Computers, Materials & Continua

Tech Science Press

Doi:10.32604/cmc.2025.063537

ARTICLE

Three-Level Intrusion Detection Model for Wireless Sensor Networks Based on Dynamic Trust Evaluation

Xiaogang Yuan*, Huan Pei and Yanlin Wu

School of Cyber Security, Gansu University of Political Science and Law, Lanzhou, 730070, China

*Corresponding Author: Xiaogang Yuan. Email: xiaogang061218@163.com

Received: 17 January 2025; Accepted: 16 June 2025; Published: 30 July 2025

ABSTRACT: In the complex environment of Wireless Sensor Networks (WSNs), various malicious attacks have emerged, among which internal attacks pose particularly severe security risks. These attacks seriously threaten network stability, data transmission reliability, and overall performance. To effectively address this issue and significantly improve intrusion detection speed, accuracy, and resistance to malicious attacks, this research designs a Three-level Intrusion Detection Model based on Dynamic Trust Evaluation (TIDM-DTE). This study conducts a detailed analysis of how different attack types impact node trust and establishes node models for data trust, communication trust, and energy consumption trust by focusing on characteristics such as continuous packet loss and energy consumption changes. By dynamically predicting node trust values using the grey Markov model, the model accurately and sensitively reflects changes in node trust levels during attacks. Additionally, DBSCAN (Density-Based Spatial Clustering of Applications with Noise) data noise monitoring technology is employed to quickly identify attacked nodes, while a trust recovery mechanism restores the trust of temporarily faulty nodes to reduce False Alarm Rate. Simulation results demonstrate that TIDM-DTE achieves high detection rates, fast detection speed, and low False Alarm Rate when identifying various network attacks, including selective forwarding attacks, Sybil attacks, switch attacks, and black hole attacks. TIDM-DTE significantly enhances network security, ensures secure and reliable data transmission, moderately improves network energy efficiency, reduces unnecessary energy consumption, and provides strong support for the stable operation of WSNs. Meanwhile, the research findings offer new ideas and methods for WSN security protection, possessing important theoretical significance and practical application value.

KEYWORDS: Wireless sensor networks; intrusion detection; dynamic trust evaluation; data noise detection; trust recovery mechanism

1 Introduction

In the contemporary digital age, network attacks and data breaches pose significant security threats with far-reaching impacts on national security, social stability, and economic development. These threats manifest across diverse sectors, from disrupting critical infrastructure to eroding public trust in digital systems. With the exponential growth of IoT (Internet of Things) technology, Wireless Sensor Networks (WSNs) have become a critical component of the digital ecosystem, finding extensive and diverse applications across multiple domains. In industrial monitoring, they enable real-time tracking of equipment performance to ensure smooth manufacturing processes. In agricultural automation, they help farmers optimize irrigation and fertilization based on accurate environmental data. In environmental monitoring, they play a vital role in collecting data on air quality, water pollution, and climate change. In intelligent transportation, they contribute to traffic management and vehicle-to-infrastructure communication.

However, the inherent vulnerability of sensor nodes in WSNs to malicious activities—such as eavesdropping, tampering, and forgery—has introduced significant security challenges alongside their widespread adoption. As an integral part of IoT, WSNs face escalating security issues with the deepening of their applications. The security of WSNs has thus become a critical and indispensable element of overall network strategy [1].

1.1 Background and Significance of the Research

WSNs are self-organizing networks composed of vast numbers of low-power, low-cost micro sensor nodes, each equipped with sensing and communication capabilities. These sensor nodes are typically deployed in unattended environments, such as remote wilderness areas for environmental monitoring or inaccessible industrial facilities for equipment surveillance. Their primary function is to monitor and collect diverse environmental information, including but not limited to temperature, humidity, light intensity, pressure, sound waves, and even images.

Nevertheless, due to the large number of nodes, limited per-node resources, relatively restricted communication capabilities, and complex deployment environments, WSNs face severe security and privacy threats [2,3]. For example, malicious nodes may disrupt normal network operations through data tampering—injecting fake information into data streams and leading to flawed decisions based on false data. Additionally, denial-of-service attacks may be launched, flooding the network with excessive requests and rendering it unable to serve legitimate users. Sensitive data, such as personal health information from medical sensors or proprietary industrial data, may be intercepted, stolen, or tampered with during transmission, resulting in serious privacy violations. Therefore, ensuring security and privacy protection in WSNs has become an urgent issue demanding immediate attention and resolution.

Traditional network security technologies, such as encryption algorithms, intrusion detection systems, and firewalls, have been employed to enhance WSN security to some extent. Encryption algorithms scramble data to prevent unauthorized access. Intrusion detection systems identify and alert on suspicious activities. Firewalls act as barriers between internal networks and external threats. However, these traditional technologies have inherent limitations: they often require high computing power, imposing a heavy burden on sensor nodes with limited resources. Their high energy consumption can quickly deplete the nodes' limited battery power. Moreover, they are ineffective against internal threats (e.g., attacks from compromised nodes) and newly emerging, evolving digital threats [4,5].

Consequently, there is an urgent need to develop lightweight network security techniques. These techniques must enable fast processing speeds and low energy consumption, thereby providing novel and effective solutions for securing WSNs.

1.2 Current Research Status

WSNs have inherent limitations and vulnerabilities, making them prone to attacks. Conventional methods like authentication and encryption can only defend against external threats. Thus, an efficient intrusion detection model is essential to counter internal malicious and faulty nodes. Dynamic hierarchical trust management, which evaluates node trust based on energy, behavior, and communication quality, can better protect against malicious attacks and internal fraud, enhancing network security and reliability [6–8]. Intrusion detection algorithms based on trust can achieve high detection rates and low False Alarm Rate in typical attacks. They can defend against internal attacks with relatively low computational complexity, ensuring secure data transmission [9,10].

In 2015, Tong et al. proposed a hierarchical clustering WSNs intrusion detection scheme based on node trust value and Mahalanobis distance to detect common intrusions with high accuracy [11]. In 2019, Xu and Li combined trust and noise detection, calculating relative deviation values across layers to obtain fusion trust values, performing well in single and cross layer attacks [12]. In 2021, Muhannad and Agoyi developed a hybrid wormhole attack detection algorithm for mobile Adhoc networks, which is based on jump-based round trip time and packet transfer rate, reducing latency and energy consumption [13].

In 2022, Bharti et al. used Bayesian probability statistics for trust management, avoiding malicious nodes with high reputation [14]. Kagade and Jayagopalan proposed a two-level trust assessment intrusion detection system based on deep learning in WSNs [15]. Tao et al. addressed the vulnerability of trust models to attacks by introducing punishment and evaporation factors [16].

In 2023, Cho and Qu monitored continuous packet loss to speed up internal attacker detection, with advantages in network performance [17]. Teng et al. built a dynamic trust evaluation and prediction model using adaptive weight updates and sliding time windows [18]. Li and Sun designed a global trust intrusion detection algorithm based on attribute change rate for industrial WSNs, improving detection precision and reducing energy consumption [19].

Trust mechanism-based intrusion detection algorithms have demonstrated significant advantages in network security, exhibiting robust performance in resisting internal and external network attacks while ensuring reliable data transmission. However, these methods are not without limitations, with several key areas requiring improvement:

- Parameter-Dependent Detection Capability: In the complex and dynamic environment of wireless sensor networks (WSNs), parameters may deviate or be lost due to noise interference, node failures, or other factors. This undermines the accuracy of trust value calculations, thereby limiting the further enhancement of detection capabilities. As a result, maintaining high detection rates alongside low false alarm and missed alarm rates across all scenarios remains challenging.
- Inadequate Consideration of Node Heterogeneity: Wireless sensor nodes vary significantly in energy capacity, computing power, and communication capabilities. However, most existing intrusion detection methods fail to fully account for how such heterogeneities impact trust evaluation and detection performance. Complex detection algorithms may not be effectively deployed on low-computing-power nodes, compromising the comprehensiveness and continuity of detection and reducing overall effectiveness.
- Narrow Application Scenarios: Some methods exhibit strong dependency on specific conditions or node states. For example, a WSNs intrusion detection system based on deep learning and two-level trust evaluation relies on high-energy sensor nodes as cluster heads. In energy-constrained real-world WSNs scenarios, the limited selection of cluster heads diminishes detection efficacy and restricts its applicability across broader contexts.

