Research on Trust Evaluation of Access Devices in Ship Ad Hoc Networks Based on Zero Trust

Henan Bu [1], Bo Liu [1], Menglong Wu [1], Zhuwen Yan [2]

[1] *School of Mechanical Engineering, Jiangsu University of Science and Technology, Zhenjiang*
[2] *School of Mechanical Engineering, Nanjing Institute of Technology, Nanjing*

***Abstract* – In Ship Ad Hoc Networks, the dynamic topology and the frequent access and departure in the open environment make the trusted interaction between nodes a key issue. Traditional trust evaluation models often overlook network dynamics and the comprehensive mining of behavioral and historical data, leading to insufficient evaluation accuracy. To address this, this paper proposes a comprehensive trust evaluation model for access devices in Ship Ad Hoc Networks under a Zero Trust architecture. The model integrates direct trust based on behavioral evidence and indirect trust based on historical interactions. In direct trust evaluation, the fuzzy analytic hierarchy process and an improved artificial bee colony algorithm-optimized random forest model are combined to calculate subjective and objective weights, respectively, with optimal weight allocation achieved through the distance function method. Meanwhile, indirect trust evaluation enhances the weight of recent data and improves the timeliness and credibility of evaluation results by designing a time window mechanism and introducing a time decay factor. Experimental results demonstrate that the proposed model effectively improves trust evaluation accuracy. Additionally, it outperforms existing methods in terms of accuracy and detection rate under different malicious device proportions, significantly enhancing the dynamic adaptability and reliability of trust evaluation.**

DOI: 10.18421/TEM153-20
https://doi.org/10.18421/TEM153-20

Corresponding author: Henan Bu,
School of Mechanical Engineering, Jiangsu University of Science and Technology, Zhenjiang
Email: buhn_just_edu@163.com

Received: 16 July 2025.
Revised: 17 January 2026.
Accepted: 31 January 2026.
Published: 27 August 2026.

***Keywords* – Ship Ad Hoc Networks, access devices, Zero Trust, Random Forest, trust evaluation.**

1. Introduction

With the rapid development of the modern ship industry and the waterborne shipping industry, the scale of global maritime transportation has been expanding and the number of ships is increasing rapidly, and about 90% of international trade is transported by sea [1]. However, the maritime environment is complex and changeable, and ships may face various emergencies and contingencies during long-distance voyages [2], so efficient and safe maritime ship transportation communication is particularly important. The complexity and uncertainty of the maritime communications environment will result in conventional communications systems often facing problems such as signal attenuation, transmission delays, and frequent interruptions, making it difficult to effectively support emergency response to emergencies. Therefore, to more effectively respond to maritime emergencies and promote the development of maritime transportation, national maritime security capacity, and the modernization process of comprehensive maritime governance, it is crucial to build a stable, reliable, and highly secure emergency communication network [3].

As an integration of mobile communication and computer networks, ad hoc network features highly flexible devices and powerful communication system capabilities. With their rapid deployment capability and high-reliability support, they demonstrate extensive application potential in emergency communications, monitoring, command and dispatch, and other fields. They can be flexibly adjusted according to different application scenarios, making them suitable for the needs of fixed and mobile platforms such as drones, vehicles, ships, and other unmanned devices [4]. In ad hoc network applications, the authors [5] proposed a UAV base-station aerial networking scheme to enhance wireless communication coverage and service quality in disaster scenarios.

In study [6], a multi-hop ad hoc network using multiple UAVs to provide communication services for disaster-stricken areas was presented. Study [7] proposed a carrier strike group communication networking model, in which ships, buoys, lighthouses, and coastal terrestrial networks are integrated to form a unified communication network. Existing research indicates that although various communication networking methods derived from ad hoc networks can provide stable technical support in complex environments such as disaster rescue and dynamic scheduling command scenarios, significantly enhancing the success rate of various operations, their security protection remains a critical issue that urgently needs to be addressed.

The openness of the Ship Ad Hoc Networks allows new devices to be accessed and serviced at any time, greatly enhancing the communication capabilities between ships. However, with the increase in the degree of networking and the dynamic topology and openness of Ship Ad Hoc Network access devices frequently joining or leaving, the Ship Ad Hoc Network emergency communication network is also facing more and more serious network security threats [8], which requires the adoption of effective measures to safeguard the security of Ship Ad Hoc Network communication. The Zero Trust concept provides a new approach for rebuilding network security architecture [9]. It breaks away from traditional network security boundary designs and follows the principle of "never trust, always verify." Centered around identity authentication, continuous trust evaluation, and dynamic access control, it ensures the allocation of minimum privileges, thereby safeguarding the security of ad hoc network communication links. To apply the Zero Trust model, scholars both domestically and internationally have conducted related research. An edge-based Zero Trust model was proposed in which real-time dynamic trust evaluation is used to detect anomalous behavior of compromised terminals, enabling rapid decay of trust values [10]. A Zero Trust security protection technique for the power Internet of Things is presented in [11] by constructing a data protection architecture covering the device layer, data layer, and service layer.

The implementation of a Zero Trust architecture for Internet scenarios is described in [12], which effectively protects network communications and service access.

Trust evaluation is an essential part of the zero-trust architecture to ensure the security of the main body of the access device.

The trust evaluation engine evaluates the trustworthiness of the access device and at the same time provides the trust evaluation value to the access control engine to realize the least privilege authorization. Both domestic and foreign countries have also achieved better research results in trust evaluation models and applications. The paper [13] presented a model that combines Zero Trust with an access control framework, in which trust evaluation is incorporated into the access control process to better reflect user intentions. A Zero Trust-based access control model is developed in [14] to achieve fine-grained access control for power grid cloud services through rule matching and behavior analysis based on variational autoencoders. The work in [15] proposed a distributed authentication model that pushes trust evaluation and terminal authentication in the Zero Trust security architecture down to edge devices.

In [16], a security authentication method incorporating both direct trust evaluation and indirect trust evaluation is proposed, effectively addressing the security issues of new vehicular nodes joining the network. Study [17] established a trust evaluation mechanism model for IoT edge devices that combines identity authentication, direct trust, and indirect trust. Although the above studies have achieved promising results and provided a solid theoretical foundation for the establishment of trust evaluation models, existing trust evaluation models still suffer from issues such as poor dynamic adaptability, difficulty in real-time evaluation, and limited evaluation dimensions.

Given the lack of reports on security protection in Ship Ad Hoc Networks, this paper focuses on Ship Ad Hoc Network access devices as the research object. By introducing the Zero Trust concept, a comprehensive trust evaluation model is constructed under the Zero Trust architecture, incorporating direct trust based on behavioral evidence and indirect trust based on historical data, with continuous trust evaluation to validate the security of the subject. Existing direct trust evaluations primarily rely on subjective weighting for trust evaluation of behavioral evidence, while this paper introduces objective weighting to reduce the impact of subjective judgment, thereby improving the accuracy of trust evaluation. Furthermore, this paper optimizes the indirect trust evaluation process by introducing a time decay factor, thereby improving the accuracy and timeliness of the indirect trust evaluation. This paper integrates direct and indirect evaluations to provide more precise trust evaluation results for dynamic authorization in Ship Ad Hoc Networks, thereby enabling fine-grained dynamic authorization and ensuring the security of Ship Ad Hoc Network links.

2. Security Protection Design of Ship Ad Hoc Network

Ship Ad Hoc Networks operate in open and highly dynamic maritime environments, where communication security faces challenges such as frequent topology changes, heterogeneous devices, and potential internal threats. To address these challenges, this section focuses on the security protection design for Ship Ad Hoc Networks. The overall network structure and the application of Zero Trust-based security mechanisms are presented to provide a secure foundation for subsequent trust evaluation.

2.1. Ship Ad Hoc Network Structure

To support reliable communication in maritime emergency and dynamic sea environments, it is essential to understand the fundamental structure of Ship Ad Hoc Networks. This subsection introduces the overall architecture of ship-based ad hoc networks, including node composition, communication links, and network organization. These structural characteristics form the basis for subsequent discussions on security mechanisms.

2.1.1. Analysis of Ship Ad Hoc Network Structure

Flat structure: The topology of the ad hoc networks is generally divided into two types: flat structure and hierarchical structure [18]. Therefore, the flat structure and hierarchical structure can serve as the main forms of the ship's ad hoc network structure. Ship Ad Hoc Networks flat structure in which all nodes have equal status and there is no central control node, and information transmission relies on a multi-hop forwarding mechanism. This topology is simple, easy to implement and maintain, and is suitable for small-scale network environments.

Ship Ad Hoc Networks with flat structure is suitable for ships in special sea areas far away from coasts and waterways, such as ocean transportation, distant naval missions, and emergency rescue. There are many paths between nodes in this network topology, and ship nodes in the network can communicate with any node in the network as needed, and local failures do not affect the entire network. Due to the lack of central node control in the flat structure network, all nodes are equal in status [19]. When a new ship node joins, it can discover one or more nearby neighboring nodes and establish a direct communication link with them, thus becoming part of the topology, as shown in Figure 1.

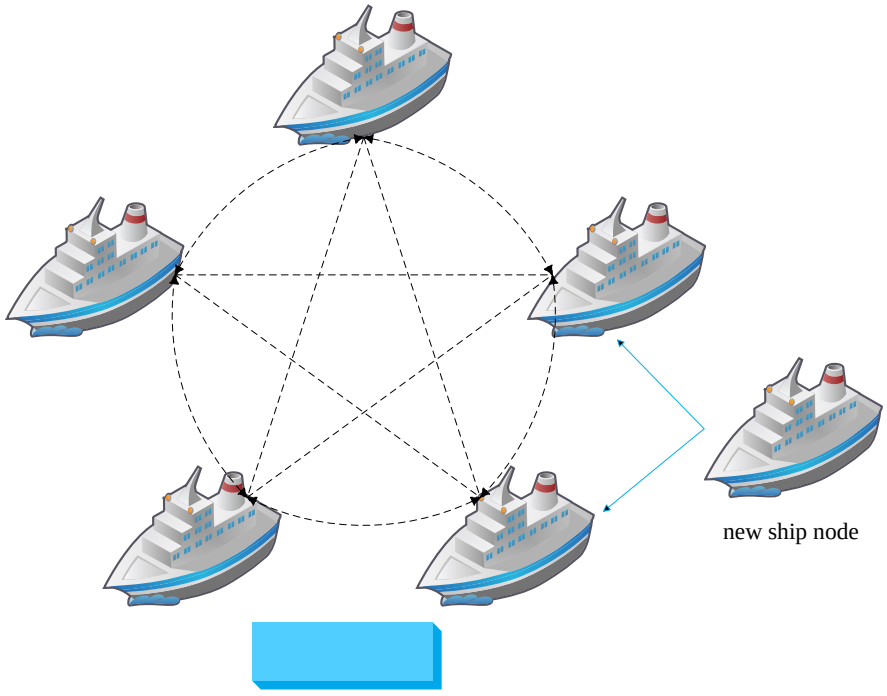


Figure 1. Flat structure of Ship Ad Hoc Network

Under this structure, communication problems such as high communication demand, high communication quality, and strict requirements on time delay can be effectively solved for ships [20].

Ships can communicate directly with any node in the network, and ships can interact with each other, which improves the level of resource sharing, reduces the cost of information interaction, and is conducive to improving the level of interaction between ships.

