVM. The distance calculation of the hyperplane is shown in equation (1).

$$\begin{cases} \dfrac{2}{|\omega|} \\ \omega^T x + b = 0 \end{cases} \tag{1}$$

In equation (1), $\frac{2}{|\omega|}$ means the distance of the hyperplane, ω means the normal vector, T represents a point in the hyperplane, x represents the vector of that point, and b represents the set threshold. When partitioning difficult to segment linear data, relaxation variables and PFs are introduced to determine the constraint conditions of the hyperplane [16]. The constraint conditions are shown in equation (2).

$$\begin{cases} y_i\left(\omega^T \cdot x_i + b\right) \geq 1 - \xi \\ \min \dfrac{1}{2}\omega^T \omega + C\sum_{i=1}^{n} \xi_i \end{cases} \tag{2}$$

In equation (2), $y_i \in [-1,1]$, ξ represents the slack variable, C means the PF of the algorithm, and n represents the sample size. When misclassifications allowed by slack variables occur, the PF controls the degree of error occurrence. If the PF is large, SVM increases the penalty for misclassification to avoid misclassification. When the PF is small, the model sacrifices some class accuracy to improve generalization,

so it is essential to select the suitable PF grounded on various cases. In order to simplify the complexity of the algorithm, RBF with fewer parameter requirements is selected as the kernel function, and the calculation is shown in equation (3).

$$K\left(x_1, x_2\right) = \exp\left(-\gamma \left\| x_1 - x_2 \right\|^2\right) \tag{3}$$

In equation (3), $K(x_1, x_2)$ represents the RBF kernel function, γ represents the hyperparameters that determine the shape of the kernel function, x_1 represents the vector of point 1 on the hyperplane, and x_2 represents the vector of point 2 on the hyperplane. The anomaly detection process of multi-hop network based on SVM is shown in Figure 1.

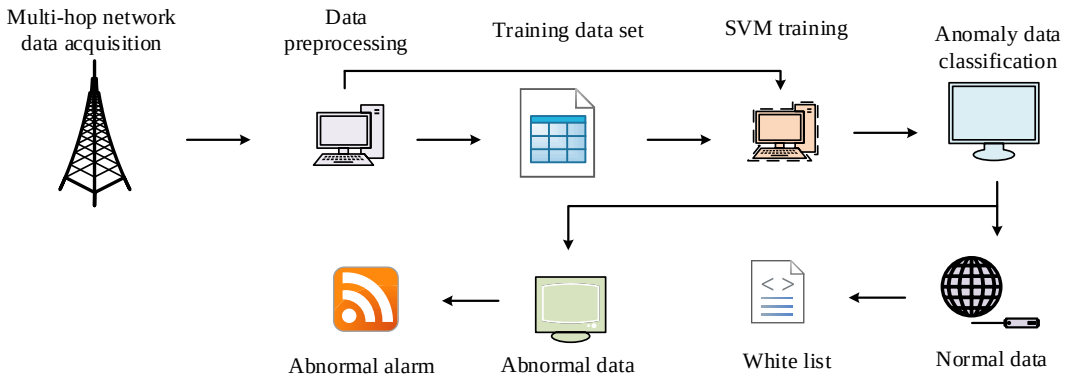


Figure 1: Multi-hop network anomaly detection flow based on SVM

In Figure 1, the data is first extracted from the multi-hop network, preprocessed, and then combined with the attack data into the training dataset. The training dataset is used to train an SVM, and the data to be detected is input into the SVM algorithm. Abnormal data is classified based on the decision function, with detected normal data being added to the whitelist. If abnormal data is detected, an alarm is issued. The study used PSO algorithm to reform the PF and KF size of SVM. On the basis of traditional PSO algorithm, inertia weight coefficients were added. By adjusting the size of inertia weight coefficients in real time, the initial global search capability and later local search accuracy of PSO algorithm were improved. A larger inertia weight is good for global search. It allows the particles to explore the solution space on a larger scale. This helps the algorithm to discover a wider range of potential solution regions at an early stage. A smaller inertia weight is more conducive to local search. It restricts the particle's motion. This allows the particles to focus more on refining the search in the current search region, and helps the algorithm to locally optimize the solution space at a later stage. The optimized particle update speed calculation is shown in equation (4).

$$v_{ij}(t+1) = \varepsilon v_{ij}(t) + c_1 k_1(t)\left[p_{ij}(t) - x_{ij}(t)\right] + c_2 k_2(t)\left[p_{ij}(t) - x_{ij}(t)\right] \tag{4}$$

In equation (4), ε represents the inertia weight coefficient, $v_{ij}(t+1)$ represents the particle's movement speed at time $(t+1)$, c_1 and c_2 represent learning factors, k_1 and k_2 are random numbers with values between 0 and 1, and $p_{ij}(t)$ represents the optimal position of the population at time t. There should be a certain difference in the values of learning factors c_1 and c_2 to further enhance population diversity. According to relevant research, the values of learning factors should be between 1 and 2.5. Linear changes should be made to the learning factors to improve individual information attention. The calculation is shown in equation (5).

$$c_1 = c_2 = \frac{c_{\max} - c_{\min}}{T} \cdot t + c_{\min} \tag{5}$$

In equation (5), $c_{\max}$ means the maximum value of the learning factor, $c_{\min}$ means the minimum value of the learning factor, t means the number of iterations at present, and T means the total amount of iterations. To further enhance the global search capability of the PSO algorithm, the size of the learning factor c_1 is adjusted to change in real-time with the rise of iteration times, as shown in equation (6).

$$c_1 = 1.3 + 1.2\cos\frac{t}{T}\pi \tag{6}$$

In equation (6), the value of c_1 is larger in the prophase of iteration and smaller in the later stage, showing a monotonically decreasing state. The calculation of c_2 is shown in equation (7).

$$c_2 = 2 - 1.2\cos\frac{t}{T}\pi \tag{7}$$

In equation (7), the value of c_2 is relatively small in the early stage of iteration and relatively large in the later stage, showing a monotonically increasing state. The operation of improving the PSO algorithm is represented in Figure 2.