1.3 Content and Main Contributions of the Research

In order to improve the detection accuracy and reduce the detection energy consumption of WSNs intrusion detection, a WSNs intrusion detection model based on dynamic trust sensing and data noise classification technology is designed. The research mainly makes contributions in the following three aspects:

- By analyzing the continuous packet loss and the characteristics of energy consumption change in WSNs under different types of attacks such as selective forwarding attack, Sybil attack, and black hole attack, a trust evaluation model is established from three aspects: communication trust, data trust, and energy consumption trust. These models can accurately and quickly respond to the changing characteristics of the trust degree of the attacked nodes.

- According to the requirements of WSNs intrusion detection algorithm design, the grey Markov model is used to dynamically predict the node trust value. In this way, the dynamic trust value of nodes can better reflect the comprehensive cognition of the future change trend of network security and improve the sensitivity and speed of intrusion detection.
- The improved DBSCAN (Density-Based Spatial Clustering of Applications with Noise) data noise detection technology is used to detect communication trust, data trust, and energy consumption trust. Furthermore, a trust recovery mechanism is added to reduce the False Alarm Rate of intrusion detection, which effectively improves the Detection Rate and reduces the False Alarm Rate.

This paper first analyzes the characteristics of WSNs and the changes of node attributes in detail, calculates the detection parameters according to different intrusion methods, uses the grey Markov model to dynamically predict the node trust value, and establishes a dynamic hierarchical trust evaluation model for WSNs. According to the three-level detection structure of base station, cluster head, and ordinary node, the DBSCAN data noise monitoring technology is used to quickly identify the attacked nodes, and the trust recovery mechanism is used to restore the trust of temporary fault nodes to reduce the False Alarm Rate, so as to establish the WSNs intrusion detection model TIDM-DTE.

The rest of this paper is organized below. Section 2 designs the network topology and energy consumption model of the WSNs, followed by the design of the trust evaluation and intrusion detection model in Section 3. Section 4 is the experimental part, which introduces the experimental design and specific content, and analyzes the experimental results in detail. Finally, Section 5 presents conclusions and future research directions.

2 Network Topology and Model of Energy Consumption

Network topology is the basis of a safe and stable network operation, and it is also the focus of WSNs research. The organization of each node in WSNs is determined by the network topology. The larger the scale of WSNs is, the larger the energy consumption is. In this research, a more typical cluster topology WSNs is selected as the research object for analysis, and its basic structure is shown in Fig. 1.

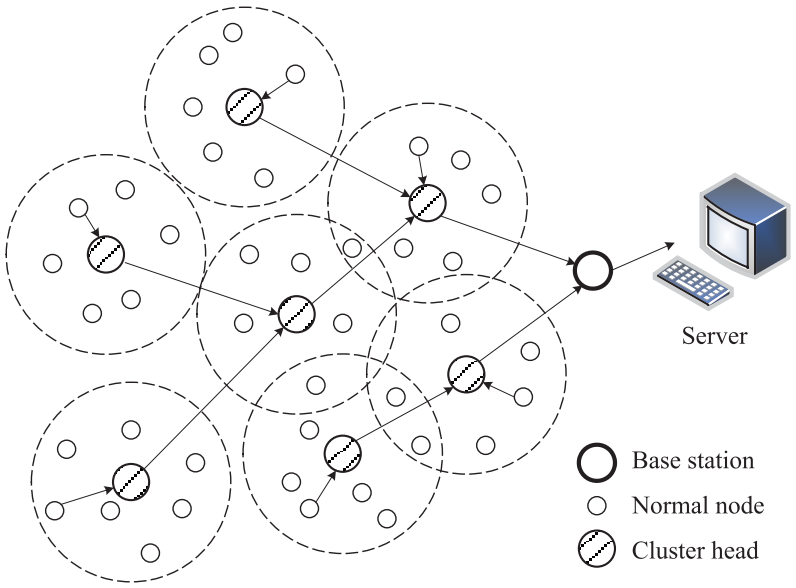

Figure 1: Structure of cluster-like WSNs

2.1 Model of WSNs Network

It is assumed that WSNs consist of a base station h_0 and K sensor nodes distributed in a square monitoring area with side length L. $CH = \{h_1, h_2, \ldots, h_M\}$ is a cluster head node set, $G = \{g_1, g_2, \ldots, g_N\}$ is a common node set, and $K = M + N$. $d_{g_p h_i}$ is the distance between the node g_m and the node h_n.

The network has the following features [20,21]:

1. The base station is trusted and has unlimited energy, and the initial energy of all sensor nodes is the same.
2. The relative position of the nodes in the network is directly estimated by the location method.
3. The positions of sensor nodes and base stations will not change after they are determined, and all sensor nodes have an ID.
4. The sensor nodes have an energy control mechanism, which can adjust the amount of energy sent according to the transmission distance.

2.2 Model of Energy Consumption

The energy consumed $E_{Tx}(q,d)$ of a node sending q bytes of data to a location with distance d is calculated as [21,22]:

$$E_{Tx}(q,d) = E_{Tx-elsc}(q) + E_{Tx}(q,d) = \begin{cases} qE_{elsc} + q\varepsilon_{fs}d^2 & , d < d_0 \\ qE_{elsc} + q\varepsilon_{fs}d^4 & , d \geq d_0 \end{cases} \tag{1}$$

$$d_0 = \sqrt{\varepsilon_{fs}^2 / \varepsilon_{amp}} \tag{2}$$

where, E_{elec} is the energy consumption of sending or receiving 1 bit of data, $E_{Tx\text{-}elec}(q)$ is the energy consumption of sending q bits of data, ε_{fs} is the magnification of the free space model.

The energy consumption $E_{Rx}(q)$ of a node to receive q bytes of data is calculated as:

$$E_{Rx}(q) = E_{Rx-elec}(q) = qE_{elec} \tag{3}$$

where, $E_{Rx\text{-}elec}(q)$ is the energy consumption of receiving q bits of data.

The energy consumed $E_{DA}(q)$ of a node to fuse q bits of data is:

$$E_{DA}(q) = E_{fu} \times q \tag{4}$$

where, E_{fu} is the energy consumption of 1 bit data fusion.

3 Model of Trust Evaluation and Intrusion Detection

All sensor nodes in WSNs have limited energy and may be attacked and become malicious nodes. The base station has unlimited energy and can not be attacked, so the trust value of all nodes is calculated by the base station. Intrusion detection adopts a three-level structure, that is, the base station is responsible for detecting the attack of the cluster head, and the cluster head is responsible for detecting and monitoring the attack of the member nodes in the cluster.

3.1 Model of Trust Value Evaluation

TIDM-DTE model calculates and monitors the data trust, communication trust and energy consumption trust of sensor nodes.

3.1.1 Data Trust

When nodes in WSNs are subjected to insider attacks, it is common to experience continuous packet loss. Normal nodes, in general, are unlikely to experience sequential packet loss naturally. Therefore, continuous packet loss can be used as one of the characteristics of intrusion detection, and the malicious nodes that receive internal attacks can be monitored and isolated by observing the continuous packet loss rate [17,23]. If it is normal for continuous packet loss and isolation network node, trust TIDM-DTE model design recovery mechanism will also avoid the effects of false alarm.

The trust model measures the trustworthiness of the monitored nodes based on the data collected in the previous phase. When a node is observed to forward a packet s times and drop a packet f times, the Beta trust model will assign a trust value $D_{j\_beta}(s,f)$ to node j according to the following formula:

$$D_{j\_beta}(s,f) = E[bata(p|s+1,f+1)] = \frac{s+1}{s+f+2} \tag{5}$$

where, $E[beta(P|s+1,f+1)]$ is the expectation of the probability density function of the beta distribution given s and f.

When a failure occurs, each trust model decreases the trust value by a certain amount. A penalty function $PD_j(n)$ is included in the data trust model, which determines how much the trust value should be reduced at a node that produces n consecutive failures. Using $PD_j(n)$, given the number of n consecutive failures, the new trust function $D_j(n)$ is expressed as follows:

$$D_j(n) = D_j(0) - PD_j(n) \tag{6}$$

where, $D_j(0)$ is the initial trust value of the evaluation node that produces n consecutive failures at the evaluation node, which is the expected value of $P(s)$ at $n = 0$ in the Beta trust model.

Therefore, when an evaluated node generates n consecutive failures ($n \geq 1$), we measure its trust value by using $D_j(n)$ by subtracting a certain amount of penalty $PD_j(n)$ from $D_j(0)$ before generating n consecutive failures.

$$P[f] = 1 - D_j(0) \tag{7}$$

where, $P[f]$ is the probability that a packet is dropped at a normally functioning node.

