Kernel-PCA + RBM Feature Extraction with Optimised Naïve Bayes for Intrusion Detection in Impaired Wireless Sensor Networks

Shengguo Guo*, Dandan Xing
School of Information Engineering, Zhenzhou College of Finance and Economics, Zhengzhou Henan 450000, China
E-mail: guosg@imte.ac.cn

Keywords: network impairment, wireless sensor network, data dimensionality reduction, feature extraction, abnormal intrusion detection, naive bayes

Received: August 14, 2025

The high-dimensional communication data generated by wireless sensor networks often contains substantial redundant and irrelevant information, which hampers the effective retention of critical features. Consequently, the characteristics of network impairment states and abnormal intrusion behaviors become intertwined and difficult to distinguish, ultimately compromising the accuracy of intrusion detection. Therefore, this paper studies the method of abnormal intrusion detection of wireless sensor network communication under network impairment. First, global node perception is achieved through the wireless sensor network networking model to obtain high-dimensional communication data. Second, the kernel principal component analysis (KPCA) method is used to perform nonlinear dimensionality reduction on the data, significantly reducing the data dimension and computational complexity while retaining the key information in the data. Subsequently, a restricted Boltzmann machine (RBM) is introduced to extract the deep features of the dimensionality-reduced data to distinguish the feature differences between network impairment states and abnormal intrusions. Finally, a high-precision abnormal intrusion detection is achieved through an optimized naive Bayes classifier. This classifier effectively improves the anti-interference ability under network impairment states by feature weighting and micro conditional probability optimization, highlights key features, and realizes abnormal intrusion detection. The experiment was conducted on a WSN dataset containing 50000 records, simulating a damaged scenario with a 30% packet loss rate and a 40% bandwidth limitation. The results showed that the proposed method reduced the data dimensionality from 90 to 15 dimensions, with a variance retention rate of 94.7%; In the detection of 10 types of attacks, the F1 value reaches 0.92, which is better than CNN (0.60) and association rules (0.62); At a 75% network damage rate, the false positive rate is only 5%, with accuracy and recall rates of 0.94 and 0.86, respectively, and a single sample prediction time of only 0.21 ms. This method maintains high detection accuracy while having low computational overhead and strong robustness, making it suitable for WSN security protection in complex damaged environments.

Povzetek: Prispevek predstavlja učinkovito metodo zaznavanja vdorov v brezžičnih senzorskih omrežjih z visoko natančnostjo in nizko računsko zahtevnostjo tudi ob okvarah omrežja.

1 Introduction

Wireless sensor networks (WSNs) have been widely applied in key fields such as industrial monitoring, environmental perception, and intelligent transportation due to their advantages [1] of self-organization, low cost, and high flexibility [2]. Abnormal intrusion detection in wireless sensor network communication [3] aims to identify and defend against malicious behaviors such as illegal node access, data tampering, and denial-of-service attacks in real time [4], ensuring the security and reliability of network data transmission [5]. However, in actual application scenarios, the network often faces multiple impairment risks such as channel interference, node failure, and resource constraints [6]. Conducting research on abnormal intrusion detection under network impairment not only concerns the stable operation of the sensor network itself but is also crucial for avoiding serious consequences such as industrial accidents and data leakage [7, 8], having important practical significance for building a solid security defense line for the Internet of Things and promoting the healthy development of the intelligent industry [9].

Many scholars have conducted research on intrusion detection for abnormal communications in wireless sensor networks. For example, Niccolò et al. reconstructed the data packets transmitted by wireless