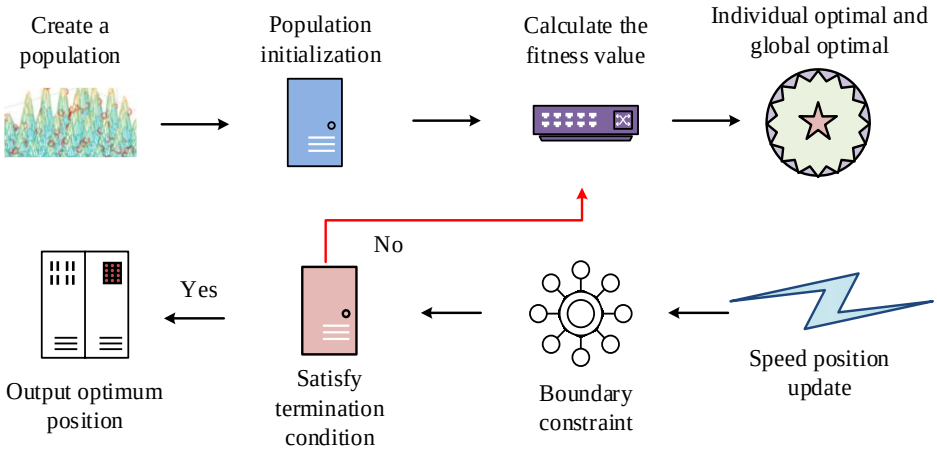


Figure 2: Operation flow of improved PSO Algorithm

In Figure 2, a particle population is created and the population is initialized. The initialization process includes random generation of particle positions, random assignment of initial number of particles and velocity, initialization of individual and global optimums, and setting of boundary constraints. The fitness value of each node is calculated, and the single best value of the node and the global best value of the population are calculated. The place and velocity of particles are updated and adjusted according to the set velocity and boundary constraints. It will be decided whether the termination condition is met or whether the iteration count has been reached. If it is met, the optimal individual is out put, otherwise the fitness is recalculated. Combining SVM and PSO, the classification accuracy capability of SVM is used to screen the fitness function of PSO and improve its fitness. The specific flow of PSO-SVM algorithm is represented in Figure 3.

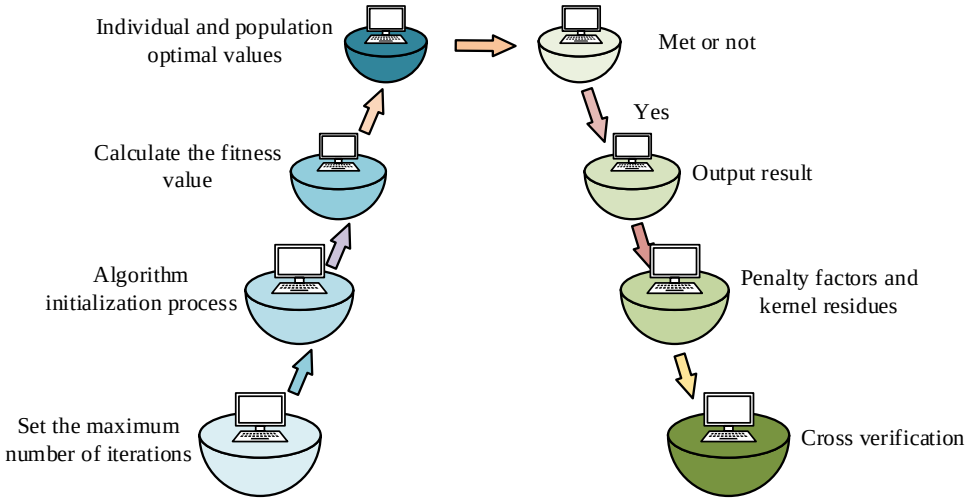


Figure 3: Specific Flow of PSO-SVM Algorithm

In Figure 3, the algorithm first optimizes the PF and KF hyperparameters, and then performs data detection and classification based on the optimal parameters to alert for irregular data. According to relevant research, the max value of iterations for PSO algorithm is defined to 100, the population is initialized, and the PF and KF hyperparameters are set to the particle component values. The fitness values of each particle in the population are computed, the optimal values of individuals and populations are updated, determining if the termination conditions are met, and the position and velocity of particles will be updated if they are met. The fitness value of the particles at the latest position is computed, the PF and hyperparameters are obtained, and cross validation is used to determine accuracy.

2.2 Optimization of multi-hop network security protection algorithm for ACO and PSO fusion

To further improve the optimization accuracy of the algorithm, the combination of PSO algorithm and ACO

algorithm is studied to enhance the detection capability of irregular data. ACO algorithm allows individuals to leave pheromones while searching for food, making it easier for subsequent individuals to follow up. The path with the highest concentration of pheromones is the optimal path. However, ACO algorithm is prone to encounter the traveling salesman problem during the optimization process, which is how to obtain the optimal path to access all nodes only once for each node. After accessing a node, an individual in the ant algorithm will store the node in memory to ensure that it will not be accessed repeatedly. After the individual completes the access, they will randomly select the next node. The probability calculation of an individual from node P to node Q is shown in equation (8).

$$Ch_{PQ} = \frac{\tau_{PQ}^{\alpha}(t')\eta_{PQ}^{\beta}(t')}{\sum \tau_{PM}^{\alpha}(t')\eta_{PM}^{\beta}(t')} \tag{8}$$

In equation (8), τ represents the initial pheromone, η represents the heuristic information, α means the information heuristic factor, β means the expected heuristic factor, t' represents the departure time, and M represents the remaining nodes available for selection.

$$\eta_{PQ}(t') = \frac{1}{d_{PQ}} \tag{9}$$

In equation (9), $\eta_{PQ}(t')$ means the heuristic function, which means the expected degree from point P to point Q, and d_{PQ} represents the range from point P to point Q. When the distance between nodes is shorter, the value of η increases, and the probability of ant colony individuals transferring to that node increases. The probability of subsequent individuals choosing this path also increases, and the residual pheromones continue to increase. When an individual completes the search for nodes near the node, residual pheromones will interfere with subsequent searches, so it is necessary to clean them up. The calculation is represented in equation (10) [17].

$$\tau_{PQ}(t'+1) = \rho\tau_{PQ}(t') + \Delta\tau_{PQ}(t') \tag{10}$$

In equation (10), ρ represents the residual factor, and $\Delta\tau_{PQ}(t')$ represents the total sum of residual pheromones from time t'.

$$\Delta\tau_{PQ}(t') = \sum {}^{n}\tau_{PQ}^{b}(t') \tag{11}$$

In equation (11), $\tau_{PQ}^{b}(t')$ represents the amount of pheromone released by ant colony individual b when passing between two cities. The heuristic function of the ordinary ACO algorithm is conversely proportional to the interval size between two nodes, resulting in low search efficiency. Therefore, the research has improved the heuristic function by adopting an adaptive mechanism to raise the optimization speed of ACO [18]. The new heuristic function adopts the relationship between the interval between the current point and the next point and the interval between the next point and the targetpoint, as calculated in equation (12).

$$\eta_{PQ} = \frac{\phi_{PQ}}{\lambda d_{PQ} + (1-\lambda d_{QD})} \tag{12}$$

In equation (12), ϕ represents the amplification function, d_{QD} means the interval between the next point and the target point, and λ means the adjustment balance factor with values between 0 and 1. The calculation of ϕ is shown in equation (13).