Let:

$$PD_j(n) = P[f]\,PD_j(n-1) + \alpha n = \alpha \sum_{i=1}^{n} \frac{1-P[f]^i}{1-P[f]} = D_j(n) - D_j(n-1) \tag{8}$$

where, α is the punishment for a failure.

$$D_j(n) = D_j(n-1) - PD_j(n) \tag{9}$$

$$PD_j(n) = \sum_{i=1}^{n} \frac{(n-i+1)\times\alpha\times\left(1-P[f]^i\right)}{1-P[f]} \tag{10}$$

$$PD_j(n) - PD_j(n-1) = \alpha \sum_{i=1}^{n} \frac{1-P[f]^i}{1-P[f]} \tag{11}$$

$$PD_j(n) = \sum_{i=1}^{n} \frac{(n-i+1)\times\alpha\times\left(1-P[f]^i\right)}{1-P[f]} \tag{12}$$

where, $PD_j(n)$ is a penalty function which determines how much we should lower the trust value of a node that generates n consecutive failures.

The data trust $D_j(n)$ of the node j is as follows:

$$D_j(n) = D_j(0) - \sum_{i=1}^{n} \frac{(n-i+1) \times \alpha \times \left(1 - P[f]^i\right)}{1 - P[f]} \tag{13}$$

3.1.2 Communication Trust

Communication trust is the most basic factor to verify the credibility of sensor nodes in trust evaluation, which can be used to detect black hole attacks and selective forwarding attacks [24]. The communication trust of a node reflects its packet forwarding behavior with its neighbors, and each node can calculate the trust value of its neighbors independently.

Then, the communication trust $C_j^i(t)$ of node j computed by node i can be obtained by the forwarding trust value $F_j^i(t)$ and the recommendation trust value $R_j^i(t)$.

$$C_j^i(t) = \tau \times F_j^i(t) + (1-\tau) \times R_j^i(t) \tag{14}$$

where, $C_j^i(t) \in [0,1]$, and τ is the weight of forwarding trust.

$$\tau = \frac{I_t(i,j)}{I_t(i,j) + M_t(i,j)} \tag{15}$$

where, $I_t(i,j)$ is the number of packets of node i forwarded by node j, and $M_t(i,j)$ is the average of the total number of packets forwarded by node j except the packets of node i.

$$M_t(i,j) = \frac{\sum_{x \in X_j - i} \left[R_i^x(t) \times I_t(i,j)\right]}{\left|X_j\right| - 1} \tag{16}$$

where, X_j is a collection of a set of nodes communicating with the node j.

3.1.3 Energy Consumption Trust

Sybil attack and other internal attacks usually start after the network has been running for a period of time, and the intruder node usually needs to consume more energy than the normal node to launch the attack, or drastically reduce the energy consumption to ensure the energy required for the attack. Therefore, the energy consumption rate of the node under internal attack will be different from that of the normal node, which is a kind of attack with energy consumption sensitive characteristics. This can be considered as a factor in the direct trust evaluation of the cluster head to the node [25,26].

Calculation of Energy Consumption Trust of the Cluster Heads

The calculation process of the energy consumption trust of the cluster head by the base station is as follows: by collecting the residual energy values of the cluster head connected to the base station in the current cycle and the previous cycle, the energy consumption rate ΔE_j of the cluster head j in this cycle is calculated. And by comparing the average energy consumption rate in the same area to see whether meet the average energy consumption rate equation, the results into the energy consumption of trust trust update equation node energy consumption.

Suppose that the residual energy E_{res_j} of any cluster head j connected to the base station in a certain trust update cycle is as follows:

$$E_{res\_j} = E_{init} - E_{Sx\_j} - E_{Rx\_j} \tag{17}$$

where, E_{init} represents the initial energy of the cluster head, and the residual energy of the cluster head can be calculated from the energy consumption E_{Sx_j} of sending data and E_{Rx_j} of receiving data.

The base station can calculate the energy consumption rate ΔE_{j_now} at this time by using the residual energy of the cluster head at the current time t_{now} and the residual energy of the last time t_1:

$$\Delta E_{j\_now} = \frac{\left[E_{res\_j}(t_1) - E_{res\_j}(t_{now})\right]}{\Delta t} \tag{18}$$

Using this equation, the energy consumption rate of all nodes connected to the base station can be calculated.

Let $N(j)$ denote the set of neighbor nodes of any cluster head j, then the number of neighbor nodes is $|N(j)|$, and the average energy consumption rate $\Delta E_{j\_avg}(t_{now})$ of its neighbor nodes at the current time t_{now} is calculated by the following Eq. (19):

$$\Delta E_{j\_avg}(t_{now}) = \frac{\sum_{i=1}^{|N(j)|} \Delta E_j}{|N(j)|} \tag{19}$$

In practical applications, the cluster head and its neighbor nodes are adjacent in geographical location and similar in sensing data and functional structure, so there is a similarity in their energy consumption rate. Therefore, the deviation degree of energy consumption rate d_{j_E} is defined to represent the deviation degree of energy consumption rate of node j from the average energy consumption rate of its neighbor nodes. The base station node checks whether the difference between the energy consumption rate E_j of the cluster head and the average energy consumption rate of its neighbor nodes is greater than the deviation degree d_{j_E}.

$$d_{j\_E} = \frac{l\varepsilon_{fs} Dist_{ch\_j}}{\Delta t} \tag{20}$$

$$\Delta E_{j\_avg}(t_{now}) - d_{j\_E} \le E_j \le \Delta E_{j\_avg}(t_{now}) + d_{j\_E} \tag{21}$$

where, $Dist_{ch\_j}$ is the square of the difference between the intra-cluster radius and node j distance, and l is the number of data packets sent.

When its energy consumption rate satisfies Eq. (21), it is recorded as the success of primary energy consumption and is included in the success queue. The direct energy consumption trust of the base station to the cluster head is calculated as follows [27]:

$$E_j(\Delta t) = \left[\frac{S_j(\Delta t)}{S_j(\Delta t) + U_j(\Delta t)} \cdot \frac{1}{\sqrt{U_j(\Delta t)}}\right] \tag{22}$$

where, Δt represents unit time, $S_j(\Delta t)$ represents the number of times that the current trust cycle energy consumption rate satisfies Eq. (21), $U_j(\Delta t)$ is the number of times that it does not satisfy, the value range of $ET_j(\Delta t)$ is $[0, 1]$, and $1/\sqrt{U_j(\Delta t)}$ is the energy consumption trust inhibitory factor.

Through similar queue data structure to store the deviation of the number of node energy consumption rate, the new data into at the same time remove the history data, by adjusting the length of queue can get different period of the energy consumption of cluster heads to trust. In Eq. (22), $1/\sqrt{U_j(\Delta t)}$ is the energy consumption trust inhibitory factor, which can quickly reduce the energy consumption trust of cluster heads that do not satisfy the trust equation in a short time to 0.

Calculation of Energy Consumption Trust of Normal Node

Cluster heads to the next layer of cluster heads attached to it by normal node calculation process of trust and the base station energy consumption calculation of cluster heads trust values of energy consumption of the process is similar. The cluster head calculates the energy consumption rate ΔE of the node in the current cycle by collecting the residual energy values of the cluster member nodes in the current cycle and the previous cycle. The energy consumption trust $ET_k(\Delta t)$ of member k in the cluster was calculated by the above Eqs. (17)–(22).

3.2 Model of Trust Value Prediction

In view of the complexity and variability of network environment, attack behavior and other factors, in order to quickly reduce the trust of malicious nodes, it is necessary to improve the accuracy of trust evaluation and the detection speed of malicious nodes [18]. Grey theory is good at nonlinear evaluation, especially suitable for predicting uncertain systems with small samples and poor information [28]. Using grey theory to evaluate the trust value of nodes has the advantages of less processing samples, less calculation, fuzzy data, random dynamic changes, and high prediction accuracy. However, node reputation may be affected by external factors, resulting in large random volatility, diversity of changing trends, complexity and other issues. Therefore, the state transition matrix of Markov theory is used to improve the evaluation results of grey model.

In this research, the grey Markov model is used to predict the data trust, communication trust and energy consumption trust of WSNs nodes. The prediction process of node dynamic trust value based on grey Markov model is shown in Fig. 2, and the following is the prediction process and specific algorithm of data trust.