Hierarchical structure: In the hierarchical structure of a Ship Ad Hoc Network, the network is divided into multiple clusters, each managed by a cluster head. The cluster heads then form a higher-level backbone network, as shown in Figure 2. This structure effectively reduces the complexity of the routing algorithm and improves the scalability and stability of the network [21].

The hierarchical structure of Ship Ad Hoc Networks is suitable for coastal areas, shorelines, and special maritime regions such as water traffic management, coastal patrol, law enforcement, and emergency response and rescue operations.

This hierarchical structure selects nodes with stronger communication capabilities as cluster heads, which are responsible for managing intra-cluster nodes and maintaining cluster stability. Cluster heads communicate through loop connections, enabling direct communication between cluster headships, while intra-cluster members communicate only with their respective cluster headships. Unlike the planar structure, new access device nodes or ship nodes attempt to discover nearby cluster head nodes for connection rather than directly connecting with ordinary nodes.

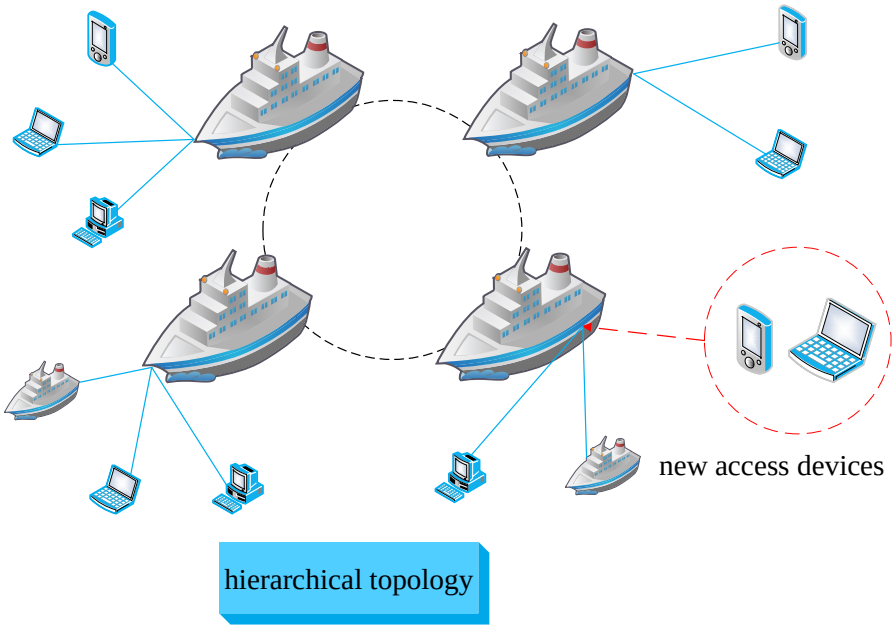


Figure 2. Hierarchical structure of Ship Ad Hoc Network

The greatest advantage of the hierarchical structure is its excellent scalability, unrestricted network size, small routing, and control overhead, easy-to-realize mobile management of ships, and local synchronization of the network, so it largely improves the network performance of Ship Ad Hoc Networks [22].

2.1.2. Analysis of Security Threats to Ship Ad Hoc Networks

Ship Ad Hoc Networks can access new devices and provide services at any time, thus significantly improving the communication capability between ships. However, the independence of nodes in a Ship Ad Hoc Network and the traditional static configuration protection means is difficult to meet the dynamic characteristics of the frequent joining and leaving of devices [23].

Moreover, the nodes in the ad hoc network of the Ship Ad Hoc Network have dual responsibilities as terminals and routers, with limited memory and computational power, resulting in the emergency communication network of the Ship Ad Hoc Network also facing serious network security threats. Therefore, it is essential to introduce a flexible security protection mechanism that adapts to dynamic topology changes.

The traditional security protection mechanisms for ad hoc networks mainly include two types, one is security attack defense [24], which is the first line of defense against external attacks using encryption, but internal attackers can take it down from the inside. The second is security attack detection and mitigation, The intrusion detection system as the second line of defense against security attacks, which aims to detect and stop abnormal activities in the network in time before they damage the communication network [25].

2.2. Zero Trust-Based Security Protection for Ship Ad Hoc Networks

Due to the open communication environment and highly dynamic topology of Ship Ad Hoc Networks, traditional perimeter-based security mechanisms are often insufficient to address evolving security threats. Zero Trust security, which emphasizes continuous authentication, authorization, and trust evaluation, provides a promising approach for securing such networks. This subsection introduces the application of Zero Trust principles in Ship Ad Hoc Networks and outlines the key security protection mechanisms that support secure and reliable maritime communications.

2.2.1. Zero Trust and Zero Trust Architecture

Ship Ad Hoc Network is applied with the characteristics of ad hoc network open peer-to-peer network architecture without clear boundaries and limited computation, storage, and energy of the nodes [26], which makes the traditional ad hoc network security protection mechanism limited.

Zero-trust breaks the traditional network security boundary design idea, abandons the network-centered security system, reconstructs the identity-centered new security architecture, follows the concept of "never trust, continuous verification", continuously verifies the identity of the subject, checks the legitimacy of the device and evaluates the authority of the subject of access.

The description given by NIST in the Zero Trust Architecture [27] standard is that Zero Trust architecture provides a set of concepts, ideas, and component relationships for removing uncertainty from the process of making precise access decisions about information systems and services. That is, the zero-trust architecture helps to identify the core elements and major functional components of zero trust, and completes the transformation from abstract ideas to concrete components to guide the unfolding of the implementation. The core logical components of the zero-trust architecture are shown in Figure 3.

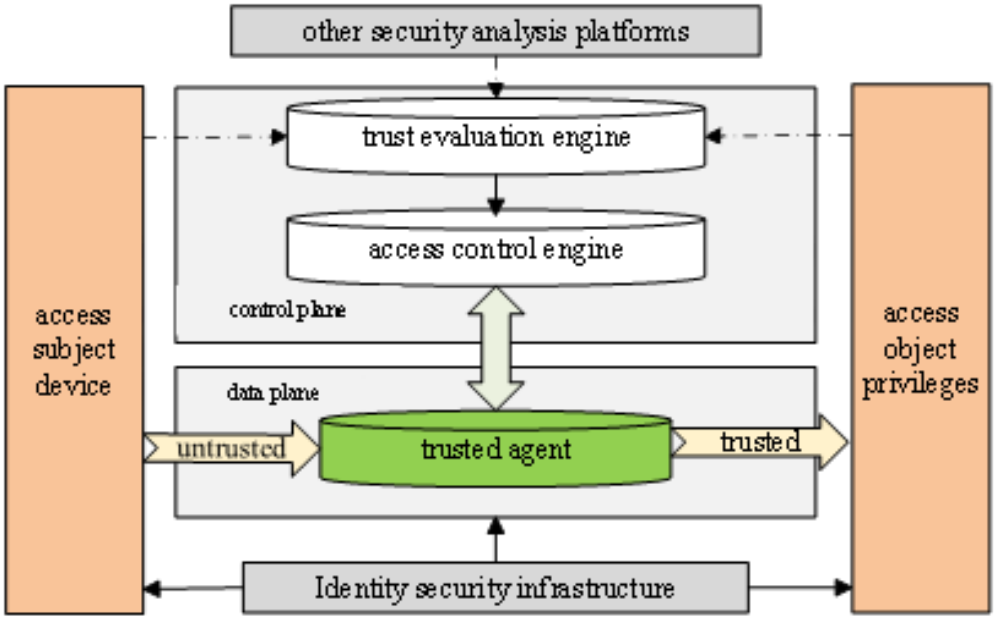


Figure 3. Zero Trust Architecture core logic components

2.2.2. Zero Trust Protection for Ship Ad Hoc Network Access Devices

The Zero Trust architecture breaks the traditional authentication-as-trust, boundary protection, static access control, network-centric, and other protection ideas, with authentication as the cornerstone, continuous trust assessment, minimum privilege allocation, and dynamic access control, to establish an advanced network security framework in different application scenarios with different ways of implementation [28].

Ship Ad Hoc Networks have the dynamic characteristics of frequent access or departure of device nodes and no clear network boundaries, this paper takes the Ship Ad Hoc Networks access device as the research object, introduces the concept of zero-trust with end-to-end security protection as the core, and implements the zero-trust security in the ad hoc network access device as shown in Figure 4.

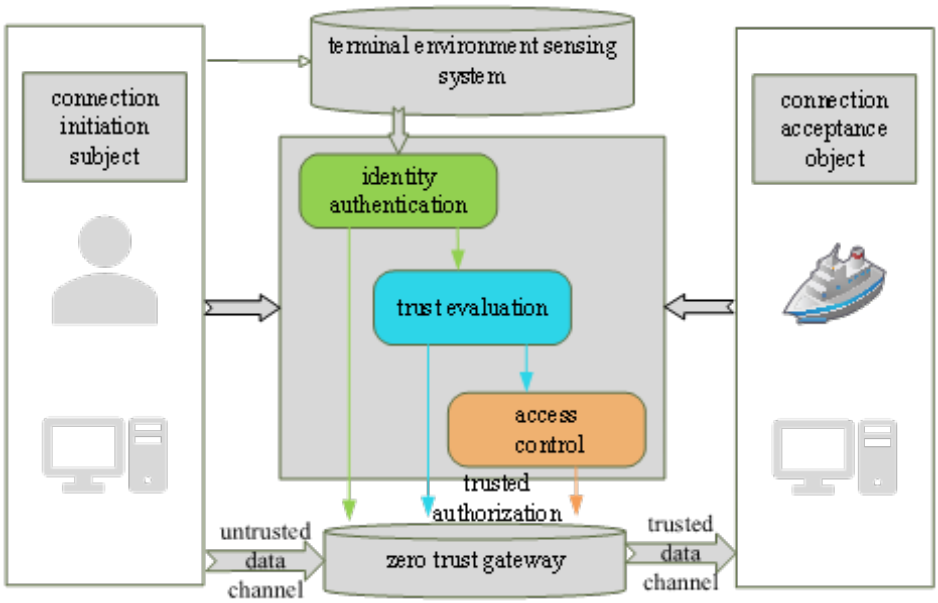


Figure 4. Zero Trust security protection system

Before accessing a device to a Ship Ad Hoc Network to become a trusted node, in addition to completing the integrity identity authentication, the access behavior of the access device node needs to be assessed for trust, identity authentication, and trust assessment. After passing, it will get certain authority and establish communication links with the ad hoc network, and the access device will also monitor its behavior and continuously trust assessment after establishing a connection, and at the same time, combine with the access control model to realize fine-grained dynamic authorization to guarantee the overall link security, to achieve the whole network real-time, dynamic and trustworthy.

3. Analysis and Computation of Trust Evaluation Models

In Zero Trust–based Ship Ad Hoc Networks, security decisions rely on continuous and quantitative trust assessment rather than static credentials. To enable fine-grained access control and dynamic authorization, it is necessary to establish a systematic trust evaluation model and corresponding computation methods. This section analyzes the key components of trust evaluation in Ship Ad Hoc Networks and presents the computational models used to derive node trust values.