$$\phi_{PQ} = \frac{d_{\max} - d_{PQ}}{d_{\max} - d_{\min}} \tag{13}$$

In equation (13), $d_{\max}$ means the maximum interval between the current point and adjacent nodes, and $d_{\min}$ means the minimum interval between the current point and adjacent nodes. In the standard ACO algorithm, when an individual stumbles upon the optimal path close to the sub-optimal one, most individuals tend to follow the sub-optimal path more frequently, continuously depositing pheromones that mislead subsequent individuals. Therefore, studying pheromone update strategies for optimization allows only a subset of individuals to produce pheromones after discovering shorter paths [19]. These individuals are sorted according to the length of the searched path. Individuals with shorter paths are allowed to leave more pheromones, while those with shorter paths leave fewer pheromones. The calculation is represented in equation (14).

$$\tau_{PQ}(t'+1) = (1-\mu)\tau_{PQ}(t') + \mu\sum_{k=1}^{n'}\Delta\tau_{PQ} \tag{14}$$

In equation (14), μ represents the volatility coefficient and n' means the overall amount of ant colony individuals. The expression of $\Delta\tau_{PQ}$ is represented in equation (15) [20].

$$\Delta\tau_{PQ} = \frac{Q'}{L_{K'}}\left(1 - \frac{K'-1}{\varphi n'}\right) \tag{15}$$

In equation (15), K' represents the K' th individual, Q' represents the pheromone enhancement coefficient, $L_{K'}$ represents the length traveled by the

K' th individual, and φ represents the proportion of individuals that can leave pheromones in the total number of ant colonies. The specific operation process of improving the ACO algorithm is shown in Figure 4.

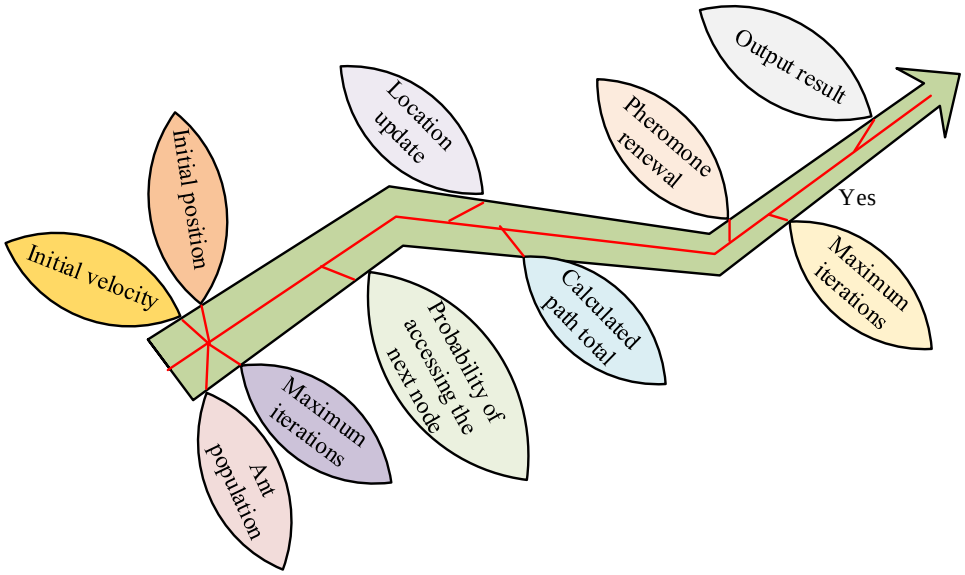


Figure 4: Specific operation flow of the improved ACO algorithm

In Figure 4, the initial population of ant colony is set, including the size of each parameter, maximum iteration times, etc., the possibility of individuals accessing the next node is estimated, their positions are updated, the length of the path traveled by each individual is calculated, and the optimal path is recorded. pheromones are updated in order of individual path length, determining if the max value of iterations is achieved, the calculation result will be output if yes, otherwise the second step will be repeated until the max value of iterations is achieved. PSO and ACO algorithms need to consider the order of fusion. Based on the advantages of each algorithm, PSO algorithm has fast global optimization speed and high accuracy in the prophase of iteration, while ACO algorithm has high local optimization precision in the anaphase of iteration, which can effectively avoid the generation of local optimal solutions [21-22]. Therefore, the fusion algorithm adopts PSO to accelerate the improvement of population diversity and optimization speed in the prophase of iteration, and ACO algorithm to raise optimization accuracy in the later stage of iteration. The specific operation process of the fused ACO-PSO algorithm is represented in Figure 5.