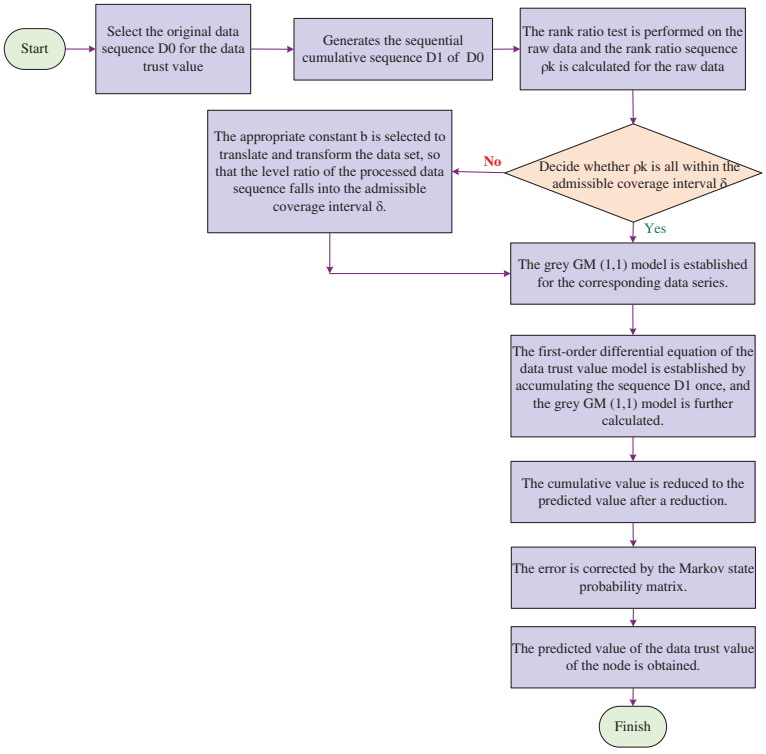

Figure 2: Prediction process of node dynamic trust value based on grey Markov model

The original data sequence of the data trust is selected, denoted as $D_0 = \{d_{0,1}, d_{0,2}, \ldots, d_{0,n}\}$, and the sequential accumulation sequence $D_1 = \{d_{1,1}, d_{1,2}, \ldots, d_{1,n}\}$ of D_0 is generated.

$$d_{1,k} = \sum_{i=1}^{k} d_{0,i} \left(k = 1, 2, \ldots, n\right) \tag{23}$$

where, n is the number of samples.

To test the level ratio of the original data, first calculate the level ratio sequence ρ_k of the original data:

$$\rho_k = \frac{d_{0,k-1}}{d_{0,k}} \tag{24}$$

Then determine whether ρ_k is all within the admissible coverage interval $\delta = \left(e^{-2/(n+1)}, e^{2/(n+1)}\right)$. If so, the grey $GM(1,1)$ model can be established for the corresponding data sequence. Otherwise, the appropriate constant b should be selected to translate and transform this group of data, so that the level ratio of the processed data sequence $Y_0 = \{y_{0,1}, y_{0,2}, \ldots, y_{0,n}\}$ falls into the admissible coverage interval, and the translation and transformation process is as follows:

$$y_{0,k} = d_{0,k} + b \tag{25}$$

By accumulating sequence D_1 once, the first-order differential equation of data trust $GM(1,1)$ model is established as follows:

$$\frac{dD_1}{dt} + \alpha D_1 = q \tag{26}$$

where, α and q are development coefficient and grey action, respectively.

Let $a = (\alpha, q)^T$, using the least squares method, solve α and q as follows:

$$a = (\alpha, q)^T = \left(B^T B\right)^{-1} B^T D \tag{27}$$

where, $B = \begin{bmatrix} -0.5d_{1,1} & \mathrm{L} & 1 \\ \mathrm{M} & \mathrm{O} & \mathrm{M} \\ -0.5d_{1,n-1} & \mathrm{L} & 1 \end{bmatrix}$ and $D = \begin{bmatrix} d_{0,2} \\ \mathrm{M} \\ d_{0,n} \end{bmatrix}$.

According to Eqs. (26) and (27), the grey $GM(1,1)$ model is obtained as follows:

$$\hat{d}_{1,k+1} = \left(d_{0,1} - q/\alpha\right) e^{-\alpha k} + q/\alpha \tag{28}$$

The cumulative value $\hat{d}_{1,k+1}$ is subtracted once and restored to the predicted value $\hat{d}_{0,k+1}$:

$$\hat{d}_{0,k+1} = \hat{d}_{1,k+1} - \hat{d}_{1,k} \tag{29}$$

Then, in view of the limitations of the grey model, the error of the Markov state probability matrix is corrected [29,30].

The steps are as follows:

Step 1: According to the maximum value $e_{\max}$ and minimum value $e_{\min}$ in the trust residual sequence $\hat{E}(t) = \{e(t_1), e(t_2), \ldots, e(t_{n-1})\}$ of historical data, the sequence is divided into several state intervals.

Step 2: The state transition probability is established. According to the state of $e\left(t_k\right)$ $(k = 1, 2, \ldots, n-1)$, the transition probability between $e\left(t_k\right)$ states is calculated through the statistics of the state change of $e\left(t_k\right)$ at the adjacent time, and the state transition matrix is established.

Step 3: Calculate the predicted value, according to the state of $e\left(t_{n-1}\right)$ at the current time, combined with the state transition probability matrix to judge the most likely state of residual $e\left(t_n\right)$ at n time, the middle value of the state interval is taken as the value of $e\left(t_n\right)$, and the risk value at n time predicted by $GM\left(1,1\right)$ model is corrected. The predicted value $\hat{d}'\left(t_n\right)$ of the node data trust of the Grey Markov model at n time is obtained.

$$\hat{d}'\left(t_n\right) = \hat{d}\left(t_n\right) - e\left(t_n\right) \tag{30}$$

Through the above steps, the predicted value of the data trust of the node can be obtained. The communication trust and energy consumption trust are also calculated through the above steps to obtain the dynamic prediction value.

3.3 Data Noise Detection

DBSCAN algorithm is a density-based clustering method. The advantages of DBSCAN are that it can find categories of arbitrary shapes, has strong noise immunity, and only needs to scan the dataset once to complete clustering [12]. The basic idea of density-based clustering method is: for any data object in the same cluster, the data object is taken as the center of the circle, a radius (*Minpts*) is given to limit a region, and the region must contain at least the minimum number of data objects (*Eps*). In this research, DBSCAN algorithm is used to detect the data noise point of the trust value of the node to realize the network-based intrusion detection function. The intrusion detection process based on DBSCDN model is shown in Fig. 3.

The steps of intrusion detection using DBSCAN model in WSNs are as follows [31]:

Step 1: The data trust, communication trust and energy consumption trust of network nodes form a three-dimensional sample space, calculate the Euclidean distance between sample point x_i and other sample points x_j, and sort the distance set $\left\{j = 1, \ldots, n\left(j \neq i\right) | d_{ij}\right\}$ from large to small to obtain a new distance set $\left\{1 \leq m \leq \left(n-1\right) | d_m\right\}$.

Step 2: Use the new distance set $\left\{1 \leq m \leq \left(n-1\right) | d_m\right\}$ to fit the curve based on the least square method to generate a cubic equation, calculate the inflection point radius r_i of the sample point x_i and the number of sample points n_i by taking the second derivative of the cubic equation, and then calculate the corresponding density ρ of the sample point.

Step 3: Loop Step 1–Step 2, traverse each sample point of the data set, calculate the corresponding density ρ of each sample point, and form the density set *densitydata*.

Step 4: The density ρ of each sample point in *densitydata* set was arranged in order of size, and a cubic equation was generated based on the least square curve fitting method. The bump D of the curve was calculated by taking the first derivative of the cubic equation.

Step 5: Using convex point D corresponding radius and the sample points as *Eps* and *MinPts* parameters in DBSCAN clustering.

Step 6: Check the unchecked sample points in the data set x_i, and if they have not been processed, check their neighborhood. If the number of objects contained in the neighborhood is not less than the minimum number of included points *MinPts*, a new cluster C_i is established, and all the sample points x_i are assigned to the candidate set N. Otherwise, x_i is marked as a noise point.

Step 7: For all the unprocessed sample points x_i in the candidate set N, check the neighborhood of sample point x_i. If it contains at least *MinPts* sample points, add these sample points x_i to the candidate set N.