3.1. Model Establishment

The trust evaluation model constructs a comprehensive trust evaluation framework from the perspectives of behavioral evidence and historical interaction data of ship access devices, as shown in Figure 5. The entire comprehensive trust evaluation model includes direct trust evaluation based on behavioral evidence and indirect trust evaluation based on historical interaction data. In the direct trust evaluation process, first, the fuzzy analytic hierarchy process (FAHP) is used to calculate the subjective weights. Second, to reduce inaccuracies caused by subjectivity, this paper introduces random forest (RF) to calculate objective weights based on the existing subjective weight calculation, optimizing the hyperparameters through the improved artificial bee colony algorithm (SABC) and using out-of-bag (OOB) error to compute the objective weights. Then, the combination weights are calculated using the distance function method. Finally, the direct trust evaluation value is obtained by multiplying the processed behavioral evidence vector with the combination weight vector. For indirect trust evaluation, a time window mechanism based on historical data is designed to select recent data with a reference value, and a time-based exponential decay factor is introduced to enhance the weight of recent data, thereby determining the indirect trust evaluation value.

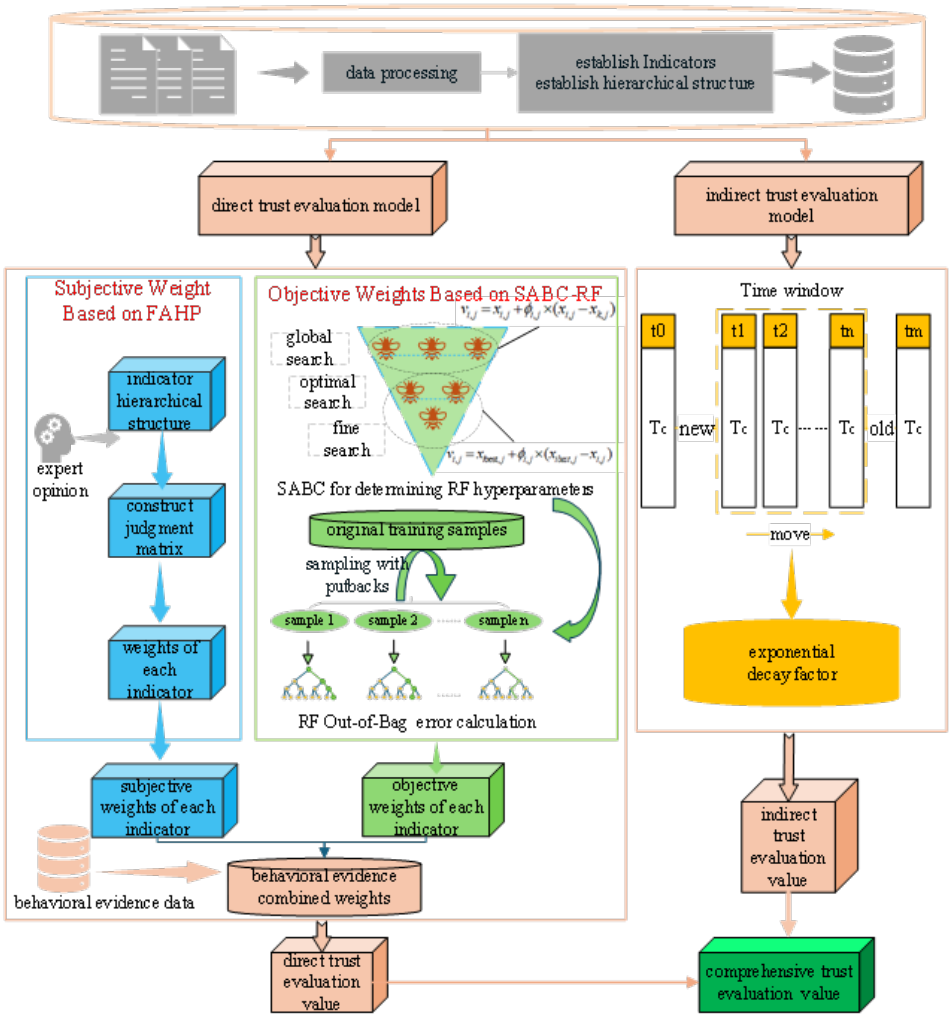


Figure 5. Model establishment

3.2. Direct Trust Evaluation Based on Behavioral Evidence of Ship Ad Hoc Network Access Devices

Direct trust reflects the trustworthiness of access devices derived from their observed behaviors during network interactions. In Ship Ad Hoc Networks, access devices exhibit dynamic and heterogeneous behavior patterns, which can directly indicate their reliability and security status. This subsection focuses on direct trust evaluation based on behavioral evidence and describes how device behaviors are analyzed to compute direct trust values.

3.2.1. Subjective Weights Based on FAHP

The FAHP used in this paper can refine the fuzzy uncertainty assessment problem of Ship Ad Hoc Networks access devices into simple trust evidence weighted sum problem while avoiding consistency tests in terms of process [29].

1. Establishment of Access Device Behavior Hierarchy: To address the diverse trusted service requirements of maritime Ship Ad Hoc Network access devices, a multidimensional identity processing approach is adopted. Through a hierarchical structure model, the trust of access devices is decomposed step by step, breaking down the broad and abstract concept of Ship Ad Hoc Network access devices trust into intuitive and specific indicators [30]. The indicators for each tier of the ship access devices were determined based on expert opinion and research as shown in Figure 6.

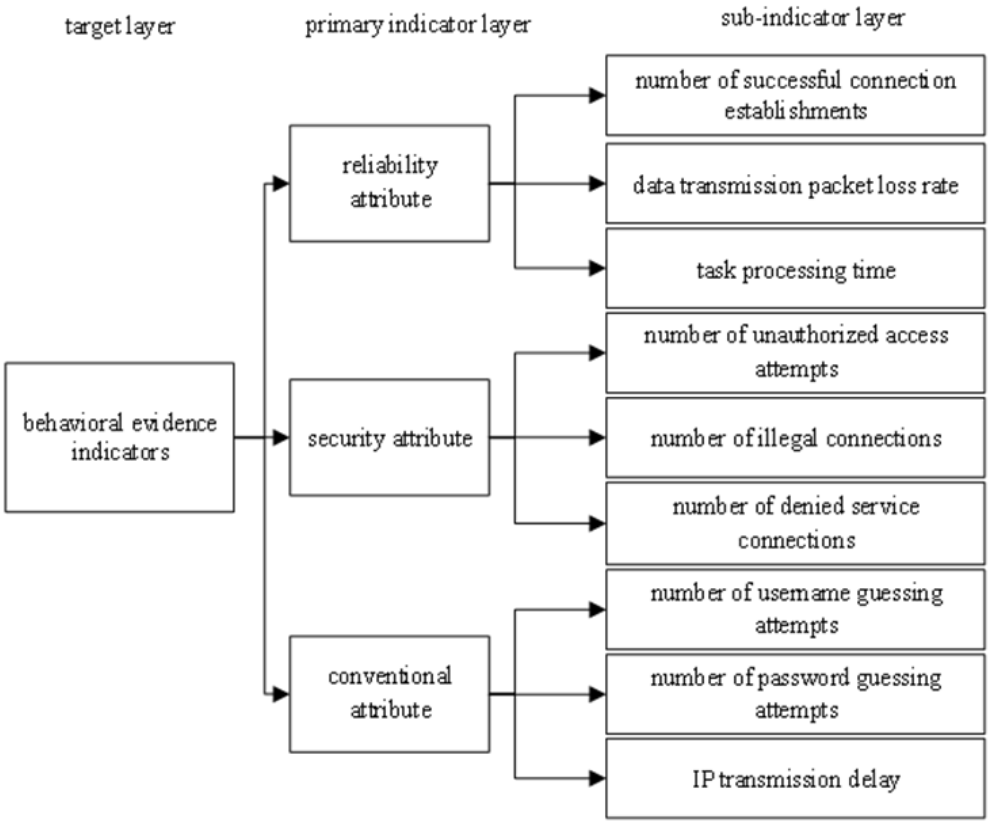


Figure 6. Behavioral evidence hierarchy

2. Establishment of Fuzzy Judgment Matrix: Analyzing the importance of behavioral evidence of Ship Ad Hoc Network access device based on expert opinions, and constructing a fuzzy judgment matrix by the 0.1-0.9 scale method. If there are n behavioral evidences, P1, P2, ..., Pn, these n behavioral evidences are compared two by two to get the n-order fuzzy judgment matrix:

$$P = \begin{bmatrix} P_{11} & \cdots & P_{1n} \\ \vdots & \ddots & \vdots \\ P_{n1} & \cdots & P_{nn} \end{bmatrix} \quad (1)$$

3. Establishment of Fuzzy Consistency Matrix: Calculates the sum of the elements of each row in the judgment matrix P: $r_i = \sum_{j=1}^{n} P_{ij}$; Through mathematical transformations: $r_{ij} = (r_i - r_j)/2(n - 1) = 0.5$; The fuzzy consistency matrix is obtained as follows: $R = (r_{ij})_{\circ}$

4. Calculation of the Subjective Weight Vector for Indicators: Calculate the weight of each metric for the Ship Ad Hoc Networks access device $W = 1/n - 1/2\alpha + 1/\alpha n \times \sum_{j=1}^{n} r_{ij}$; Collated to obtain subjective weights for evidence indicators for Ship Ad Hoc Network access device:

$$W_s = [W_1, W_2, W_3, \cdots, W_n]^T \quad (2)$$

3.2.2. Objective Weights Based on SABC-RF

Objective Weight Calculation By RF: The RF model can handle both continuous and categorical variables and has the advantages of better tolerance of outliers and noise and higher prediction accuracy, which can be used to obtain better objective weights for indicators [31]. In this paper, the RF is applied to assess the significance of behavioral evidence of access devices for Ship Ad Hoc Networks to accurately identify behavioral evidence that has a critical impact on security and to improve the reliability of trust assessment. The model constructs multiple decision trees using bootstrap sampling and evaluates the prediction error rate with the out-of-sample data. The larger the out-of-bag error, the more important the feature is, and the importance of the behavioral evidence is assessed by calculating the increase in the out-of-bag error corresponding to each Ship Ad Hoc Network access device behavioral evidence, and finally the importance of each behavioral evidence is normalized to obtain the objective weights.

(1) Construct Out-of-Bag (OOB) Data: Constructing Out-Of-Bag (OOB) datasets by random sampling with put-backs. Moreover, the optimal number of individual learners in the Random Forest is determined as k using the improved artificial bee colony algorithm. While constructing k training datasets for the k individual learners, the RF algorithm simultaneously generates k out-of-bag (OOB) datasets, denoted as OOB_1, OOB_2, ..., OOB_k.

(2) Calculation of Behavioral Evidence Indicator Importance: Each OOB dataset is fed into its corresponding decision tree, resulting in k OOB prediction accuracies, denoted as OA_1, OA_2, ..., OA_k. For the behavioral evidence indicator Q_i, the indicators under this assessment indicator in all OOBs are randomly replaced, and the other behavioral evidence indicators remain unchanged, thus obtaining a new OOB, which is inputted into the corresponding decision tree, and the prediction accuracy of the assessment indicator Q_i can be obtained aOA_{1i}, OA_{2i}, ..., OA_{ki}. The importance of the behavioral evidence indicator Q_i, denoted as VIMi, is calculated by comparing the two sets of prediction accuracies. The calculation is given by the following equation (3):

$$VIM_i = \frac{1}{k}\sum_{t=1}^{k}(OA_t - OA_{ti}) \tag{3}$$

By repeating the above process, the importance of each behavioral evidence indicator can be calculated: VIM_1, VIM_2, ..., VIM_n.