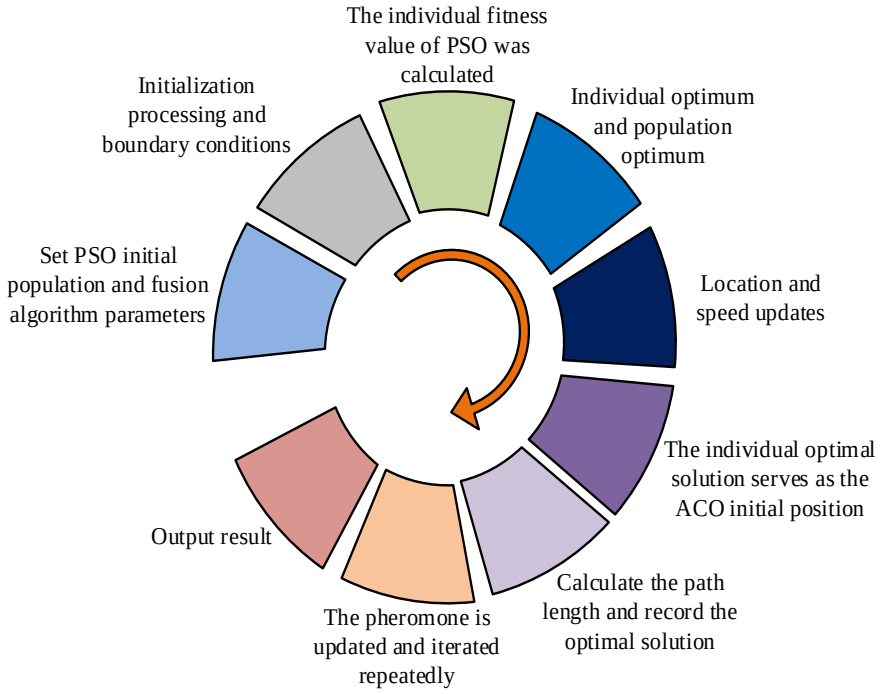


Figure 5: Specific operation flow of ACO-PSO algorithm

In Figure 5, the PSO algorithm population is to be set, population initialization processing is performed, various parameters of the fusion algorithm are set, and constraints are set, including maximum iteration times, PSO algorithm population boundaries, etc. The individual fitness value of PSO, the individual optimal value and population optimal value will be calculated. The individual position and velocity are updated, and it is determined whether the termination condition is met. If the condition is met, the current individual optimal solution will be used as the initial position of ACO, the path length traveled by the ant colony will be calculated, the current best solution will be recorded, and the pheromone will be updated in order of the individual path length. It will be determined whether the max value of iterations is achieved, and if so, the calculation result will be output. After the fusion algorithm is solved, the best PF and KF are input into SVM to classify the data of the multi-hop network, detect abnormal traffic data, and issue an alarm. SVM algorithm has good classification performance and can effectively differentiate network attacks, but the performance of SVM algorithm is greatly affected by the penalty factor and kernel function. Therefore, the study uses swarm intelligence algorithm to search for the best SVM parameters. According to the advantages of the two algorithms, the PSO algorithm is fast in global optimization in the early iteration period and has a wider search range, while the ACO algorithm has a higher accuracy in local optimization in the late iteration period, which is able to effectively avoid the generation of locally optimal solutions. The study adopts the fusion of the two algorithms to jointly search for the optimal parameters of the SVM algorithm and improve the classification performance. The pseudo-code of the ACO-PSO fusion algorithm is shown in Figure 6.

```
Algorithm: Hybrid ACO-PSO

Input: Problem space P, number of particles N, number of ants M,
parameters for ACO (e.g., pheromone evaporation rate rho, pheromone
influence alpha), parameters for PSO (e.g., cognitive component c1,
social component c2, inertia weight w), maximum iterations T

Output: Best solution found

1. Initialize the particle positions and velocities randomly within the
problem space P
2. Initialize the pheromone trails in the problem space P
3. Evaluate the fitness of each particle
4. For each iteration t = 1 to T do
   5. For each particle i = 1 to N do
      6. Update the pheromone trails based on the fitness of the
particles
      7. Use the updated pheromone trails to influence the velocity
update in PSO
      8. Update the velocity of particle i using the PSO velocity update
rule
      9. Update the position of particle i using the new velocity
     10. If the new position of particle i is better than its personal
best, update its personal best
     11. If the new position of particle i is better than the global
best, update the global best
     12. End For
    13. For each ant j = 1 to M do
      14. Construct a solution using the pheromone trails and heuristic
information
      15. Evaluate the fitness of the solution constructed by ant j
      16. If the solution is better than the current global best, update
the global best
      17. End For
    18. Apply pheromone evaporation to the trails
    19. Update the pheromone trails based on the quality of the solutions
found
    20. End For
21. Return the best solution found
```

Figure 6. Pseudo-code for the ACO-PSO Fusion algorithm

3 Results

3.1 Experimental analysis of SVM based improved PSO algorithm for multi-hop network anomaly detection

The hardware environment of the experiment was Inter Core i7-12600K, the base frequency was 3.7GHz, the GPU was GeForce GTX 3070, and the memory was 16GB. The experiment was conducted using MATLAB software for simulation testing, with a simulation area set within a range of 500m×500m, a node count of 600, a node communication radius of 15m, and 100 event packets. The experiment used deep recurrent neural network and region adaptive synthetic oversampling algorithm (DRRS), as well as Variational Autoencoder -

Generative Adversarial Network (VAE-GAN) for comparison. The experimental dataset consisted of UNSW_NB15 and Honeynet. Both datasets contain millions of pieces of cyberattack data, with the UNSW_NB15 dataset having a high level of diversity, encompassing a wide range of attacks such as DoS, PortScan, and DDoS, as well as being authentic, balanced, and providing clear labeling. The Honeynet dataset contains a wide range of attack types, as well as being collected through honeypots from global deployments. The Honeynet dataset encompasses a wide range of attack types as well as collects real-time attack data through honeypots from global deployments to accurately reflect current advanced cyber threats. Because of the dynamic update mechanism of the UNSW_NB15 dataset, it is more complex than the Honeynet dataset. The information exposure probabilities of different algorithms are shown in Figure 7.

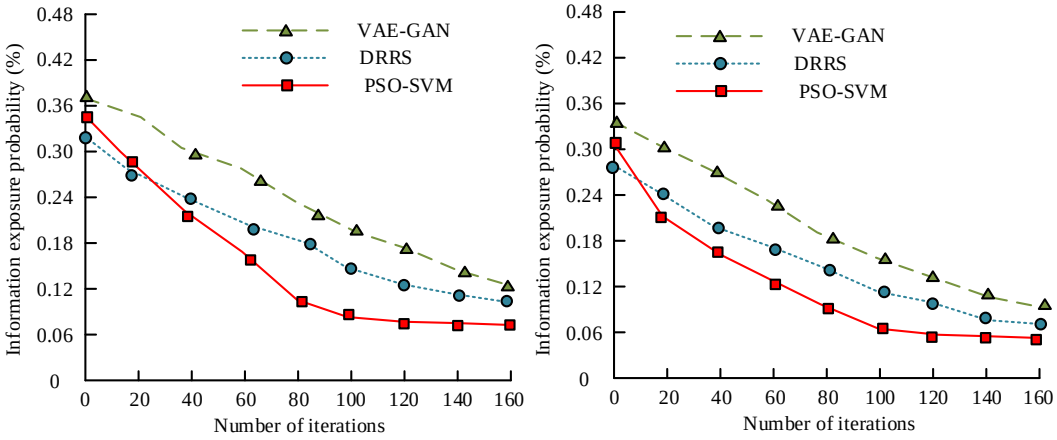


Figure 7: Information exposure probabilities of different algorithms

In Figure 7 (a), the relevant test data were averaged using multiple sets of data, and the *P* values between the test data of different algorithms were less than 0.05, which was statistically significant. The information exposure probability of PSO-SVM gradually decreased with the increase of iteration times, approaching convergence at around 100 iterations. The information exposure probability decreased from 0.35% to 0.10%, and the minimum information exposure probability was 0.06% and 0.04% lower than VAE-GAN and DRRS, respectively. In Figure 7 (b), the convergence of PSO-SVM remained unchanged because the complexity of the dataset decreased and the scale of abnormal information shrank. The minimum information exposure possibility of PSO-SVM was 0.06%, which was 0.08% and 0.05% lower than VAE-GAN and DRRS, respectively. The precision of anomaly recognition using different algorithms is shown in Figure 8.