Step 8: If sample point x_i is not assigned to any cluster, then assign sample point x_i to C_i.

Step 9: Repeat Step 7 and Step 8, continuing to check unprocessed objects in the candidate set N until the candidate set N is an empty set.

Step 10: Repeat Step 6 to Step 9 until all samples are assigned to a cluster or labeled as noise, thus completing the detection of malicious nodes in the network.

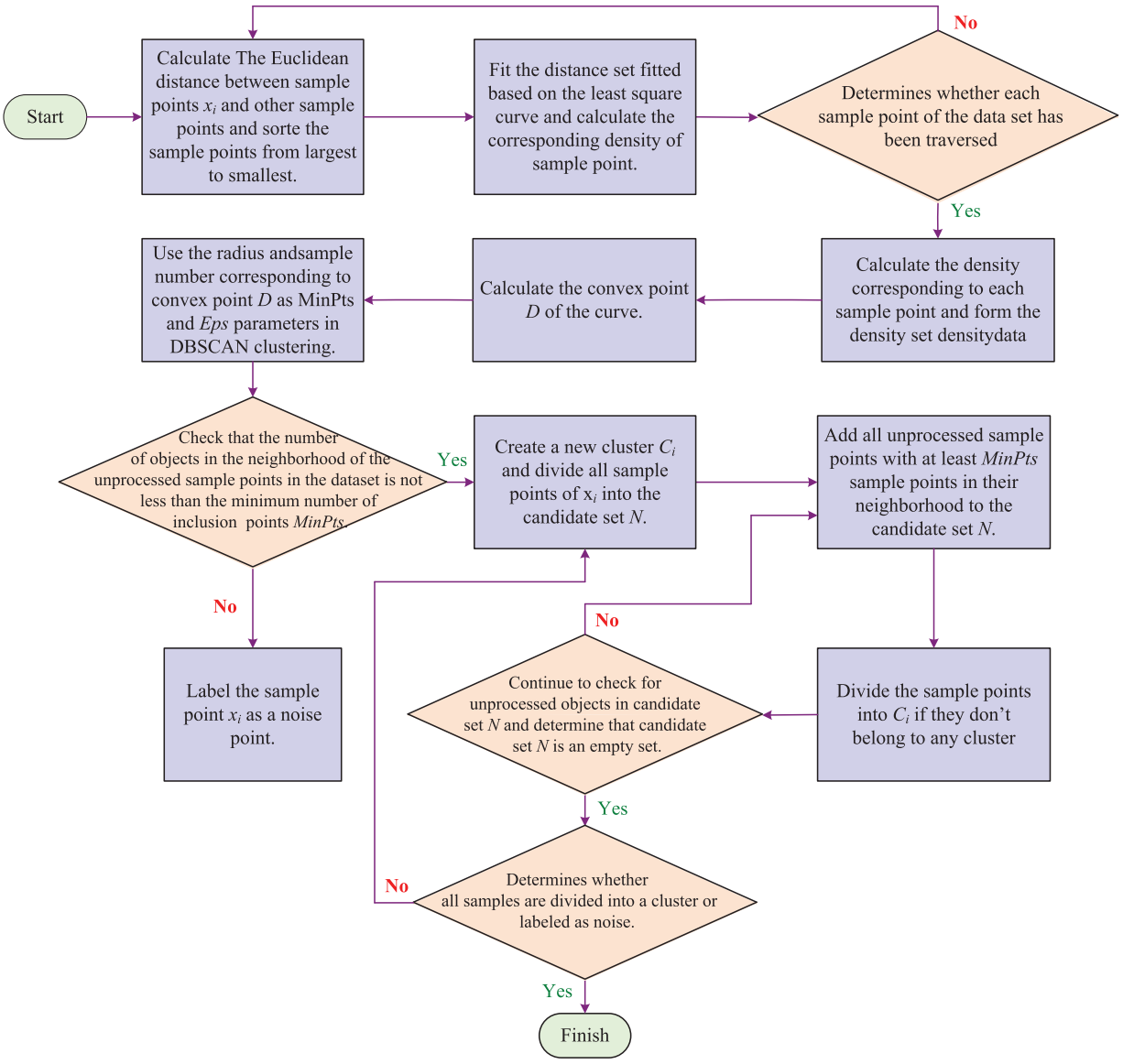

Figure 3: Intrusion detection process based on DBSCDN model

3.4 Trust Recovery Mechanism

During the normal operation of sensor nodes, temporary failures may occur, leading to misclassification as malicious nodes and reduced credibility. For example, network congestion can cause repeated transmission failures of node data packets. To address this issue, a trust recovery mechanism is employed to restore the trust of temporarily faulty nodes, enhancing the performance of the intrusion detection mechanism and reducing False Alarm Rate [19,32].

When a wireless sensor node is initially flagged as a suspected malicious node, it is not immediately identified as malicious or isolated from the network. Instead, the TIDM-DTE model uses a trust recovery mechanism to reintegrate the node into the normal node set for further evaluation. A node is only finally classified as malicious and isolated from the network if it is repeatedly identified as a suspected malicious node three consecutive times.

The TIDM-DTE model achieves a lower False Alarm Rate and higher Detection Rate by having trusted sensor nodes review suspicious nodes and reinstate normal nodes through the recovery mechanism.

3.5 Three-Level Intrusion Detection Model Based on Trust Evaluation

Because only the base station is trustworthy, and the base station resources are not limited. Therefore, the intrusion detection of sensor nodes is carried out at the base station. The anomaly detection algorithm model based on TIDM-DTE model is shown in Fig. 4.

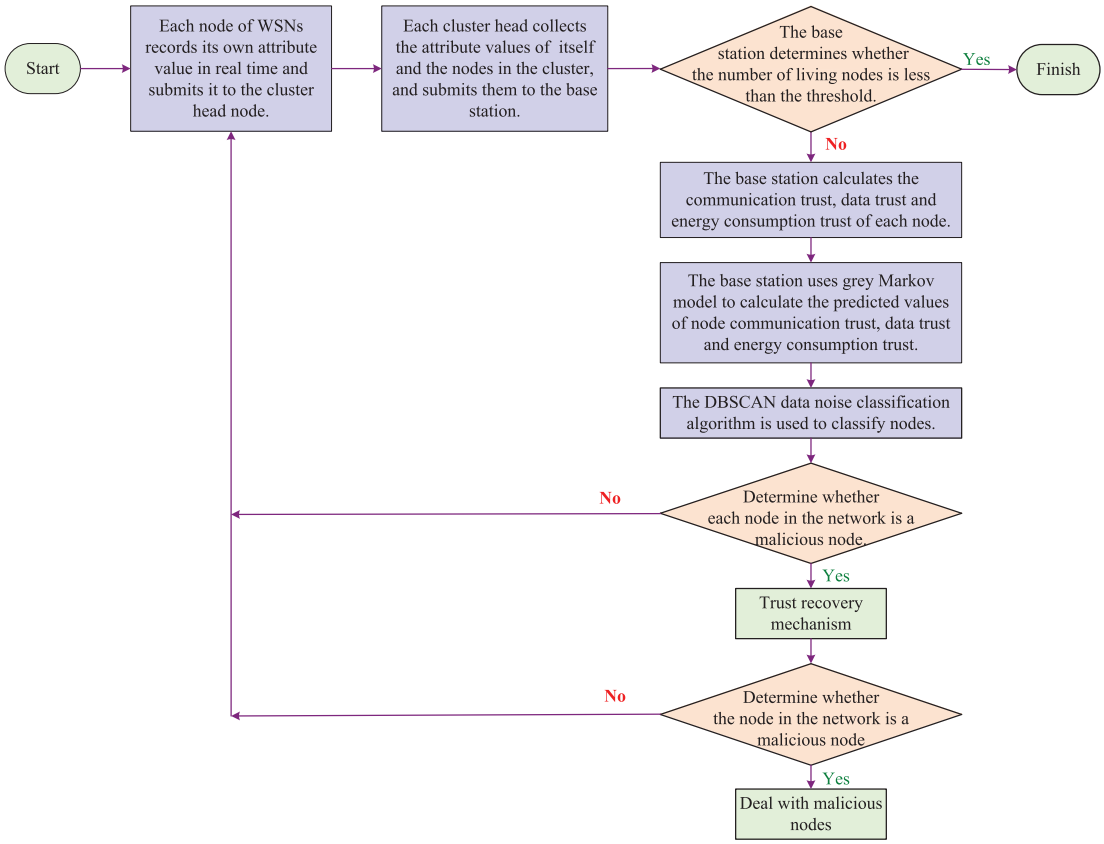

Figure 4: TIDM-DTE intrusion detection model

The overall steps of intrusion detection are as follows:

Step 1: The member node records its own specific attribute value and submits it to the cluster head node to enter step 2.