sensor nodes through an autoencoder, identified abnormal traffic based on the reconstruction error, and achieved the detection of unknown intrusions [10]. However, the performance of autoencoders heavily depends on the reconstruction mode of normal traffic. Under network damage, abnormal traffic generated by channel interference or node failure may have reconstruction errors that are highly similar to malicious intrusion behavior, making it difficult for the model to effectively distinguish at the feature representation level, resulting in poor detection performance. Karrothu et al. adopted an end-cloud-fog detection structure. They collected sensor data at the endpoint layer and transmitted it. The data of the wireless sensor network was transformed at the cloud computing layer through the Yeo-Johnson transform, and feature selection was carried out with the Kulczynski similarity. Then, the selected features were sent to an ensemble classifier optimized by the GDO (Gazelle-Dog) algorithm, and intrusion detection was completed using the ensemble classifier at the fog computing layer [11]. However, the Kulczynski similarity relies on the statistical relationship between data for feature screening. When a new attack pattern or environmental mutation occurs in the wireless sensor network, the relationship between data features changes, and the existing similarity calculation may misjudge the importance of features, thus missing key abnormal features and reducing the detection accuracy. Arkan et al. combined the wireless sensor network with the software-defined network by constructing a software-defined wireless sensor network architecture (SDWSN). The sensor runs an unsupervised intrusion detection algorithm module locally, clusters and analyzes the data based on entropy and cumulative point similarity, and sends the results to the SDWSN controller. The controller comprehensively analyzes the data analysis results of each region to determine whether the data is abnormal and complete abnormal intrusion detection [12]. However, in the case of network damage, this method uses entropy and cumulative point similarity as clustering criteria. In the case of network damage, packet loss and noise interference can significantly affect the stability of entropy and cumulative point similarity calculations, causing deviations in these clustering criteria and ultimately incorrectly dividing normal and abnormal data, affecting the accuracy of intrusion detection. Mutambik adopted the IoT-FIDS (Internet of Things Intrusion Detection Based on Data Streams) lightweight framework to achieve abnormal intrusion detection. This framework captures details such as node communication patterns and service usage by checking data streams, and only analyzes benign traffic during the detection process to identify abnormal behaviors, avoiding the dependence on pre-labeled data and a large amount of computing power. While reducing resource consumption, it can accurately detect most abnormal traffic, reduce false alarms, and provide practical protection for network security [13]. However, this method cannot highlight the role of key features and is difficult to accurately distinguish between normal traffic changes and malicious behaviors, resulting in misjudgment.

In addition to the research on detection architecture mentioned above, from the perspective of data processing and feature engineering, existing works have also attempted to introduce various technologies. In terms of data dimensionality reduction, Zhang B et al. [14] used t-SNE for nonlinear dimensionality reduction, which focuses on preserving the local neighborhood structure of data points and mapping high-dimensional features (such as texture features extracted by GLCM) to a low dimensional space. However, such methods typically focus on maintaining the topological structure of data for visualization, with high computational complexity and a lack of clear inverse mapping for dimensionality reduction results, making it difficult to directly serve efficient online detection tasks. Shen Z et al. [15] used UMAP technology to reduce and visualize high-dimensional features, effectively evaluating the class separability of features in low dimensional space. However, the dimensionality reduction results of UMAP have randomness, and their output is sensitive to initialization parameters, which can lead to inconsistent feature representations after dimensionality reduction at different times or network states, seriously damaging the stability of online detection models. In terms of deep feature extraction, Alshehri et al. [16] proposed a model that combines Wasserstein GAN and autoencoder (WGAN-AE), which utilizes autoencoder reconstruction to learn robust latent feature representations. However, the training process of such generative models is unstable, and under the noise interference introduced by network damage, the dynamic balance between the generator and discriminator is more difficult to maintain, resulting in a decrease in the reliability of feature extraction. Brian W et al. [17] constructed a hybrid model integrating Transformer and random forest, which utilizes the self attention mechanism of Transformer to dynamically screen and weight key features. However, this model has high computational complexity and strict hardware resource requirements, making it difficult to deploy on wireless sensor network nodes with limited computing power; At the same time, its powerful feature filtering ability highly relies on a large amount of high-quality annotated data. In practical scenarios where the network is damaged, attack patterns are variable, and labels are scarce, its performance faces severe challenges.

The summary of research on anomaly intrusion detection in wireless sensor networks is shown in Table 1.