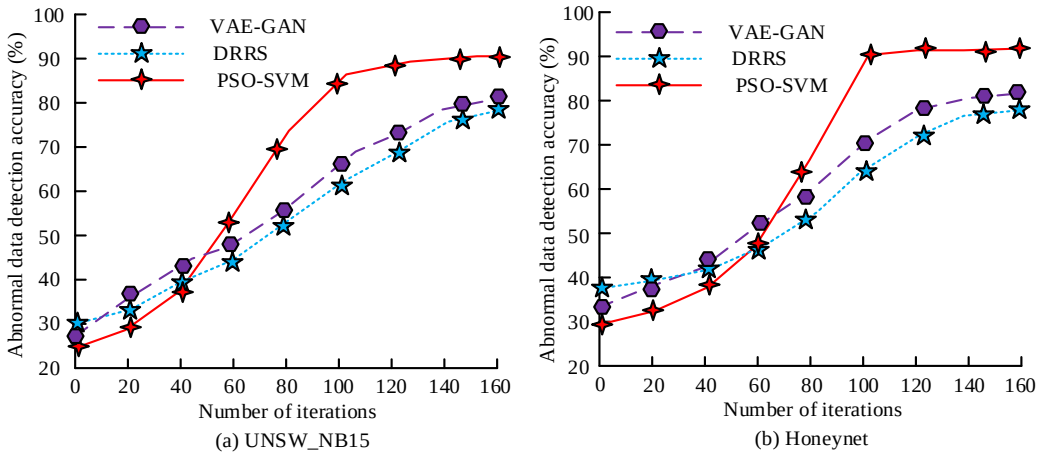
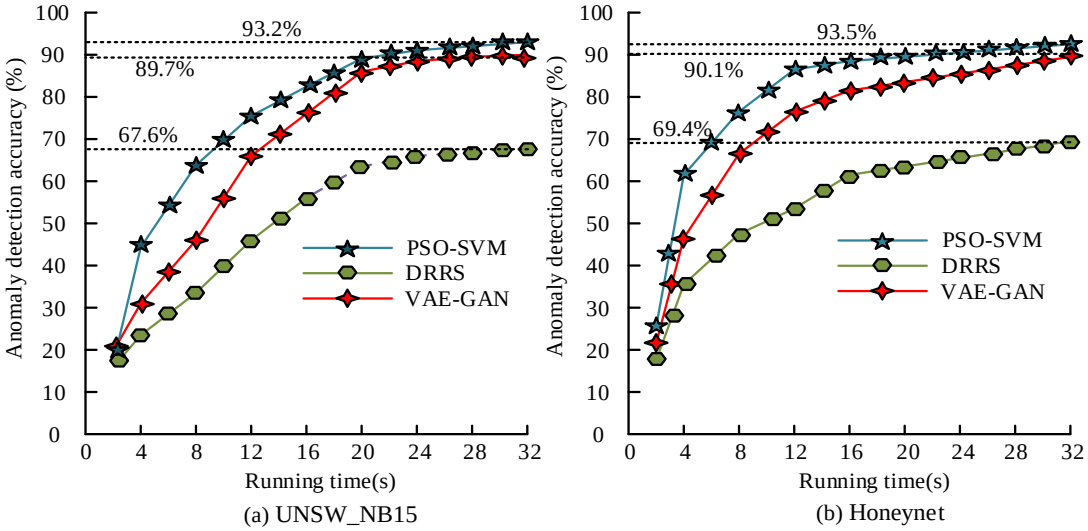


Figure 8: Anomaly detection accuracy of different algorithms

In Figure 8 (a), the convergence speed of PSO-SVM's anomaly detection accuracy was faster than the other two methods, with a maximum value of 89.6%, which was 9.4% and 11.2% higher than VAE-GAN and DRRS, respectively. In Figure 8 (b), the abnormal information detection accuracy of PSO-SVM approached convergence after about 100 iterations, with a maximum value of 93.5%, which was 11.3% and 13.8% higher than

VAE-GAN and DRRS, respectively. Because the Honeynet dataset is simpler than the UNSW_NB15 dataset and does not have dynamically updated network attack types, its anomaly detection accuracy was increased and convergence was closer. Detection accuracy can reflect the ability of the security system to identify threats, is a more intuitive indicator, the user can easily feel its effect, and it is important to reduce false alarms and omissions. The accuracy of anomaly detection using different algorithms is shown in Figure 9.



(a) UNSW_NB15 (b) Honeynet

Figure 9: Anomaly detection accuracy of different algorithms

In Figure 9 (a), the convergence speed of abnormal information detection accuracy of PSO-SVM was not significantly different from that of VAE-GAN and DRRS, with a maximum value of 93.2%, which was 3.5% and 27.6% higher than VAE-GAN and DRRS, respectively. In Figure 9 (b), due to the decrease in complexity of the dataset, the convergence speed of PSO-SVM's anomaly detection accuracy was 12 seconds and 20 seconds faster than VAE-GAN and DRRS, respectively. The maximum value was 93.5%, which was 3.4% and 24.1% higher than VAE-GAN and DRRS, respectively.

3.2 Experimental analysis of multi-hop network security protection algorithm for optimizing ACO and PSO fusion

The simulation software and basic parameters of the experiment were the same as before. By improving PSO on two datasets, the optimal PF and KF obtained were UNSW-NB15:236.35 and 2.19, and Honeynet: 27.63 and 4.07, respectively. The optimal PF and KF obtained by improving ACO-PSO in two datasets were UNSW-NB15:131.25 and 12.05, and Honeynet: 243.21 and 8.01, respectively. The response time in the experimental metrics is the time between the appearance of a network attack and the discovery of the attack by the security protection algorithm, the processing time is the time taken by the protection algorithm to resolve the network attack, and the root mean square error is the root mean square of the difference between the actual value and the predicted value during classification. The performance of different algorithms in performing multi-hop network anomaly detection is shown in Table 2.

Table 2: Multi-hop network anomaly detection performance of different algorithms

Algorithm	Data set	Response time(ms)	Disposal time(ms)	Root mean square error(ms)
DRRS	UNSW-NB15	71.8	125.1	6.7
	Honeynet	69.5	120.5	6.4
VAE-GAN	UNSW-NB15	42.3	95.3	3.6
	Honeynet	40.9	93.6	3.4
PSO-SVM	UNSW-NB15	46.7	98.7	4.1
	Honeynet	44.2	97.2	3.8
ACO-PSO-SVM	UNSW-NB15	22.4	72.6	1.3
	Honeynet	21.5	68.4	1.2
P-value	/	0.018	0.007	0.035

In Table 2, the p-value between the various data was less than 0.05, which was statistically significant. The performance of ACO-PSO-SVM is optimal in all aspects. In the more complex UNSW-NB15 dataset, the danger response time of ACO-PSO-SVM was 22.4ms, which was 24.3ms, 19.9ms, and 49.4ms faster than PSO-SVM,

VAE-GAN, and DRRS, respectively. The danger handling time of ACO-PSO-SVM was 26.1ms, 22.7ms, and 53.5ms faster than the other three algorithms, respectively. The root mean square error of ACO-PSO-SVM was 2.8ms, 2.3ms, and 5.4ms lower than the other three algorithms, separately. Reducing the dangerous response time and processing time of the algorithm can minimize the damage caused by cyber attacks. Responding to cyber security incidents and organizational counterattacks in a timely manner can effectively protect the user's personal privacy and sensitive information of the enterprise. Timely responses also enhance organizational resilience and maintain business continuity. The operating costs of multi-hop network anomaly detection using different algorithms are shown in Figure 10.