Step 2: Each cluster head summarizes the attribute values of cluster head nodes and submits them to the base station to enter step 3.

Step 3: The base station determines whether the number of surviving nodes is less than the threshold: (1) If it is not less than the threshold, enter step 4; (2) If it is less than the threshold, the network operation is terminated.

Step 4: The base station calculates the communication trust, data trust, and energy consumption trust of each node and enters step 5.

Step 5: The base station uses the Grey Markov model to calculate the predicted values of communication trust, data trust, and energy consumption trust, and enter step 6.

Step 6: DBSCAN algorithm is used to detect the data noise of the trust of the node and enter step 7.

Step 7: To determine whether the node is a malicious node: (1) If a node is judged as safty, enter step 1; (2) If the node is judged as malicious, enter step 8.

Step 8: Through the trust recovery mechanism, the characteristics of the suspected malicious nodes were further analyzed: (1) If a node is judged as safty, enter step 1; (2) If a malicious node is judged, the base station broadcasts the number of the malicious node throughout the network before the start of the new round of setup phase, and isolates the malicious node from the network.

The network stops operating when the number of surviving nodes is not enough to maintain the normal operation of the network.

4 Experiment and Results

Experiment using Python3.8 for this TIDM-DTE model and reference [16] proposed FIBTM model (trust attack fast identification based on trust model), proposed by reference [18] FSEPM model (dynamic trust evaluation model integrating fuzzy comprehensive evaluation mechanism and similarity measure theory) for simulation comparison.

In the simulation experiment of the TIDM-DTE model, the networkx library is used to construct the topology of the wireless sensor network, simulate the communication connection and data transmission in the network, and the topological characteristics such as the degree and the shortest path of nodes can be conveniently calculated. The core computing logic is implemented based on NumPy. Communication trust is calculated through the interaction history of nodes. Data trust is based on the statistics of continuous packet loss rate. Energy consumption trust is evaluated according to the energy consumption pattern of nodes. The dynamic trust prediction based on the grey Markov model is implemented by combining the NumPy and SciPy libraries. The DBSCAN algorithm of the scikit-learn library is invoked to achieve the identification of malicious nodes. These models have constructed a complete three-level detection architecture through the vectorization calculation of NumPy, the optimization solution of SciPy, and the clustering algorithm of scikit-learn, combined with the networkx library, achieving efficient detection of various attack types.

100 nodes are randomly deployed in a 100 m × 100 m area, and the base station is set in the middle position of the edge, and malicious nodes are proportionally designed in the network to randomly launch selective attacks. There are many different types of attacks in WSNs. In this paper, selective forwarding attack, Sybil attack, on-off attack and black hole attack are selected as the simulation objects to verify and analyze the performance of three intrusion detection models: TIDM-DTE, FIBTM and FSEPM. The simulation

parameters are set in Table 1 [3,16–19]. Fig. 5 shows the initial network topology of the wireless sensor network. In Fig. 5, the blue dots represent normal nodes, the red dots represent malicious nodes, and the green square dots represent base stations.

Table 1: Setting of simulation parameters

Name of parameter	Value of parameter
Area	100 m × 100 m
Number of nodes K	100
Initial energy of nodes E_{init}	1 J
Initial trust value	0.5
Data fusion rate	0.5
The energy consumption of the transceiver data circuit E_{elec}	50 nJ/bit
Power amplification parameters in multipath attenuation propagation ε_{amp}	0.001 J/(bit · m^4)
Free space propagation medium power amplification parameters ε_{fs}	10 pJ/(bit · m^2)
Energy consumption for fusing 1 bit of data E_{fu}	5 nJ/bit
Free space maximum transmission distance $d_{\max}$	50 m

Note: m represents the unit meter, J represents the unit joule, and bit represents 1 bit of data.

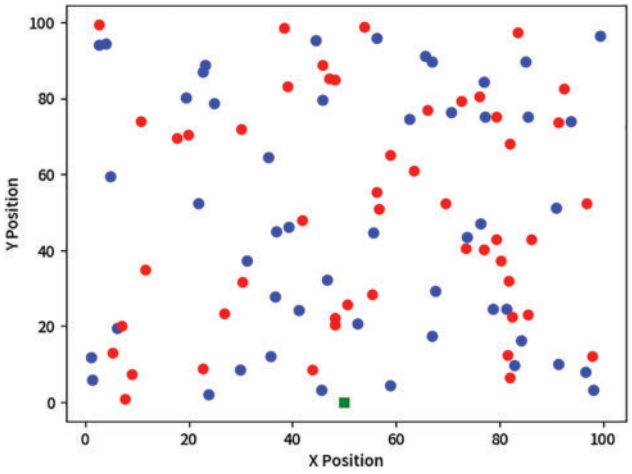

Figure 5: Initial network topology of the wireless sensor network

4.1 Parameters of Performance in Experiment

The Detection Rate refers to the proportion of intrusion detection system (IDS) that can correctly identify and report the actual intrusion attacks. It reflects the sensitivity and ability of the system to identify intrusions.

$$Detection\ rate = \frac{Number_{decected\_correct}}{Number_{\text{intrusion\_all}}} \tag{31}$$

where, $Number_{decected\_correct}$ is the number of correctly detected intrusion attacks and $Number_{\text{intrusion\_all}}$ is the total number of actual intrusion attacks.

The False Alarm Rate refers to the proportion of normal network activities or harmless events that the intrusion detection system incorrectly identifies as intrusion attacks, and it reflects the False Alarm Rate of the system.

$$False\ alarm\ rate = \frac{Number_{decected\_false}}{Number_{\det ected\_all}} \tag{32}$$

where, $Number_{decected\_false}$ is the number of false alarms and $Number_{\det ected\_all}$ is the total number of intrusion attacks marked by the system.

The Detection Accuracy Rate refers to the proportion of records that are actually intrusion attacks among the records marked as intrusion attacks by the system. It reflects the accuracy of the system's detection.

$$Accuracy\ rate = \frac{Number_{decected\_correct}}{Number_{\det ected\_all}} \tag{33}$$

where, $Number_{accuracy}$ is the number of intrusion attacks correctly detected, and $Number_{\det ected\_all}$ is the total number of intrusion attacks marked by the system.

4.2 Detection Speed of Network Intrusion Detection Model

The detection speed of network intrusion detection models is closely tied to minimizing attacker-induced network damage. Fig. 6 illustrates the variation in average Detection Rate of malicious nodes across iteration rounds for TIDM-DTE, FIBTM, and FSEPM. Compared with FIBTM and FSEPM, the TIDM-DTE model employs a data trust model based on continuous packet loss rate observation and dynamic trust prediction via the Grey Markov model. This enables TIDM-DTE to identify malicious nodes more rapidly at the onset of intrusion detection.

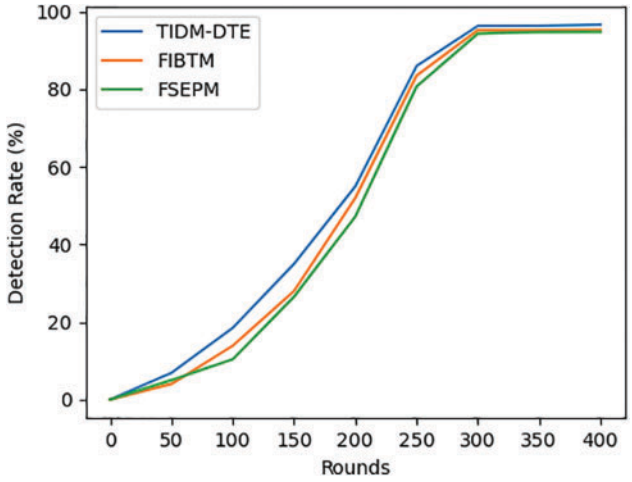

Figure 6: Comparison of detection speed of three different intrusion detection models

The simulation results in Fig. 6 demonstrate that TIDM-DTE's Detection Rate rises rapidly and stabilizes at a superior level, validating its capability to enhance the early-stage detection performance of network intrusion detection models.