(3) Calculation of Objective Weights for Each Behavioral Evidence Indicator: Normalization was done for each behavioral evidence indicator variable to obtain the weight of each behavioral evidence indicator variable:

$$W_m = \frac{VIM_m}{\sum_{i=1}^{n} VIM_i} \tag{4}$$

The final objective weights of behavioral evidence indicators for each access device in the Ship Ad Hoc Networks are:

$$W_o = \left[W_1, W_2, W_3, \cdots, W_n\right]^T \tag{5}$$

Improved Artificial Bee Colony Algorithm for Determining RF Hyperparameters: For the above random forest strategy, the choice of its parameters directly determines its accuracy and stability [32]. The artificial bee colony algorithm performs global and local optimal solution searches during each iteration of hyperparameter optimization, which can effectively avoid local optima and improve the model performance [33]. However, its drawbacks include slower convergence and lower accuracy [34]. In this paper, the artificial bee colony algorithm is improved by dividing the algorithm's optimization search process into pre-, mid, and post according to the Euclidean distance formula and the number of iterations, and the global optimal solution is introduced in the mid and post as a reference honey source for updating the nectar source, which accelerates the speed of convergence and improves the algorithm's exploratory ability and accuracy. The detailed computational flow of the improved artificial bee colony algorithm is as follows.

A nectar location represents a hyperparametric combinatorial solution to a random forest, and an employed bee corresponds to collecting a nectar source. Therefore, the number of employed bees (i.e., population size: SN1) should be equal to the amount of nectar in the initial stage, and the stochastically initialized population is generated by the following equation:

$$x_{i,j} = x_{\min,j} + rand(0,1) \times (x_{\max,j} - x_{\min,j}) \tag{6}$$

where $i \in \{1,2,...,SN1\}$, $j \in \{1,2,...,D\}$(D is the dimension of the solved problem and the number of hyperparameters of the solved random forest), $x_{max,j}$ and $x_{min,j}$ are upper and lower bounds for the values of $x_{i,j}$.

(1) Pre-stage global search phase: Next is the pre-global search phase process, where the SN1 scale employed bees begin their work. Generate a new position where the current position $x_{i,j}$ is known:

$$v_{i,j} = x_{i,j} + \phi_{i,j} \times (x_{i,j} - x_{k,j}) \tag{7}$$

where $k \in \{1,2..., SN\}$ and $j \in \{1,2,..., D\}$ are randomly chosen subscripts, $k \neq i$; $\emptyset_{i,j}$ is a random number within [-1,1].

Onlooker bees will select employed bees to discover the nectar source according to the probability and then search further. The selection probability is as in equation (8):

$$p_i = \frac{f_i}{\sum_{i=1}^{n} f_i} \tag{8}$$

where f_i is the fitness value of the feasible solution.

If no better nectar source is available after passing the required number of cycles of search, the nectar source is abandoned. The scout bees will randomly select a new nectar source by using equation (6).

(2) Mid-stage optimal search phase: To reduce ineffective searches of the bee colony and accelerate algorithm convergence, the diversity of the colony is calculated using the Euclidean formula, as shown in Equation (9). Based on the determined D value and the number of iterations, the colony size is adjusted to SN2 to enter the mid-stage optimal search phase. In Euclidean space, the Euclidean distance between points $P_x=(x_1,\cdots,x_n)$ and $P_y=(y_1,\cdots,y_n)$ is:

$$d(P_x, P_y) = \sqrt{\sum_{i=1}^{n} (x_i - y_i)^2} \tag{9}$$

The average distance is:

$$D = \frac{2}{N(N-1)} \sum_{i=1}^{N} \sum_{j=1+i}^{N-1} d(P_i, P_j) \tag{10}$$

SN2 scale employed bees, onlooker bees, and scout bees start working. When the colony is updated, the bees refer to the global best nectar source to improve the exploration capability of the algorithm. The honey sources are updated according to equation (11).

$$v_{i,j} = x_{\text{ibest},j} + \phi_{i,j} \times (x_{ibest,j} - x_{i,j}) \tag{11}$$

(3) Late-stage fine search phase: The later stage is based on the intermediate stage and is once again scaled down to perform a fine search, which leads to fast and hyper-parametric optimal results. The D value or the number of iterations specified in the midterm is calculated according to equation (9) and (10) thereby reducing the colony size to SN3, which also contains employed bees, onlooker bees, and scout bees, and the updating mechanism uses the midterm updating of the nectar source equation (11).

Objective Weight Calculation Model Based on SABC-RF: Parameter optimization plays a key role in the performance of machine learning algorithms, and the performance of machine learning algorithms is usually improved by adjusting the parameters in practical applications [35]. In this paper, the SABC algorithm is used to optimally adjust the hyperparameters of RF to improve the performance of the objective weight model of RF calculation index. The flow chart of the objective weight calculation of SABC-RF is shown in Figure 7.

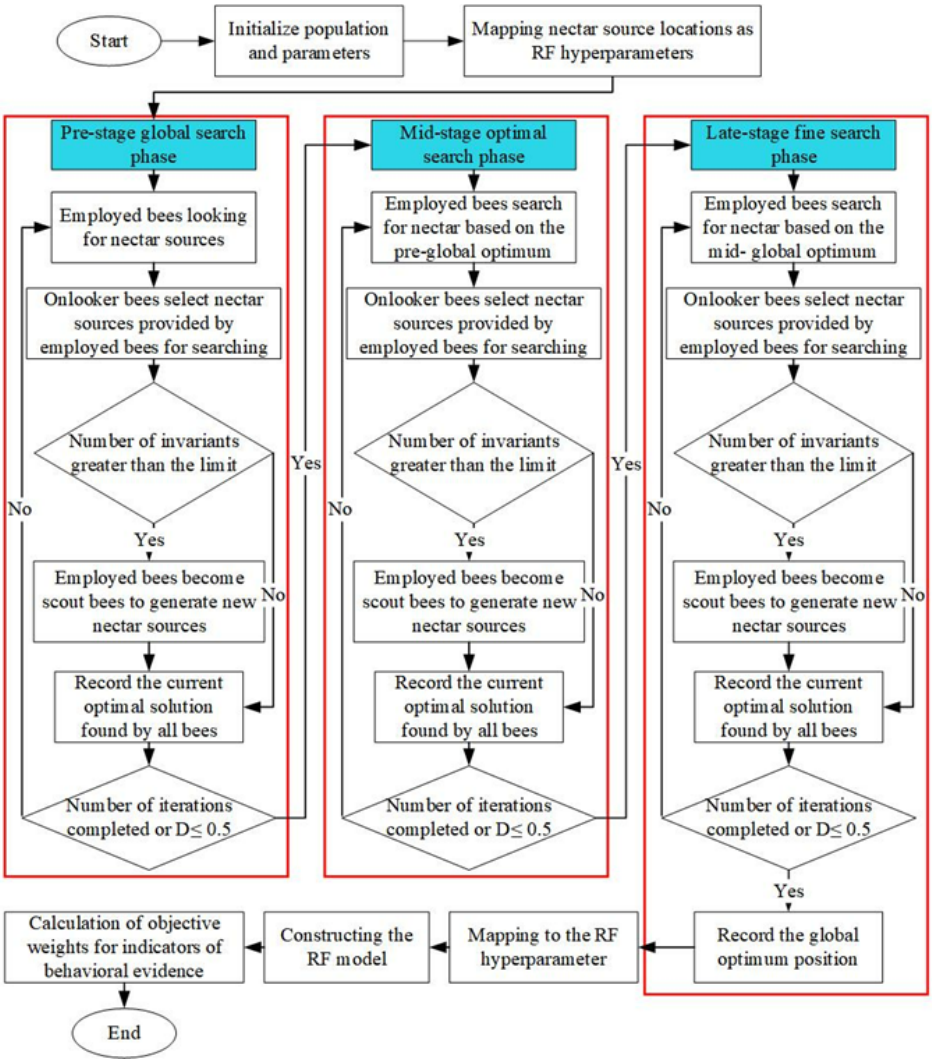


Figure 7. Flow of objective weight calculation based on SABC-RF

3.2.3. Combination Weights Based on Weighted Coefficients

In order to balance the subjective and objective weights of the behavioral evidence of the access devices of the Ship Ad Hoc Networks in the establishment process of the coefficient allocation problem, the distance function is used to allocate the weighting coefficients. The distance function expressions for both subjective and objective are shown in equation (12):

$$d(W_s,\ W_o) = \sqrt{\frac{1}{2}\sum_{i=1}^{n}(W_s - W_o)^2} \tag{12}$$

The Ship Ad Hoc Networks access devices behavioral evidence portfolio weights are calculated as shown in equation (13):

$$W = \alpha W_s + \beta W_o \tag{13}$$

where W portfolio weights, α, β are subjective and objective weight coefficients, respectively.

To reduce the difference between subjective and objective weights and ensure that the allocation coefficient is equal to the distance function, the weight coefficient is calculated using equation (14):

$$\begin{cases} \alpha + \beta = 1 \\ d(W_s,\ W_o)^2 = (\alpha - \beta)^2 \end{cases} \tag{14}$$

3.2.4. Calculation of Direct Trust Evaluation Value

The direct trust evaluation value directly reflects the credibility of the access device and is obtained by collecting behavioral evidence of the access device through traffic monitoring tools and other hardware and software detection methods. However, due to the diversity of the behavioral evidence of Ship Ad Hoc Networks access devices, as well as the directional and monotonic nature of each piece of evidence, to facilitate the calculation of the trust evaluation value for the Ship Ad Hoc Networks access devices, these pieces of evidence are standardized and normalized.

The degree of evidence membership to the fuzzy concept ‘f-optimal’ is characterized by the superiority degree formula .

For the "the more, the better" type of evidence: g=[e-sup(e)]/[sup(e)-inf(e)], For the "the less, the better" type of evidence: g=[sup(e)-e]/]sup(e)-inf(e)].

Where g is the degree of superiority of the evidence and e is the value of the evidence obtained directly or after a simple calculation, sup(e) and inf(e) are the upper and lower bounds of the evidence values, respectively, and the evidence superiority takes values between [0, 1], with larger values being better.

The processed behavioral evidence was multiplied with the combined weight of each behavioral evidence to obtain the final direct trust assessment value as in equation (15):

$$T = GW = \sum_{i=1}^{n} [G_i W_i] \tag{15}$$

3.3. Indirect Trust Evaluation Based on Historical Data

The indirect trust assessment value directly reflects the credibility of the historical interaction of the access devices, and the indirect trust assessment integrates the historical data, which is the comprehensive trust value that has been interacted with and gradually accumulated by the Ship Ad Hoc Network access devices in the network over a long period [36]. As devices continue to interact in the ad hoc network, new comprehensive trust assessment data will continue to be generated, and long-ago historical data may lose its reference value in the assessment process. By setting a reasonable time window mechanism as shown in Figure 8, only the historical interaction data within that time window is retained, discarding the long-ago historical data and improving the assessment accuracy.