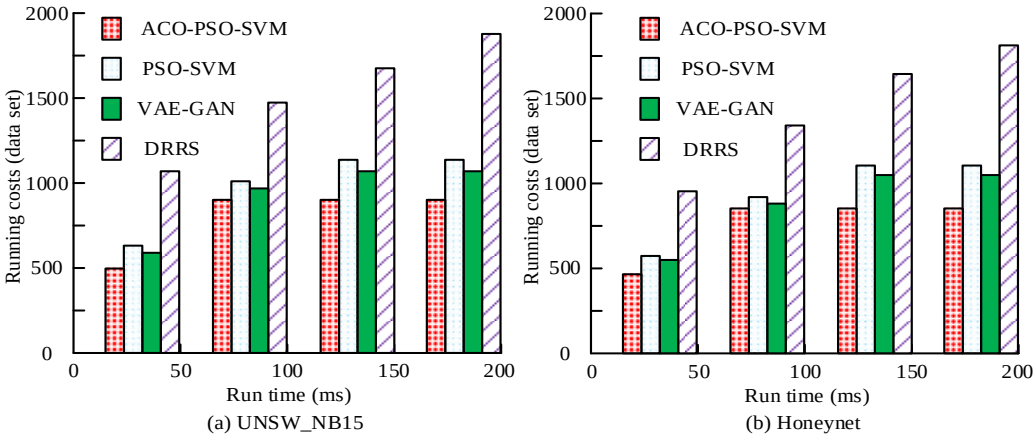


Figure 10: Comparison of operating costs of different algorithms

In Figure 10 (a), the multi-hop network anomaly detection cost of ACO-PSO-SVM was the lowest, reaching a maximum of 890 datasets at a running time of 100ms, which was 310, 210, and 910 datasets lower than PSO-SVM, VAE-GAN, and DRRS, respectively. In Figure 10 (b), the running cost of ACO-PSO-SVM reached its maximum value of 800 datasets at 100ms, which was 300, 240, and 950 datasets lower than the other three algorithms, separately. The accuracy comparison of multi-hop network anomaly detection using ACO-PSO fusion algorithm is shown in Figure 11.

In Figure 11 (a), due to the faster local optimization speed and higher precision of the ACO algorithm, the convergence curve of ACO-PSO-SVM was the same as that of PSO-SVM in the early stage of iteration, and the convergence speed was faster in the middle stage. The maximum detection accuracy was 92.5%, which was 2.9%, 12.3%, and 14.1% higher than that of PSO-SVM, VAE-GAN, and DRRS, separately. In Figure 11 (b), the maximum detection accuracy of ACO-PSO-SVM was 95.9%, which was 2.4%, 13.7%, and 16.2% higher than PSO-SVM, VAE-GAN, and DRRS, respectively. The convergence speed of the fusion algorithm was improved compared to Figure 11 (a). The comparison of PR and ROC curves for different algorithms is shown in Figure 12.

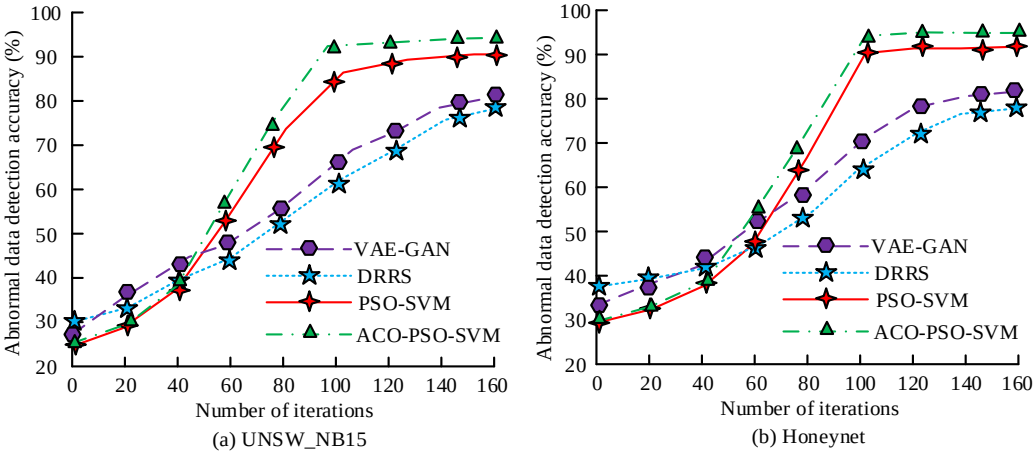
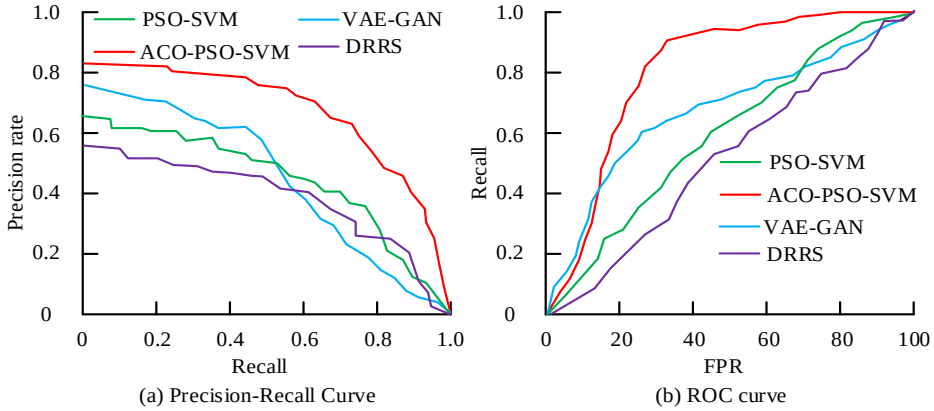


Figure 11: Comparison of Multi-hop network anomaly detection accuracy of ACO-PSO Fusion Algorithm



(a) Precision-Recall Curve (b) ROC curve

Figure 12. Comparison of PR Curve and ROC Curve of Different Algorithms

In Figure 12 (a), the PR curves of PSO-SVM, VAE-GAN and DRRS were intertwined with each other. To judge the performance of the algorithms, it is necessary to find the balance point and the point where the precision and recall are equal. At this point, the two performances of the classifiers were higher, which indicated that the classifiers performed well. The PR curve of ACO-PSO-SVM completely wrapped around the other three curves, indicating that the equilibrium point of the fusion algorithm was always above the equilibrium point of the other algorithms, so it can be concluded that the performance of ACO-PSO-SVM was better than the other three algorithms. In Figure 12 (b), the curve of ACO-PSO-SVM was steeper because the ideal target of the model was a true class rate of 1 and a false positive class rate of 0. The closer the curves of all algorithms are to the upper left corner, the better the performance of the algorithm. Sensitivity analysis was carried out on the individual proportion parameter of the ACO algorithm and the inertia weight parameter of the PSO algorithm, and the experimental results were shown in Table 3.