4.3 Detection Rate, False Alarm Rate and Detection Accuracy Rate of Network Intrusion Detection Model

In network intrusion detection, Detection Rate, False Alarm Rate, and Detection Accuracy Rate are interrelated yet distinct performance metrics. A high Detection Rate aids in timely intrusion detection but may be accompanied by a high False Alarm Rate. A low False Alarm Rate reduces false positives but may compromise Detection Rate to some extent. By contrast, a high Detection Accuracy Rate aims to maximize the inclusion of actual intrusions among records flagged as intrusions. This study evaluates the performance of three intrusion detection models—TIDM-DTE, FIBTM, and FSEPM—by analyzing Detection Rate, False Alarm Rate, and Detection Accuracy Rate under varying proportions of malicious nodes, as depicted in Fig. 7.

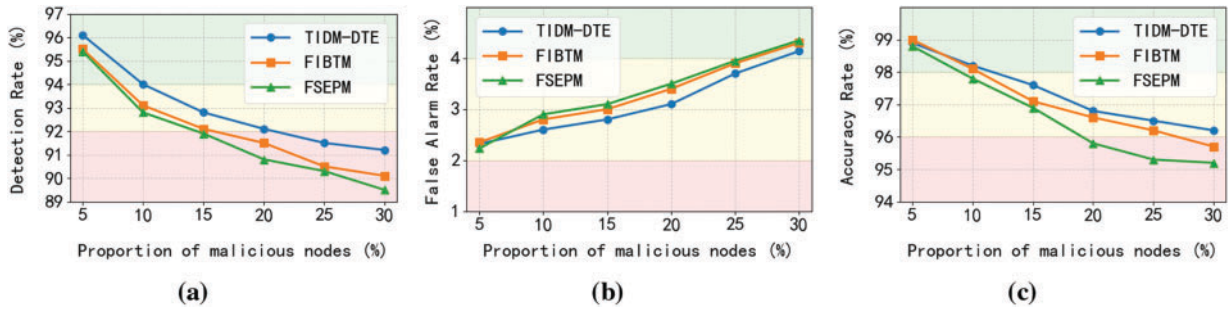

Figure 7: Performance comparison of intrusion detection models. (**a**) detection rate comparison under varying proportions of malicious nodes. (**b**) false alarm rate comparison under varying proportions of malicious nodes. (**c**) detection accuracy comparison under varying proportions of malicious nodes

Fig. 7 shows that as the proportion of malicious nodes increases, the Detection Rate and Detection Accuracy Rate of all three methods decline to some degree, while their False Alarm Rate increase. FIBTM and FSEPM rely on fused node trust values for judgment, but the inherent difficulty in increasing trust values (combined with their tendency to decrease) hinders the speed of node attribute determination. In contrast, the TIDM-DTE model uses data noise classification technology to identify malicious nodes, achieving superior detection performance. Notably, FIBTM lacks dynamic trust value prediction and perception, leading to significantly poorer performance compared to TIDM-DTE and FSEPM. These results demonstrate TIDM-DTE's robust attack detection capability.

4.4 Detection Rate of Different Types of Attacks

Different types of attacks induce distinct changes in sensor node parameters within WSNs. A selective forwarding attacker deliberately drops data packets, reducing inter-node data transmission reliability and increasing packet loss rates. Nodes must retransmit lost packets, thereby escalating network communication delays and energy consumption. A Sybil attacker forges multiple identities, confusing network node authentication and causing excessive consumption of resources like bandwidth and power. An on-off attacker disrupts network connectivity by manipulating node switch states, halting data transmission and degrading overall network performance. A black hole attacker masquerades as a high-energy or high-trust node to attract and intercept data, leading to data loss and network resource waste. Fig. 8 illustrates the Detection Rate comparison of three intrusion detection models against the four network attack types described above.

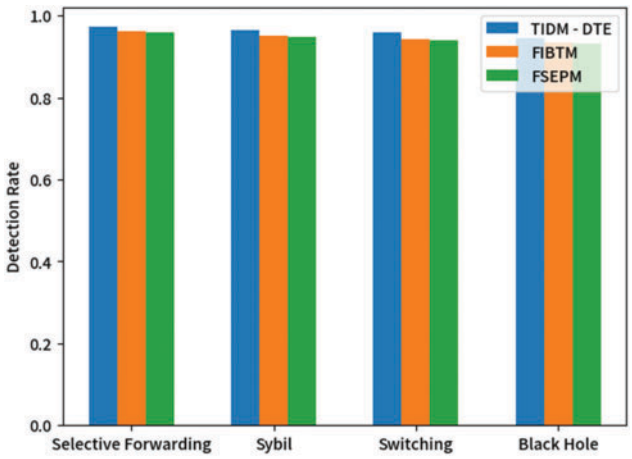

Figure 8: Detection rate comparison of three intrusion detection models for different attack types

As shown in Fig. 8, the TIDM-DTE model demonstrates significantly higher detection rates than FIBTM and FSEPM across four typical attacks: selective forwarding, Sybil, on-off, and black hole attacks. The communication trust mechanism in TIDM-DTE effectively detects black hole and selective forwarding attacks. Attacks such as selective forwarding and Sybil cause continuous packet loss, which the TIDM-DTE model's data trust calculation monitors through continuous packet loss observation, significantly enhancing detection effectiveness for these attacks. Moreover, selective forwarding, Sybil, and black hole attacks notably impact wireless sensor node energy consumption, enabling TIDM-DTE to detect them by tracking node energy changes. In contrast, FIBTM and FSEPM rely solely on Beta distribution for node trust calculation, resulting in insufficiently comprehensive monitoring and evaluation—and consequently lower intrusion detection performance. Therefore, TIDM-DTE can rapidly and accurately identify various malicious nodes, isolate them across the network, minimize network losses, and ensure reliable data transmission.

4.5 Effect of Trust Recovery Mechanism

The False Alarm Rate serves as a critical performance metric in network intrusion detection systems. Excessively elevated False Alarm Rate generate excessive non-critical alerts, compromising both the reliability and practical utility of detection outcomes. This study proposes a trust recovery mechanism to mitigate False Alarm Rate in intrusion detection processes. Through 20 experimental trials, we evaluated system performance using three key metrics: average Detection Rate, average False Alarm Rate, and average Detection Accuracy Rate. Comparative analysis between the detection results from the trust recovery mechanism vs. those from a baseline system demonstrated the effectiveness of our approach. Fig. 9 illustrates these findings, with simulation parameters configured at a 25% malicious node density.

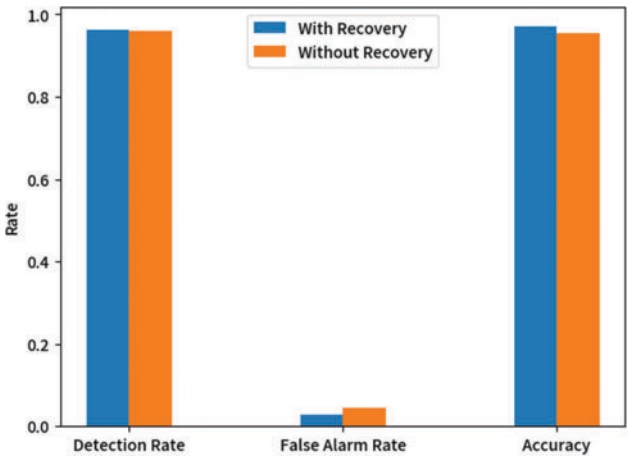

Figure 9: Impact of trust recovery mechanism on network intrusion detection model performance

The experimental results in Fig. 9 show that deploying the trust recovery mechanism achieves higher detection accuracy and lower False Alarm Rate. This indicates the mechanism can reinstate communication functions for normal nodes misclassified as malicious. The reduction in False Alarm Rate and improvement in overall detection accuracy validate the trust recovery mechanism's feasibility.

5 Conclusions

By innovatively introducing a dynamic trust evaluation mechanism, this study analyzes the impact of different attacks on node trust and constructs trust models for data, communication, and energy consumption, fully considering node status. The grey Markov model dynamically predicts node trust values to sensitively reflect trust changes under attacks. The TIDM-DTE model, leveraging DBSCAN technology, enhances intrusion detection against malicious attacks—particularly insider threats in WSNs. Experimental results confirm TIDM-DTE's effectiveness in improving detection accuracy, reducing False Alarm Rate, and optimizing resource utilization. This research contributes a novel theoretical framework to WSNs security and provides robust practical support for real-world security implementations.