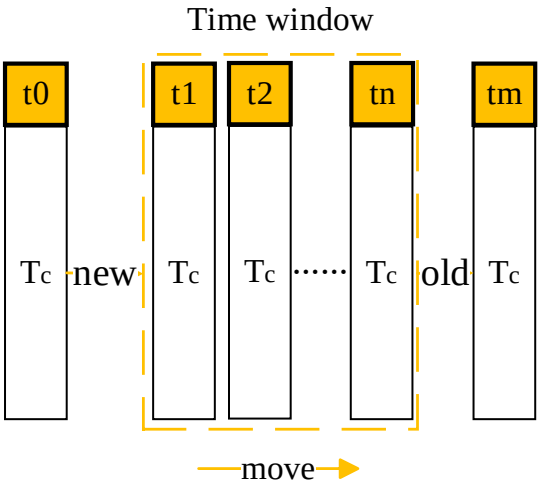


Figure 8. Comprehensive weighting time window

In conducting indirect trust assessments, it is necessary to both refer to and correct historical data for time decay to ensure the accuracy and usefulness of the assessment. Therefore, a decay factor based on time difference is introduced into the indirect trust assessment calculation as in equation (16), which makes the historical data of earlier periods have less influence and the historical data of more recent periods have higher weights to improve the accuracy and reliability of trust assessment. Each data weight is obtained by normalization as in equation (17):

$$w_i = e^{-\lambda i} \tag{16}$$

$$S_i = \frac{w_i}{\sum_{i=1}^{n} w_i} \tag{17}$$

Assuming that there are n sets of data in the time window, the indirect trust of the access device is calculated as in equation (18):

$$\begin{cases} T_u = \sum_{i=1}^{n} (T_i \times S_i) & n \geq 1 \\ T_u = 0 & n = 0 \end{cases} \tag{18}$$

3.4. Calculation of Comprehensive Trust Evaluation Value

Comprehensive trust assessment is a combination of direct trust assessment based on behavioral evidence and indirect trust assessment based on historical data to get a more comprehensive and accurate trust assessment of the access devices, calculated as in equation (19):

$$T_c = aT + bT_u \tag{19}$$

where a is the direct trust factor and b is the indirect trust factor, a+b=1.

4. Experimental Design and Results Analysis

In this section, the experiments are designed and the results are analyzed in detail. First, the convergence and accuracy of the improved artificial bee colony algorithm in this paper are verified by designing comparative experiments, while the optimal parameters of RF are determined to improve the accuracy of objective weights. Second, the combined weights of the direct trust evaluation model in this paper are calculated, and the detection effects of the direct trust evaluation model with combined subjective and objective weights proposed in this paper and the traditional direct trust evaluation model are analyzed by designing different ratios of malicious devices.

Again, by comparing the different λ taken in the indirect trust evaluation, the accuracy and detection rate of the model are analyzed to determine the λ value of the indirect trust evaluation to ensure its accuracy. Finally, to further verify the accuracy and superiority of the comprehensive trust evaluation model proposed in this paper, similar methods applied to the same scenario are compared, and the results are analyzed.

4.1. Verification of the Improved Artificial Bee Colony Algorithm

To accurately verify the convergence speed and precision of the improved Artificial Bee Colony algorithm (SABC) proposed in this paper, 500 sets of device data were collected from commonly used maritime ad hoc network equipment, including law enforcement recorders, airborne ad hoc radios, and handheld ad hoc wireless terminals. Among these, 30% of the devices with trust evaluation values below 0.5 were identified as malicious. The performance of the optimization algorithm was evaluated by comparing the accuracy and detection effectiveness of a Random Forest model constructed using hyperparameters optimized by the algorithm on the dataset, thereby demonstrating the advantages and disadvantages of the optimization method.

This study compares the improved Artificial Bee Colony algorithm (SABC) with the traditional Artificial Bee Colony algorithm (ABC), an existing improved Artificial Bee Colony algorithm (iqABC), and the Genetic Algorithm (GA) to analyze the performance of Random Forest models constructed using the optimal parameter combinations found by each approach. The parameters for GA are set as follows: 100 generations, a population size of 100, a chromosome length of 14, a crossover factor of 0.7, and a mutation factor of 0.3. For ABC and iqABC, the population size is set to SN = 100, with an iteration limit of 50 and a total of 200 iterations. The SABC employs a phased strategy: in the early stage, a swarm size of SN1 = 100 is used for global search; when the fitness criterion D reaches 0.5 or the early iteration count reaches 100, the algorithm enters the mid-stage, where the swarm size is reduced to SN2 = 60 for optimal search; when D further decreases to 0.3 or the mid-stage iteration count reaches 60, the algorithm transitions to the late stage, where the swarm size is further reduced to SN3 = 30 for a fine-tuned search over 40 iterations.

In this study, accuracy and detection rate are used to evaluate the performance of the model. Accuracy represents the proportion of correctly classified samples to the total test samples, while the detection rate measures the ratio of detected malicious devices to the total number of malicious devices.

$$\text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN} \tag{20}$$

$$\text{Detection Rate} = \frac{TP}{TP + FN} \tag{21}$$

Where TP (True Positive) represents correctly predicted malicious device states, FP (False Positive) indicates normal devices mistakenly classified as malicious, TN (True Negative) refers to correctly predicted normal devices and FN (False Negative) denotes malicious devices incorrectly classified as normal. The detailed evaluation results are defined in Table 1.

Table 1. Table of definitions of assessment results

Actual / Prediction	Malicious device	Normal device
Malicious device	TP	FN
Normal device	FP	TN

The optimal parameter combinations (n_estimators, max_depth, max_features, min_samples_leaf) of the random forest solved by each optimization algorithm were obtained experimentally. Where ABC is (108, 6, 4, 4), iqABC is 102, 5, 4, 5), SABC is (98, 4, 7, 5), GA is (89, 5, 6, 4). The time to solve the optimal parameter combination of each optimization algorithm and the evaluation results of building the random forest model are obtained as shown in Figure 9.

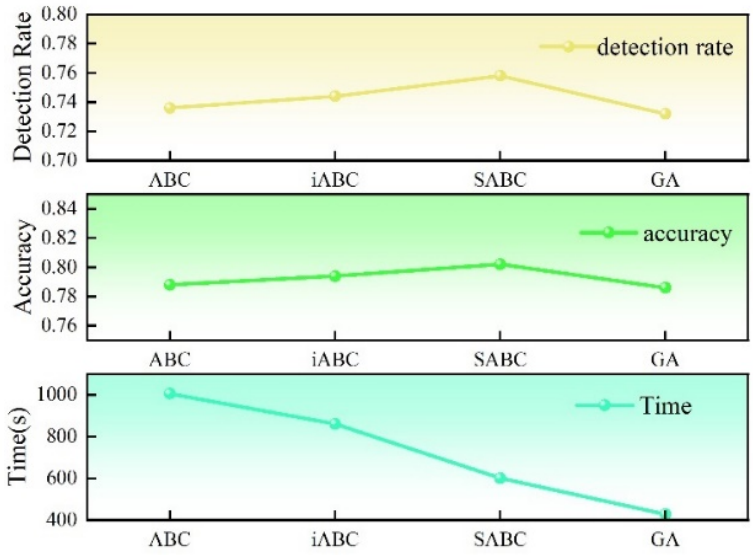


Figure 9. Comparison of results of each optimization algorithm

As shown in Figure 9, the proposed SABC algorithm obtained the optimal hyperparameters for the Random Forest model in 600.5 seconds, whereas the GA algorithm required 482.4 seconds, indicating that SABC is less efficient in terms of time compared to GA. However, SABC outperforms GA in terms of accuracy and detection rate, improving GA's 78.6% accuracy and 73.2% detection rate by 1.6% and 2.6%, respectively. While the accuracy and detection rate improvements over ABC and iqABC are relatively small, SABC demonstrates a significant advantage in time performance, reducing computation time by 405.1 seconds compared to ABC's 1005.6 seconds and 260 seconds compared to iqABC's 860.5 seconds. Therefore, based on a comprehensive analysis, the proposed SABC algorithm proves to be more advantageous for optimizing the hyperparameters of the Random Forest model.

4.2. Calculation and Verification of Direct Trust Evaluation Weights

In direct trust evaluation, different behavioral indicators contribute unequally to the overall trust assessment of access devices. To ensure objectivity and reliability in trust computation, it is necessary to assign appropriate weights to these indicators and validate their effectiveness. This subsection focuses on the calculation of direct trust evaluation weights and presents the corresponding verification process to demonstrate the rationality of the weighting results.

4.2.1. Calculation of Direct Trust Evaluation Weights

In this paper, behavioral evidence indicators are determined based on expert opinions and relevant knowledge, and the trust evaluation is calculated by obtaining behavioral evidence and normalizing it through traffic monitoring tools, and the indicators at each level are determined as shown in Table 2.

Table 2. Table of behavioral evidence for indicators at each level

Target layer	Primary indicator layer	Sub-indicator layer	Information
Behavioral evidence indicators	Reliability attribute	Number of successful connection establishments	Positive
		Data transmission packet loss rate	Negative
		Task processing time	Negative
	Security attribute	Number of unauthorized access attempts	Negative
		Nmber of illegal connections	Negative
		Number of denied service connections	Negative
	Conventional attribute	Number of username guessing attempts	Negative
		Number of password guessing attempts	Negative
		IP transmission delay	Negative

In this paper, subjective weights are calculated through the FAHP with subjectivity, the importance of indicators is analyzed according to expert opinions, and the fuzzy judgment matrix is constructed through the 0.1-0.9 scaling method so as to solve the weights of each level and the subjective weights as in Table 3. The objective weights based on the SABC-RF show the objectivity through the analysis of the data, and the optimal parameters of the Random Forest are solved through the SABC as (98, 4, 7, 5); based on the optimal hyperparameter configuration of the construction of the random forest model, the use of the out-of-bag error estimation method of Ship Ad Hoc Network access device behavioral evidence indicators to assess the importance of the characteristics, and then to determine the weights of each indicator as in equation (22).

$$W_o = \left[0.1595, 0.0668, 0.0951, 0.2211, 0.2348, 0.0881, 0.0136, 0.0554, 0.0656\right]^T \quad (22)$$

Table 3. Table of subjective weighting results

Target layer	Primary indicator layer	Weight	Sub-indicator layer	Weight	Subjective weight
Behavioral evidence indicators	Reliability attribute	0.32	Number of successful connection establishments	0.39	0.1248
			Data transmission packet loss rate	0.31	0.0992
			Task processing time	0.30	0.096
	Security attribute	0.42	Number of unauthorized access attempts	0.42	0.1764
			Nmber of illegal connections	0.32	0.1344
			Number of denied service connections	0.26	0.1092
	Conventional attribute	0.26	Number of username guessing attempts	0.27	0.0702
			Number of password guessing attempts	0.39	0.1014
			IP transmission delay	0.34	0.0884

The distance function method to solve the subjective and objective weight coefficients, and according to the weight coefficients to solve the combination of the weights as in Table 4.