Table 3: Parameter sensitivity analysis of ACO and PSO Algorithms

Argument	Value	Precision rate	Recall rate	F1
φ	0.3	0.90	0.89	0.94
	0.4	0.92	0.94	0.98
	0.5	0.91	0.88	0.95
	0.6	0.87	0.84	0.91
ε	0.8	0.91	0.92	0.91
	0.9	0.92	0.94	0.98
	1.0	0.90	0.93	0.92

In Table 3, as the proportion of individuals leaving pheromones gradually increased, the performance of ACO algorithm increased first and then decreased. When the value was 0.4, the best performance was achieved, and the accuracy rate, recall rate, and F1 of the algorithm were 0.92, 0.94 and 0.98, respectively. As can be seen from the table, when the proportion increased, the recall rate of the algorithm could be greatly affected.

Table 4: Computational complexity of the proposed algorithm of the study compared to the base algorithm

Data set	Algorithm	Average processing time (ms)	Standard deviation (ms)	Time complexity $O(n^2)$ evaluation
Honeynet	SVM	20.4	1.8	Lower
	PSO	18.5	1.5	Lower
	ACO	29.8	2.4	Lower
	ACO-PSO-SVM	47.6	3.9	Lower
Maple-IDS	SVM	38.5	2.7	Lower
	PSO	29.2	2.5	Lower
	ACO	45.9	4.3	Lower
	ACO-PSO-SVM	72.4	6.2	Normal

When the proportion was 0.6, the recall rate of the algorithm was 0.10 lower than the optimal value. When the relation weight coefficient of PSO algorithm was 0.9, the best precision rate, recall rate and F1 values were obtained, and the maximum values were 0.92, 0.94 and 0.98 respectively. The computational complexity of the proposed algorithms studied against the base algorithm in datasets of different complexity levels is shown in Table 4.

In Table 4, the average processing times of the four algorithms when the dataset was simpler were 20.4ms, 18.5ms, 29.8ms, and 47.6ms, respectively, and the average processing time of the ACO-PSO-SVM algorithm was longer than the base algorithm, but it was still within the acceptable range, with a time complexity of lower. When the Maple-IDS dataset was used, the computation time of the four algorithms increased due to the fact that it contained a more number and variety

of attack data, the computation time of the different algorithms increased, and the four algorithms increased by 14.1ms, 10.7ms, 16.1ms, and 24.8ms, respectively, with the ACO-PSO-SVM algorithm increasing almost twice as much as the other algorithms, and the time complexity was normal.

4 Discussion

The study proposed a multi-hop network security protection strategy that integrates PSO algorithm and ACO algorithm, and applied it to experimental simulation analysis. The effectiveness and superiority of the strategy in multi-hop network security protection was verified by simulation analysis. Compared with the traditional method, the optimized ACO and PSO fusion algorithm had faster hazard response speed and operation efficiency, because the fusion algorithm adopted the PSO algorithm to improve the optimization speed and accuracy in global optimization, and adopted the ACO algorithm in local optimization to avoid local optimal solutions. Meanwhile, the fusion algorithm had lower detection cost and detection accuracy because the fusion algorithm can find the optimal penalty factor and kernel function of SVM. In multi-hop networks, faster convergence means that the network can quickly adapt and reconfigure routes in the event of failures or topology changes, which reduces service disruption time and improves the reliability and stability of the network. Reducing information exposure reduces the risk of network attacks, decreases the chance of sensitive data being stolen when nodes communicate, and protects user privacy and security. Reducing operational costs can enhance the competitiveness of the enterprise and customer satisfaction, while improving productivity. Multi-hop network security protection is widely used in military communications, disaster relief, mobile self-organizing networks, wireless sensor networks, and industrial network security, and plays an important role in a variety of scenarios through its rapid deployment, high flexibility, and high reliability.

5 Conclusion

A multi-hop network security protection algorithm that integrated ACO and PSO was proposed to address the issues of easy attacks on existing multi-hop network data forwarding at intermediate nodes and high data protection costs of existing methods. The experiment outcomes showed that the information exposure probability of PSO-SVM decreased from the initial 0.35% to 0.10%, and the minimum information exposure probability was 0.06% and 0.04% lower than that of VAE-GAN and DRRS, respectively. In datasets with lower complexity, the minimum information exposure probability of PSO-SVM was 0.06%, which was 0.08% and 0.05% lower than VAE-GAN and DRRS, respectively. The maximum accuracy of abnormal information detection for PSO-SVM was 89.6%, which was 9.4% and 11.2% higher than VAE-GAN and DRRS, respectively, and had a faster convergence speed. The maximum accuracy of abnormal information detection was 93.2%, which was 3.5% and 27.6% higher than VAE-GAN and DRRS, respectively. The hazard response time of ACO-PSO-SVM fusion was 22.4ms, which was 24.3ms, 19.9ms, and 49.4ms faster than PSO-SVM, VAE-GAN, and DRRS, respectively. The hazard handling time was 26.1ms, 22.7ms, and 53.5ms faster than the other three algorithms, and the root mean square error was 2.8ms, 2.3ms, and 5.4ms lower than the other three algorithms, separately. The multi-hop network anomaly detection cost of ACO-PSO-SVM was the lowest, with 310, 210, and 910 datasets lower than other methods, respectively. The maximum detection accuracy was 2.9%, 12.3%, and 14.1% higher than other methods, respectively. The PR curve of ACO-PSO-SVM completely wrapped around the other three curves, and the ROC curve was closer to the ideal target, so the performance of the fusion algorithm was better. Fusion algorithms could effectively achieve security protection for multi-hop networks, reduce the probability of user privacy data exposure, and lower algorithm operating costs. There were still some issues with this study, such as only focusing on algorithm optimization for security protection. In the future, data optimization can be considered to further raise the safety of multi-hop networks. For example, a stochastic gradient descent method is used to optimize the relevant dataset, which can be updated using a small number of samples, thus speeding up training and adapting to large-scale datasets. Deep learning methods are also able to be employed to learn the latest attack sample data in real time to improve the classification performance of the model. The ACO-PSO-SVM detection algorithm because of the fusion of multiple algorithms, resulting in a certain degree of increase in its computational complexity compared to ordinary classification algorithms. Meanwhile, its search efficiency decreases significantly when facing high-dimensional datasets, leading to a curse of dimensionality The fusion algorithm may not perform well when the dataset is noisy, and it cannot draw a clear hyperplane for accurate classification, so it cannot be detected between, and the data needs to be denoised.