TIDM-DTE's reliance on multi-dimensional trust models and technologies like the grey Markov model and DBSCAN introduces computational complexity, especially in large-scale networks where node growth amplifies calculation demands. Multi-model establishment and complex detection techniques may also increase energy consumption from data processing. While TIDM-DTE demonstrates versatility across attack types and theoretical scalability to new threats, expanding WSNs scale and topological complexity pose challenges—such as surging trust model computations and degraded detection accuracy/timeliness—that may limit scalability.

Facing evolving security challenges, future work will focus on:

- Integrating machine learning (e.g., deep learning) to enhance complex attack pattern recognition.
- Exploring privacy-protection mechanisms to safeguard node data during intrusion detection.
- Optimizing the model for large-scale, dynamic WSNs to balance generalization with minimized computational complexity.

Acknowledgement: The authors are grateful to all the editors and anonymous reviewers for their comments and suggestions.

Funding Statement: This research was supported by Gansu Provincial Higher Education Teachers' Innovation Fund under Grant 2025A-124, Key Research Project of Gansu University of Political Science and Law under Grant No. GZF2022XZD08 and Soft Science Special Project of Gansu Basic Research Plan under Grant No. 22JR11RA106.

Author Contributions: The authors confirm contribution to the paper as follows: Draft manuscript preparation, design and funding acquisition: Xiaogang Yuan; Supervision and review: Huan Pei and Yanlin Wu. All authors reviewed the results and approved the final version of the manuscript.

Availability of Data and Materials: Not applicable.

Ethics Approval: Not applicable.

Conflicts of Interest: The authors declare no conflicts of interest to report regarding the present study.

References

1. Jiang J, Han G. Survey of trust management mechanism in wireless sensor network. Inf Netw Secur. 2020;20(4):12–20. doi:10.3969/j.issn.1671-1122.2020.04.002.
2. Yang W, Ma X, Wang W. Based on credibility evaluation mechanism of WSN security routing protocol research. High Technol Commun. 2010;20(12):1211–6. doi:10.3772/j.issn.1002-0470.2010.12.001.
3. Pan L, Tao Y, Xu X. A secure clustering routing protocol based on trust and balancing energy consumption. J Beijing Univ Posts Telecommun. 2019;42(3):29–36. doi:10.13190/j.jbupt.2018-158.
4. Fang Y. Research on privacy protection technology of wireless sensor network routing protocol [master's thesis]. Nanjing, China: Nanjing University of Aeronautics and Astronautics; 2020.
5. Liang K, Huang H, Huang X, Yang Q. CS-based homomorphism encryption and trust scheme for underwater acoustic sensor networks. In: The 2020 International Conference on Machine Learning and Big Data Analytics for IoT Security and Privacy; 2020 Nov 6–8; Shanghai, China. p. 394–9.
6. Khah SA, Barati A, Barati H. A dynamic and multi-level key management method in wireless sensor networks (WSNs). Comput Netw. 2023;236(4):109997. doi:10.1016/j.comnet.2023.109997.
7. Priayoheswari B, Kulothungan K, Kannan A. Beta reputation and direct trust model for secure communication in wireless sensor networks. In: Proceedings of the International Conference on Informatics and Analytics; 2016 Aug 25–28; Pondicherry, India. New York, NY, USA: ACM; 2016. p. 1–5. doi:10.1145/2980258.2980413.
8. Zhou Y, Tao Y, Li Z. Feedback trust model for wireless sensor networks based on double cluster heads. Comput Eng. 2021;47(3):174–82. doi:10.19678/j.issn.1000-3428.0057388.
9. Kurdi H, Alfaries A, Al-Anazi A, Alkharji S, Addegaither M, Altoaimy L, et al. A lightweight trust management algorithm based on subjective logic for interconnected cloud computing environments. J Supercomput. 2019;75(7):3534–54. doi:10.1007/s11227-018-2669-y.
10. Liu Y. Trust model based on hierarchical trust management in wireless sensor networks [master's thesis]. Taiyuan, China: Taiyuan University of Technology; 2012. doi:10.7666/d.y2156817.
11. Tong WM, Liang JQ, Lu L, Jin XJ. Intrusion detection scheme based node trust value in WSNs. Syst Eng Electron. 2015;37(7):1644–9. doi:10.3969/j.issn.1001-506X.2015.07.27.
12. Xu L, Li G. Multi-protocol intrusion detection method based on trust mechanism in wireless sensor networks. J Sens Technol. 2019;32(5):739–48.
13. Tahboush M, Agoyi M. A hybrid wormhole attack detection in mobile *ad-hoc* network (MANET). IEEE Access. 2021;9:11872–83. doi:10.1109/access.2021.3051491.
14. Bharti M, Rani S, Singh P. TTSASA: three tier security against Sybil attack. J Algebr Stat. 2022;13(1):62–74.
15. Kagade RB, Jayagopalan S. Optimization assisted deep learning based intrusion detection system in wireless sensor network with two-tier trust evaluation. Int J Netw Mgmt. 2022;32(4):e2196. doi:10.1002/nem.2196.
16. Tao L, Guo Y, Han Y. WSN fast identification trust attack model based on trust. J Jilin Univ (Nat Sci Ed). 2022;60(6):1423–9.

17. Cho Y, Qu G. A hybrid trust model against insider packet drop attacks in wireless sensor networks. Sensors. 2023;23(9):4407. doi:10.3390/s23094407.
18. Teng Z, Li M, Gu J. WSN dynamic trust evaluation prediction model based on multi-index fusion. J Zhengzhou Univ (Eng Sci Ed). 2023;44(3):76–82. doi:10.13705/j.issn.1671-6833.2022.06.014.
19. Li C, Sun Z. IWSN of intrusion detection based on the variation of the properties, the global trust. J Sens Technol. 2023;36(2):294–300. doi:10.3969/j.issn.1004-1699.2023.02.018.
20. Beheshtiasl A, Ghaffari A. Secure and trust-aware routing scheme in wireless sensor networks. Wirel Pers Commun. 2019;107(4):1799–814. doi:10.1007/s11277-019-06357-3.
21. Hu H, Han Y, Yao M, Song X. Trust based secure and energy efficient routing protocol for wireless sensor networks. IEEE Access. 2021;10:10585–96. doi:10.1109/ACCESS.2021.3075959.
22. Gilbert EPK, Kaliaperumal B, Rajsingh EB, Lydia M. Trust based data prediction, aggregation and reconstruction using compressed sensing for clustered wireless sensor networks. Comput Electr Eng. 2018;72:894–909. doi:10.1016/j.compeleceng.2018.01.013.
23. Tian Z, Luo C, Qiu J, Du X, Guizani M. A distributed deep learning system for web attack detection on edge devices. IEEE Trans Ind Inf. 2020;16(3):1963–71. doi:10.1109/TII.2019.2938778.
24. Dang N. Research on trust-based intrusion detection in wireless sensor network [master's thesis]. Qufu, China: Qufu Normal University; 2019.
25. Cao Y. Research on key distribution and Sybil attack detection in wireless sensor networks [master's thesis]. Liaoning, China: Liaoning University; 2023.
26. Cao Y. Sybil attack detection method in WSN based on multiple trust factors. Inf Technol Informatiz. 2023;9:80–6.
27. Daniel DA, Roslin SE. Data validation and integrity verification for trust based data aggregation protocol in WSN. Microprocess Microsyst. 2021;80:103354. doi:10.1016/j.micpro.2020.103354.
28. Ma J, Wu Z, Zou Y, Ren P, Li Q. Water quality prediction of Nansi Lake based on Grey Markov model. Water Resour Prot. 2021;5:153–8. doi:10.3880/j.issn.1004-6933.2021.05.023.
29. Zeng M, Jiang H, Wang X. A reputation evaluation model based on Grey Markov model and its secure routing protocol. Appl Res Comput. 2013;30(12):3758–61,66. doi:10.3969/j.issn.1001-3695.2013.12.062.
30. Zhang Y, Liu C, Liu S, Pan F. 5G network function trust prediction mechanism based on Markov process. J Cyber Secur. 2023;8(4):46–61. doi:10.19363/J.cnki.cn10-1380/tn.2023.07.04.
31. Luo W, Xu C. Multi-step network intrusion detection using improved DBSCAN clustering. Small Microcomput Syst. 2020;41(8):1725–31.
32. Li C. Trust-based intrusion detection model in industrial wireless sensor networks [master's thesis]. Wuxi, China: Jiangnan University; 2023.