Table 4. Combined weights results table

Sub-indicator layer	W_s	W_o	W
Number of successful connection establishments	0.1248	0.1595	0.141803
Data transmission packet loss rate	0.0992	0.0668	0.083324
Task processing time	0.096	0.0951	0.095559
Number of unauthorized access attempts	0.1764	0.2211	0.198303
Number of illegal connections	0.1344	0.2348	0.183596
Number of denied service connections	0.1092	0.0881	0.098861
Number of username guessing attempts	0.0702	0.0136	0.042466
Number of password guessing attempts	0.1014	0.0554	0.07886
IP transmission delay	0.0884	0.0656	0.077228

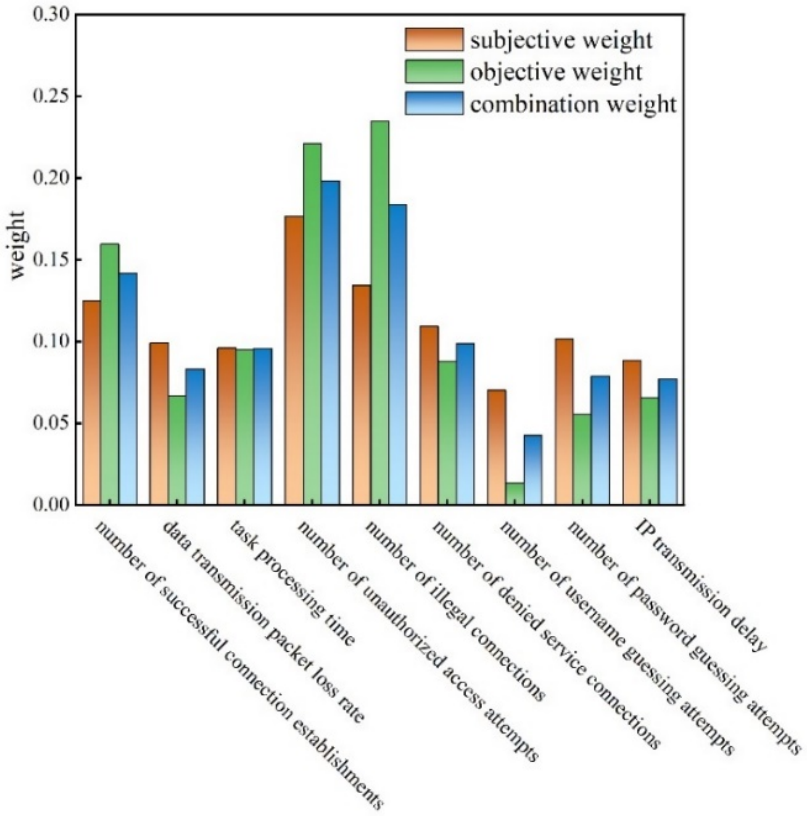
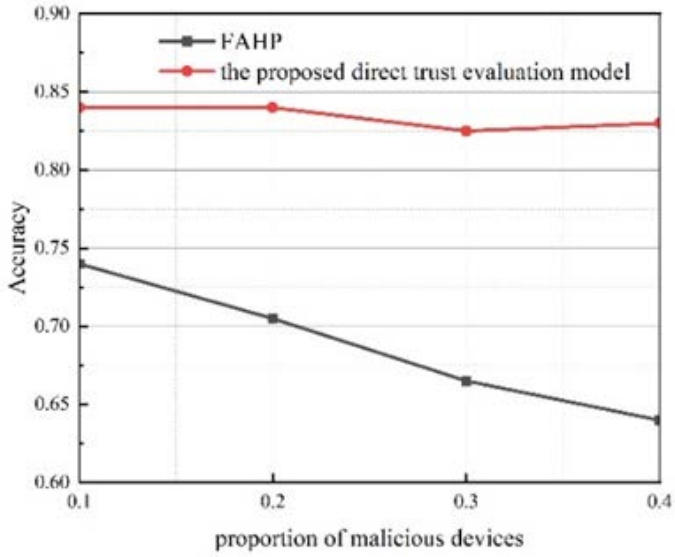


Figure 10. Comparison of weights

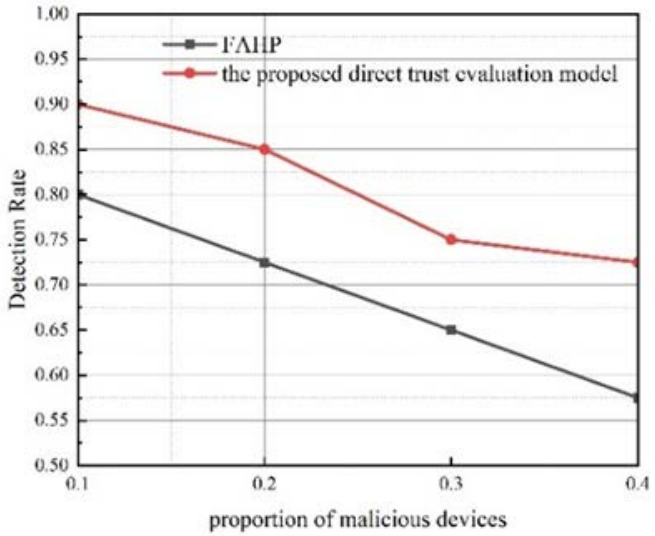
From Table 4 and Figure 10, it can be observed that the weights of the behavioral evidence indicators obtained using the fuzzy analytical hierarchy process are more concentrated, with the number of unauthorized access attempts having the greatest impact on direct trust evaluation. In contrast, the objective weights derived from the Random Forest model show larger differences in the weights of each indicator, with the number of unauthorized access attempts and the number of illegal connections having the greatest impact on direct trust evaluation.

4.2.2. Verification of Direct Trust Evaluation Model

To verify the computational accuracy of the direct trust evaluation model in this paper, this part screens 200 groups of devices with direct behavioral evidence data as experimental data, and designs 200 groups of devices containing 10%, 20%, 30%, and 40% of malicious devices with trust evaluation values below 0.5, respectively, and then compares them with FAHP to judge the accuracy of the evaluation model and to judge the effectiveness of the model in detecting malicious devices with the detection rate. Detection rate to determine the effectiveness of the model in detecting malicious devices. The model accuracy and detection rate are shown in Figure 11.



(a)



(b)

Figure 11. (a) Comparison of the accuracy of direct trust evaluation model; (b) Comparison of detection rates of direct trust evaluation model

From Figure 11(a), it can be seen that the average accuracy rate of the direct trust evaluation model in this paper is 0.834, while the average accuracy rate of the FAHP model is 0.688. The accuracy rate decreases with the increase of the proportion of malicious devices, so the direct trust evaluation model of this paper has been greatly improved on the original FAHP and the model has high stability in accuracy rate.

Figure 11(b) shows that the average detection rate of the direct trust evaluation model in this paper is about 80.6%, which is much larger than that of FAHP (68.7%); because the direct trust evaluation model in this paper is a collection of the objectivity of random forests on the subjectivity of FAHP, and the combination of the weights is obtained by the method of the distance function, which can greatly avoid the one-sided influence of subjectivity and objectivity, and improve the evaluation accuracy and detection rate.

4.3. Verification of Indirect Trust Evaluation Decay Factor

Indirect trust evaluation in Ship Ad Hoc Networks often relies on historical interactions, which may become outdated as network conditions and node behaviors change over time. To reflect the temporal validity of indirect trust information, a decay factor is commonly introduced into the trust evaluation process. This subsection verifies the effectiveness of the indirect trust evaluation decay factor and analyzes its role in maintaining the timeliness and reliability of indirect trust assessment.

4.3.1. Calculation of Indirect Trust Evaluation Decay Factor and Corresponding Weights

In the comprehensive trust evaluation model, the attenuation factor λ of the indirect trust evaluation history data also dramatically affects the accuracy of the device evaluation. To select the better attenuation factor λ, the final weights are determined by determining the value of λ and calculating the comparison between the accuracy rate and detection rate of the comprehensive trust evaluation model in this paper, to select the better attenuation factor λ. The comprehensive trust evaluation is mainly based on the direct trust evaluation as the main, and the indirect trust evaluation as the reference, so the direct trust coefficient $a = 0.65$ and the indirect trust coefficient $b = 0.35$ are determined. The weights of indirect trust evaluation under different values of λ are shown in Table 5.

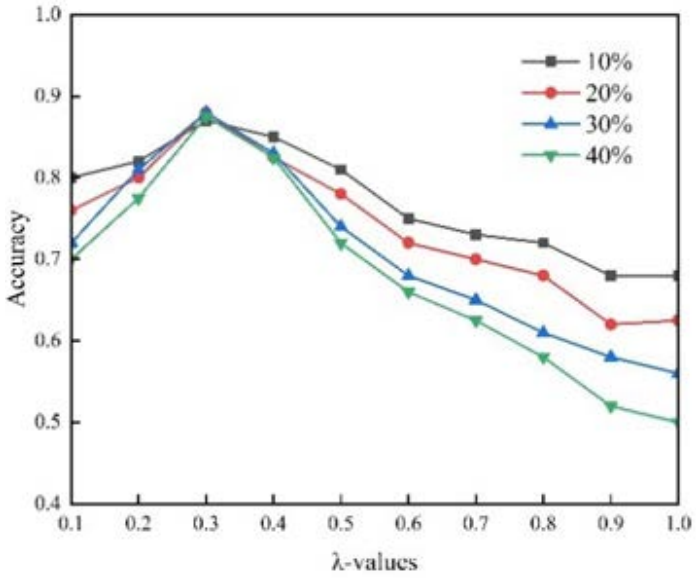
Table 5. Table of weights corresponding to the values taken

λ	Normalized weight
0.1	0.1505、0.1362、0.1233、0.1115、0.1009、0.0913、0.0826、0.0748、0.0676、0.0613
0.2	0.2096、0.1716、0.1404、0.1150、0.0941、0.0770、0.0630、0.0516、0.0422、0.0346
0.3	0.2728、0.2021、0.1497、0.1109、0.0822、0.0609、0.0451、0.0334、0.0247、0.0182
0.4	0.3358、0.2251、0.1509、0.1012、0.0678、0.0454、0.0305、0.0204、0.0137、0.0092
0.5	0.3961、0.2403、0.1457、0.0884、0.0536、0.0325、0.0197、0.0120、0.0073、0.0044
0.6	0.4523、0.2482、0.1362、0.0748、0.0410、0.0225、0.0124、0.0068、0.0037、0.0021
0.7	0.5039、0.2502、0.1243、0.0617、0.0306、0.0152、0.0076、0.0038、0.0019、0.0008
0.8	0.5509、0.2475、0.1112、0.0500、0.0225、0.0101、0.0045、0.0020、0.0009、0.0004
0.9	0.5935、0.2413、0.0981、0.0399、0.0162、0.0066、0.0027、0.0011、0.0004、0.0002
1	0.6321、0.2326、0.0856、0.0315、0.0115、0.0042、0.0016、0.0006、0.0002、0.0001

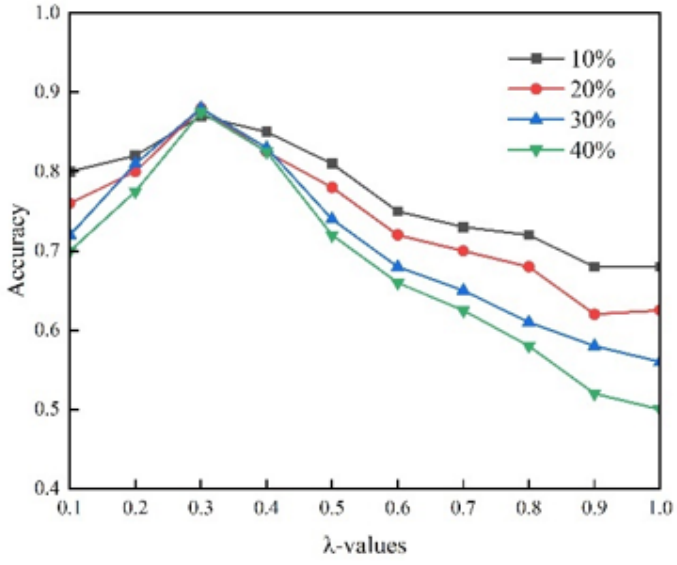
4.3.2. Comparison of Indirect Trust Evaluation Decay Factors

This part screens 200 groups of devices with direct behavioral evidence data and 10 historical interactions data as experimental data and compares the accuracy and detection rate of the model under different λ-values in the case of devices with different malicious proportions by designing the 200 groups of devices that contain 10%, 20%, 30%, and 40% malicious devices with trust evaluation values of 0.5 or less.