References

[1] Wong AW, Goh SL, Hasan MK, Fattah S. Multi-hop and mesh for LoRa networks: Recent advancements, issues, and recommended applications. ACM Computing Surveys, 2024, 56(6):1-43. https://doi.org/10.1145/3638241

[2] Li X, Li Q, Zhang J. Research on global path planning of unmanned vehicles based on improved ACO algorithm in the complex road environment. Measurement and Control, 2022, 55(9-10):945-959. https://doi.org/10.1177/00202940221118132

[3] Pervaiz S, Bangyal WH, Ashraf A, Nisar K, Haque MR, Ibrahim A, Ag AB, Chowdhry B, Rasheed W, Rodrigues JJ. Comparative research directions of population initialization techniques using PSO

algorithm. Intelligent Automation & Soft Computing, 2022, 32(3):1427-1444. https://doi.org/10.32604/iasc.2022.017304

[4] Nasri M, Lamiri A, Maaref H, Mghaieth R. Adaptive dynamic multi-hop technique for clustering protocol in wireless sensor networks assisted-Internet of Things applications. IET Networks, 2022, 11(1):27-41. https://doi.org/10.1049/ntw2.12032

[5] Vinitha A, Rukmini MS. Secure and energy aware multi-hop routing protocol in WSN using Taylor-based hybrid optimization algorithm. Journal of King Saud University-Computer and Information Sciences, 2022, 34(5):1857-1868. https://doi.org/10.1016/j.jksuci.2019.11.009

[6] Shafique A, Asad M, Aslam M, Shaukat S, Cao G. Multi-hop similarity-based-clustering framework for IoT-Oriented Software-Defined wireless sensor networks. IET Wireless Sensor Systems, 2022, 12(2):67-80. https://doi.org/10.1049/wss2.12037

[7] Singh BK, Mahapatra SN, Kumar V. A secure multi-hop relay node selection scheme-based data transmission in wireless ad-hoc network via block chain. Multimedia Tools and Applications, 2022, 81(13):18343-18373. https://doi.org/10.1007/s11042-022-12283-7

[8] Ezzati Khatab Z, Mohammadi A, Pourahmadi V, Kuhestani A. A machine learning multi-hop physical layer authentication with hardware impairments. Wireless Networks, 2024, 30(3):1453-1464. https://doi.org/10.1007/s11276-023-03577-1

[9] Mahapatra SN, Singh BK, Kumar V. Secure energy aware routing protocol for trust management using enhanced Dempster Shafer evidence model in multi-hop UWAN. Wireless Networks, 2022, 28(7):3059-3076. https://doi.org/10.1007/s11276-022-03021-w

[10] Pattanayak DR, Dwivedi VK, Karwal V, Yadav PK, Singh G. Physical layer security analysis of multi-hop hybrid RF/FSO system in presence of multiple eavesdroppers. IEEE Photonics Journal, 2022, 14(6):1-2. https://doi.org/10.1109/jphot.2022.3226351

[11] Altuwairiqi M. An optimized multi-hop routing protocol for wireless sensor network using improved honey badger optimization algorithm for efficient and secure QoS. Computer Communications, 2024, 214(7), 244-259. https://doi.org/10.1016/j.comcom.2023.08.011

[12] Altowaijri S M. Efficient next-hop selection in multi-hop routing for IoT enabled wireless sensor networks. Future Internet, 2022, 14(2), 35-52. https://doi.org/10.3390/fi14020035

[13] Tan Y, Ouyang J, Zhang Z, Lao Y, Wen P. Path planning for spot welding robots based on improved ant colony algorithm. Robotica, 2023, 41(3):926-938. https://doi.org/10.1017/s026357472200114x

[14] Zheng H, Guo J, Zhou Q, Peng Y, Chen Y. Application of improved ant colony algorithm in load balancing of software-defined networks. The Journal of Supercomputing, 2023, 79(7):7438-7460.

[15] Choudhuri S, Adeniye S, Sen A. Distribution Alignment Using Complement Entropy Objective and Adaptive Consensus-Based Label Refinement for Partial Domain Adaptation[C]//Artificial Intelligence and Applications. 2023, 1(1): 43-51. https://doi.org/10.47852/bonviewaia2202524

[16] Yang L, Tao J, Liu YH, Xu Y, Su CY. Energy scheduling for DoS attack over multi-hop networks: Deep reinforcement learning approach. Neural Networks, 2023, 161(6):735-745. https://doi.org/10.1016/j.neunet.2023.02.028

[17] Zhai Z, Lai G, Cheng B, Qian J, Zhao L, Wu J, Wan Z. Lightweight secure detection service for malicious attacks in wsn with timestamp-based mac. IEEE Transactions on Network and Service Management, 2022, 19(4):5299-311. https://doi.org/10.1109/tnsm.2022.3194205

[18] Abdollahi M, Ashtari S, Abolhasan M, Shariati N, Lipman J, Jamalipour A, Ni W. Dynamic routing protocol selection in multi-hop device-to-device wireless networks. IEEE Transactions on Vehicular Technology, 2022, 71(8):8796-809. https://doi.org/10.1109/tvt.2022.3172923

[19] Fan Y, Gao S, Duan D, Cheng X, Yang L. Radar integrated MIMO communications for multi-hop V2V networking. IEEE Wireless Communications Letters, 2022, 12(2):307-11. https://doi.org/10.1109/lwc.2022.3224566

[20] Hanif M, Ashraf H, Jalil Z, Jhanjhi NZ, Humayun M, Saeed S, Almuhaideb AM. AI-based wormhole attack detection techniques in wireless sensor networks. Electronics, 2022, 11(15):2324-2335. https://doi.org/10.3390/electronics11152324

[21] Zhang, Z. (2024). SD-WSN Network Security Detection Methods for Online Network Education. Informatica, 48(21). https://doi.org/10.31449/inf.v48i21.6257

[22] Ahmed, S. M., & Mahmood, B. A. (2024). Cloud Computing Security: Assured Deletion. Informatica, 48(3). https://doi.org/10.31449/inf.v48i3.6245