The value of λ directly affects the effect of indirect trust evaluation, as shown in Figure 12(a), when λ is taken as 0.3, the comprehensive trust evaluation model of this paper has the highest accuracy rate and less change under different proportions of malicious devices, and the average accuracy rate is about 87.6%, which is 7.6% higher than that of the model of direct trust evaluation. As shown in Figure 12(b), when λ takes the value of 3, the detection rate under different proportions of malicious devices has the smallest change and the highest detection rate, which indicates that the detection effect of this paper's model is the best and most stable.



(a)

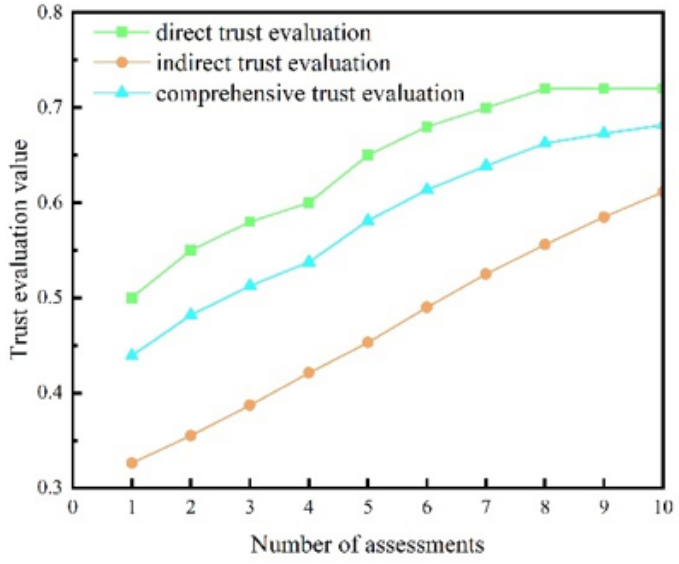


(b)

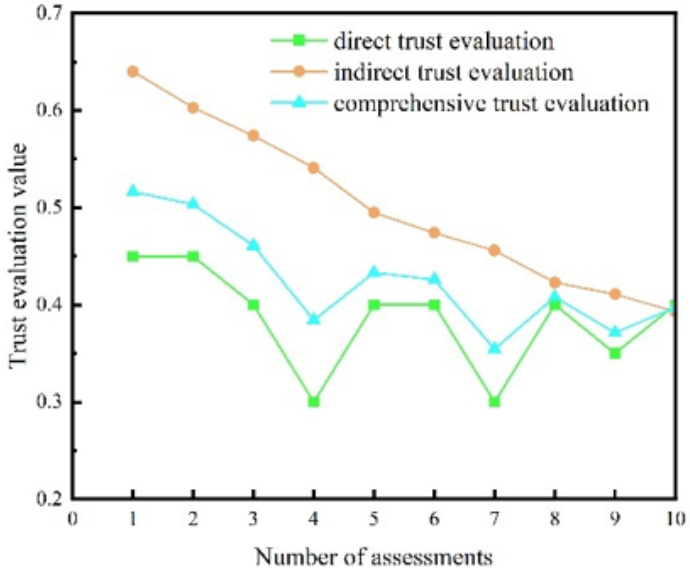
Figure 12. (a) Comparison of accuracy for different values of λ; (b) Comparison of detection rates for different values of λ

To more intuitively express the importance of the indirect trust evaluation proposed in this paper, the paper analyzes the change of the comprehensive trust evaluation value of the malicious device when the subsequent behavioral data is normal to become a normal device and the normal device when there is an illegal behavior to become a malicious device by designing experiments. Figure 13(a) shows that when the direct trust evaluation of the malicious device becomes normal, the indirect trust evaluation combined with the historical data will be evaluated as a malicious device. With the subsequent direct trust evaluation continuously belonging to the normal device, the comprehensive trust evaluation will only become normal, which can effectively avoid the disguise of the malicious device and thus cause a misjudgement.

Figure 13(b) shows normal device in the presence of illegal behavior into a malicious device; the device's indirect trust evaluation value will continue for a certain number of times judged as a normal device, the comprehensive trust evaluation will safeguard the first few evaluations as a normal device, to avoid special circumstances that lead to the device being misjudged as a malicious device. When the normal device continues to be illegal, the indirect trust evaluation will continue to decrease, and the comprehensive trust evaluation will continue to decrease, too. Thus, the device is determined to be a malicious device, improving the accuracy and detection rate.



(a)



(b)

Figure 13. (a) Plot of change in trust value of malicious device to normal device; (b) Plot of change in trust value of normal device to malicious device

4.4. Comparison of the Comprehensive Trust Evaluation Model in This Paper with Similar Application Object Models

In this part, to analyze the accuracy and superiority of the comprehensive trust evaluation model in this paper, the comprehensive trust evaluation model in this paper is compared with the models proposed in literature [13], [17], [29], and [30] by screening the data of 300 groups of commonly used types of Ship Ad Hoc Network access devices (including cell phones, tablet PCs, handheld mesh wireless terminals, etc.) in the dataset as the experimental data.

Analyze and compare the model accuracy and detection rate. Among them, literature [13] proposes a FAHP trust evaluation model.

The paper [17] presents an improved Bayesian equation-based direct trust model using satisfaction functions and time degradation factors, as well as a trust evaluation model that calculates indirect trust weights using grey relational analysis. The study [29] proposes a comprehensive trust evaluation model combining direct trust values calculated using FAHP and user-recommended trust values.

Literature [30] introduces a trust evaluation model that weakens the subjectivity of ANP using fuzzy network analysis based on triangular fuzzy numbers (FANP).

Figure 14 (a), (b), (c), and (d) show the detection rate and detection speed of the model per minute for 300 devices with malicious device proportions of 10%, 20%, 30%, and 40%, respectively. Figure 14 (e) and (f) compare the final accuracy and detection rate of the model.

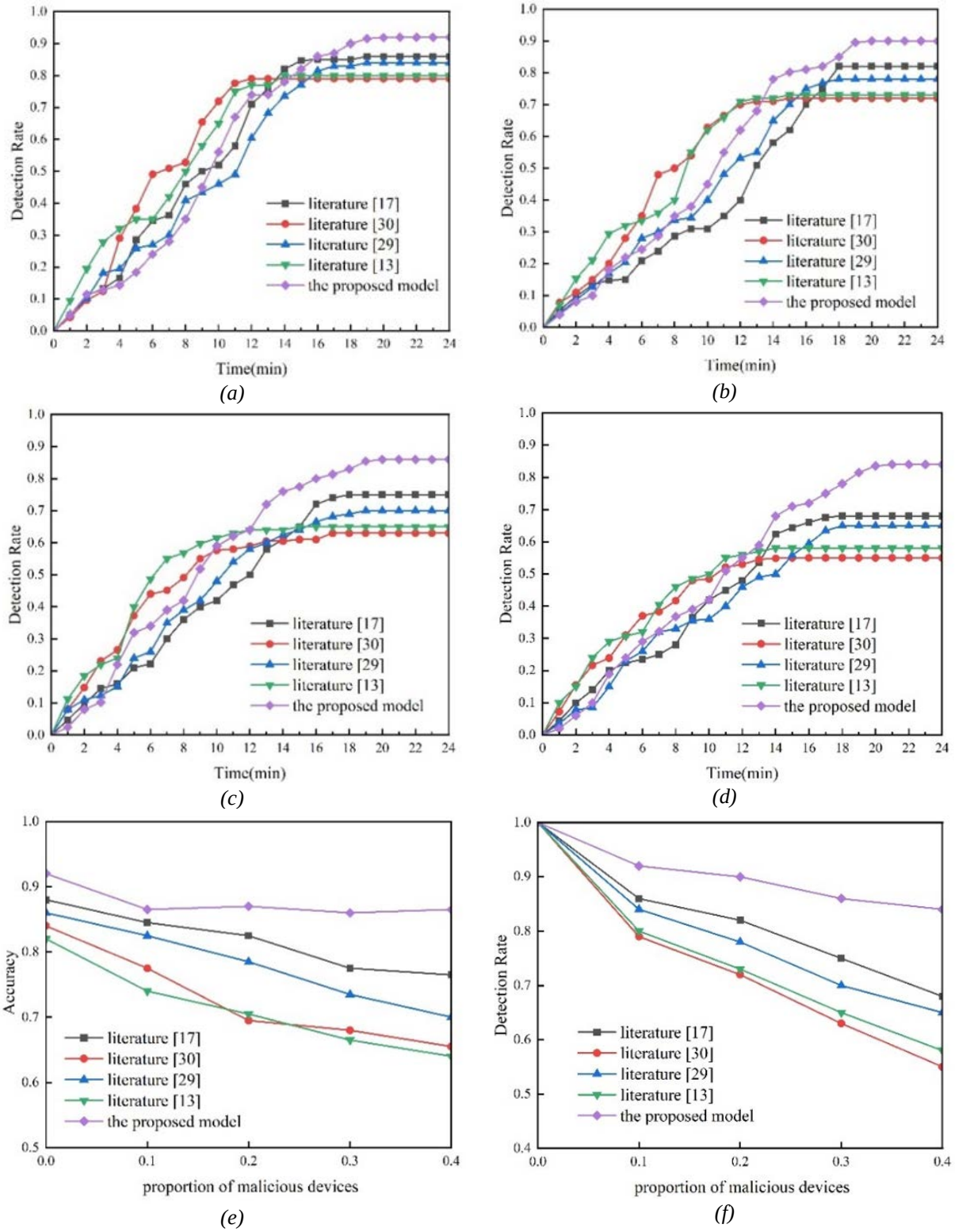


Figure 14. Comparison of accuracy and detection rate with different percentages of malicious devices: (a), (b), (c) and (d) detection rate and detection speed; (e) and (f) final accuracy and detection rate

Figure 14(a) shows that when the proportion of malicious devices is 10%, the detection performance of these models is relatively good, with only minor differences in detection rates among them, with a maximum difference of 13%. Since the proposed model incorporates both direct and indirect trust evaluation, its detection speed is lower than the trust evaluation models proposed in the literature [13] and the literature [30].

Figure 14(b) indicates that when the proportion of malicious devices increases to 20%, the detection performance of all models declines compared to Figure 14(a). However, the detection rate of the proposed model decreases by only 2%, the smallest decline among all models. Figure 14(c) and 14(d) illustrate that as the proportion of malicious devices increases to 30% and 40%, the gap in detection rates between models widens, and the detection rates of the comparison models drop significantly.

In contrast, the proposed model maintains a stable detection speed, with detection rates decreasing by only 4% and 6% at a 20% malicious device ratio, demonstrating high stability.

Figure 14(e) shows that the accuracy of this paper's model stabilizes at around 0.865 as the number of malicious devices increases, while the proposed comparison models all have different degrees of decline.

Figure 14(f) shows that the detection rate of the model decreases as the proportion of malicious devices increases, but the maximum difference of the detection rate model of this paper under different proportions of malicious devices is only 8%, and the difference of the detection rate of the proposed comparison model is up to 19%. Comprehensive analysis shows that this paper's model has the highest and most stable accuracy and detection rate under different proportions of malicious devices, mainly because the model firstly adopts the direct trust evaluation of subjectivity and objectivity to avoid the influence of subjectivity and objectivity to produce misjudgment. Secondly, it adopts the indirect trust evaluation of historical data to comprehensively take into account the historical data to improve the model accuracy, which is significantly better than the other four schemes.

To verify the performance optimization effect of the trust evaluation mechanism proposed in this paper, an experimental comparison of the trust changes under different ratios of malicious behaviors is carried out between the comprehensive trust evaluation model in this paper and the proposed comparative trust evaluation model.

Figure 15 shows the trust value changes under different malicious behavior ratios.

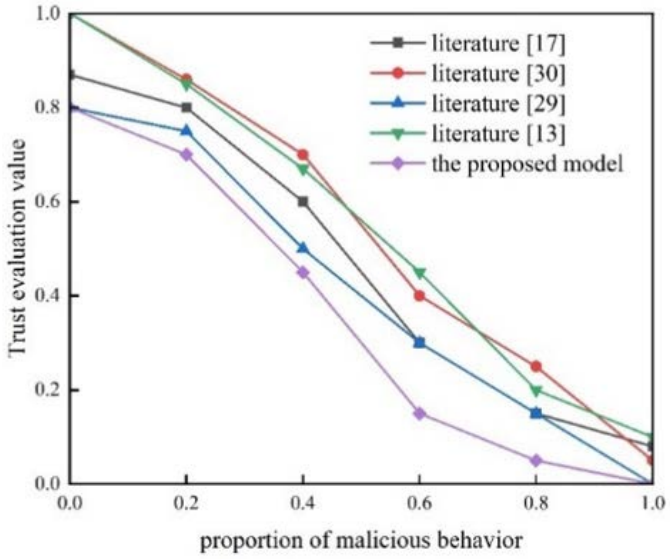


Figure 15. Variation of trust value with different rates of malicious behavior

Figure 15 shows that with the increase of the ratio of malicious behavior of the device, the trust of the device in the trust evaluation model all show a decreasing trend, but the comprehensive trust evaluation model proposed in this paper has a more significant decreasing trend than the proposed comparison model.

Under different ratios of malicious behavior, the trust value of the model in this paper is always lower than that of the proposed comparison model, which indicates that the model in this paper can accurately identify the malicious devices with a low level of trust and improve the accuracy and detection rate.

5. Conclusion

Aiming at the dynamic topology of Ship Ad Hoc Networks and the security challenges of frequent access device access and departure in an open environment, this paper proposes a comprehensive trust evaluation model for Ship Ad Hoc Network access devices based on zero-trust architecture. The model combines direct evaluation based on behavioral data and indirect evaluation based on historical data, aiming to effectively overcome the problems of insufficient adaptability of traditional trust models in dynamic environments and a single evaluation dimension. By improving the reliability and security assessment accuracy of Ship Ad Hoc Network access devices, this model can provide more accurate assessment values for the dynamic authorization process, thus realizing fine-grained authorization and precise control of Ship Ad Hoc Network access devices. The experimental results show that the proposed model can provide fine-grained and high-precision trust evaluation for Ship Ad Hoc Network access devices. It significantly enhances the adaptability and reliability of trust evaluation in the dynamic environment, provides credible decision-making support for application scenarios such as secure communication and collaborative task assignment in Ship Ad Hoc Network, and promotes the development of ship intelligence, digitization of the shipping industry, and modernization of maritime rescue.

Acknowledgements

This study is financially supported by the National Key Research and Development Program Project (No.: 2023YFC3321700) and the Natural Science Foundation General Program in Jiangsu Provincial of China (No.: BK20241965).

References:

[1]. Xu, M., et al. (2023). A systematic literature review of maritime transportation safety management. *Journal of Marine Science and Engineering*, *11*(12), 2311. Doi: 10.3390/jmse11122311

[2]. Li, B., et al. (2023). A dynamic emergency response decision-making method considering the scenario evolution of maritime emergencies. *Computers & Industrial Engineering*, *182*, 109438. Doi: 10.1016/j.cie.2023.109438

[3]. Wang, Q., et al. (2023). An overview of emergency communication networks. *Remote Sensing*, *15*(6), 1595. Doi: 10.3390/rs15061595

[4]. Al-Absi, M. A., et al. (2021). Moving ad hoc networks—a comparative study. *Sustainability*, *13*(11), 6187. Doi: 10.3390/su13116187

[5]. Li, M., et al. (2024). A solution for aerial network coverage with multiple UAV base stations in emergency scenarios. *Yangtze River Information and Communication*, 37(8), 197–200. Doi: 10.20153/j.issn.2096-9759.2024.08.059

[6]. Thuy, N. D. T., et al. (2022). Deployment of UAVs for optimal multihop ad-hoc networks using particle swarm optimization and behavior-based control. *2022 11th International Conference on Control, Automation and Information Sciences (ICCAIS)*, 304-309. Doi: 10.1109/ICCAIS56082.2022.9990164

[7]. Gao, W., Xu, D., & Zhang, G. (2017). Simulation of mesh-based communication network for aircraft carrier formation. *Computer and Modernization*, (2), 45–48. Doi: 10.3969/j.issn.1006-2475.2017.02.009

[8]. Dorri, A., Kamel, S. R., & Kheirkhah, E. (2015). Security challenges in mobile ad hoc networks:a survey. *International Journal of Computer Science & Engineering Survey*, *6*(1), 15–29. Doi: 10.5121/ijcses.2015.6102

[9]. Bobbert, Y., & Scheerder, J. (2020). Zero trust validation: from practical approaches to theory. *Sci. J. Res. Rev*, *2*(5), 830-848. Doi: 10.33552/SJRR.2020.02.000546

[10]. Feng, J., et al. (2022). An edge zero-trust model against compromised terminals threats in power IoT environments. *Journal of Computer Research and Development*, *59*(5), 1120-1132. Doi: 10.7544/issn1000-1239.20211129

[11]. Chen, Z., et al. (2021). Research on Zero-trust Security Protection Technology of Power IoT based on Blockchain. *Journal of Physics: Conference Series*, *1769*(1), 012039. Doi: 10.1088/1742-6596/1769/1/012039

[12]. Chuan, T., et al. (2020). An Implementation Method of Zero-trust Architecture. *Journal of Physics: Conference Series*, *1651*(1), 012010. Doi: 10.1088/1742-6596/1651/1/012010

[13]. Wang, J., et al. (2023). Attribute and user trust score-based zero trust access control model in IoV. *Electronics*, *12*(23), 4825. Doi: 10.3390/electronics12234825

[14]. Lv, P., et al. (2022). Dynamic Trust Continuous Evaluation-based Zero-Trust Access Control for Power Grid Cloud Service. *Journal of Physics: Conference Series*, *2402*(1), 012008. Doi: 10.1088/1742-6596/2402/1/012008

[15]. Tang, D., Cao, X., Lin, Q., Hu, S., & Tang, Z. (2024). Distributed authentication model under the zero-trust architecture of the power Internet of Things. *Information Security Research*, *10*(1), 67–74.

[16]. Zhou, A., et al. (2015). A security authentication method based on trust evaluation in VANETs. *EURASIP Journal on Wireless Communications and Networking*, *2015*(1), 59. Doi: 10.1186/s13638-015-0257-x

[17]. Feng, X., & Yuan, Z. (2022). A novel trust evaluation mechanism for edge device access of the Internet of things. *Wireless Communications and Mobile Computing*, *2022*(1), 3015206. Doi: 10.1155/2022/3015206

[18]. Ahmad, M., et al. (2019). State-of-the-art clustering schemes in mobile ad hoc networks: objectives, challenges, and future directions. *IEEE Access*, *7*, 17067-17081. Doi: 10.1109/ACCESS.2018.2885120

[19]. Su, X., et al. (2015). Case study for ship ad-hoc networks under a maritime channel model in coastline areas. *KSII Transactions on Internet and Information Systems (TIIS)*, *9*(10), 4002-4014. Doi: 10.3837/tiis.2015.10.013

[20]. Lin, B., Duan, J., Han, M., & Cai, L. X. (2022). *Next generation marine wireless communication networks*. Springer. Doi: 10.1007/978-3-030-97307-0

[21]. Wang, X., et al. (2023). Design of multi-modal ship mobile ad hoc network under the guidance of an autonomous ship. *Journal of Marine Science and Engineering*, *11*(5), 962. Doi: 10.3390/jmse11050962

[22]. Pasandideh, F., et al. (2022). A review of flying ad hoc networks: Key characteristics, applications, and wireless technologies. *Remote Sensing*, *14*(18), 4459. Doi: 10.3390/rs14184459

[23]. Khan, K., et al. (2020). A survey on intrusion detection and prevention in wireless ad-hoc networks. *Journal of Systems Architecture*, *105*, 101701. Doi: 10.1016/j.sysarc.2019.101701

[24]. Schneier, B. (1999). Risks of relying on cryptography. *Communications of the ACM*, *42*(10). Doi: 10.1145/317665.317684

[25]. Masduki, B. W., Ramli, K., & Murfi, H. (2018). Implementation and analysis of combined machine learning method for intrusion detection system. *International Journal of Communication Networks and Information Security*, *10*(2), 295-304. Doi: 10.17762/ijcnis.v10i2.3375

[26]. Ramphull, D., et al. (2021). A review of mobile ad hoc NETwork (MANET) Protocols and their Applications. *2021 5th international conference on intelligent computing and control systems (ICICCS)*, 204-211. Doi: 10.1109/ICICCS51141.2021.9432258

[27]. Latif, R. (2022). ConTrust: A novel context-dependent trust management model in social Internet of Things. *IEEE Access*, *10*, 46526-46537. Doi: 10.1109/ACCESS.2022.3169788

[28]. Dhiman, P., et al. (2024). A review and comparative analysis of relevant approaches of zero trust network model. *Sensors*, *24*(4), 1328. Doi: 10.3390/s24041328

[29]. Zhang, K., & Pan, X. Z. (2014). Access control model based on trust of users' behavior in cloud computing. *Journal of Computer Applications*, *34*(4), 1051-1054.

[30]. Lü, Y., Tian, L., & Sun, S. (2013). Trust evaluation and control analysis of user behavior based on FANP in cloud computing environment. *Computer Science*, *40*(1), 132–135.

[31]. Speiser, J. L., Miller, M. E., Tooze, J., & Ip, E. (2019). A comparison of random forest variable selection methods for classification prediction modeling. *Expert systems with applications*, *134*, 93-101. Doi: 10.1016/j.eswa.2019.05.028

[32]. Fouodo, C. J., Kronziel, L. L., König, I. R., & Szymczak, S. (2023). Effect of hyperparameters on variable selection in random forests. *arXiv preprint arXiv:2309.06943*. Doi: 10.48550/arXiv.2309.06943

[33]. Sharma, A. et al. (2020). A review on artificial bee colony and it's engineering applications. *Journal of Critical Reviews*, *7*(11), 4097-4107. Doi: 10.31838/jcr.07.11.558

[34]. Bansal, J. C., et al. (2013). Balanced artificial bee colony algorithm. *International Journal of Artificial Intelligence and Soft Computing*, *3*(3), 222-243. Doi: 10.1504/IJAISC.2013.053392

[35]. Weerts, H. J., Mueller, A. C., & Vanschoren, J. (2020). Importance of tuning hyperparameters of machine learning algorithms. *arXiv preprint arXiv:2007.07588*. Doi: 10.48550/arXiv.2007.07588

[36]. Das, A., & Islam, M. M. (2011). SecuredTrust: A dynamic trust computation model for secured communication in multiagent systems. *IEEE transactions on dependable and secure computing*, *9*(2), 261-274. Doi: 10.1109/TDSC.2011.57