Table 1: Summary of related research on wireless sensor network anomaly intrusion detection

Author(s) (Year)	Research Method	Scenario	Key Results	Limitations
Niccolò et al. (2024)	Autoencoder reconstructs data packets transmitted by wireless sensor nodes, identifies anomalies based on reconstruction error	Wireless sensor networks	Detects unknown intrusions	Performance heavily depends on normal traffic patterns; struggles to distinguish between channel interference and malicious intrusion under network impairment.
Karrothu et al. (2025)	End-cloud-fog architecture, Yeo-Johnson transform + Kulczynski similarity + GDO-optimized ensemble classifier	Wireless sensor networks	Achieves distributed intrusion detection with optimized resources	Feature selection relies on static statistical relationships; poor adaptability to new attack patterns or environmental changes.
Arkan et al. (2023)	SDWSN architecture, clustering analysis based on entropy and cumulative point similarity	Software-defined wireless sensor networks	Achieves unsupervised, hierarchical intrusion detection	Clustering criteria are sensitive to network impairment; packet loss and noise affect computational stability.
Mutambik (2024)	IoT-FIDS lightweight framework, data flow pattern inspection	IoT data streams	Low resource consumption, reduced false positives	Unable to highlight key features; normal fluctuations in complex environments are easily confused with attacks.
Zhang B et al. (2025)	t-SNE nonlinear dimensionality reduction	Defect detection (texture features)	Effectively preserves local data structure for visualization	High computational complexity, lacks inverse mapping, difficult to use for online detection.
Shen Z et al. (2024)	UMAP dimensionality reduction and visualization	Optical performance monitoring data	Effectively evaluates feature class separability	Dimensionality reduction results are stochastic, compromising the stability of online detection models.
Alshehri et al. (2025)	WGAN-AE hybrid model	IoT intrusion detection data	Learns robust latent feature representations	Unstable training process, sensitive to noise interference.
Brian W et al. (2024)	Transformer and random forest hybrid model	Satellite ground station networks	Dynamically selects and weights key features	High computational complexity, significant resource demands, relies on large amounts of labeled data.

Based on the systematic analysis of existing research (Table 1), it can be found that the current wireless sensor network anomaly intrusion detection faces three core problems: firstly, in the state of network damage, existing methods are difficult to distinguish the anomalous features of physical damage and malicious intrusion, resulting in high false alarm rates; Secondly, there is a lack of efficient and stable nonlinear feature processing solutions. Existing dimensionality reduction and feature extraction methods are either computationally complex, have unstable results, or have high resource requirements, which cannot meet the real-time online detection needs; The third issue is that the classifier lacks anti-interference ability in damaged environments, making it unable to adaptively highlight key features, resulting in a decrease in detection accuracy. Therefore, in order to systematically solve the problems faced by wireless sensor network communication anomaly intrusion detection under network damage and improve the accuracy of wireless sensor network communication anomaly intrusion detection, this paper studies a method for detecting wireless sensor network communication anomaly intrusion under network damage. It should be noted that the "network damage state" focused in this article specifically refers to systematic communication quality collapse scenarios caused by physical damage, malicious preemption, or sudden congestion with high random packet loss rates (>30%), malicious bandwidth limitations, and critical node failures. Unlike traditional static background constraints such as limited resources or environmental interference, this state leads to highly distorted and incomplete data transmission in the network, causing deep confusion between intrusion features and physical damage features, thereby undermining the assumption that existing detection methods rely on "basic data reliability". The specific technical route is as follows:

(1) Global perceptible data acquisition: By constructing a wireless sensor network networking model and based on the probability formula for node automatic identification, it ensures that the status monitoring and communication data collection of all nodes in the entire domain can still be achieved even when the network is partially damaged, providing a reliable data foundation for subsequent analysis.

(2) KPCA Nonlinear Data Dimensionality Reduction: To address the difficulty of transmitting and processing high-dimensional data in damaged networks, the Kernel Principal Component Analysis (KPCA) method is adopted. Nonlinear mapping of raw data to low dimensional space using Gaussian radial basis kernel function significantly reduces data dimensionality and computational complexity while preserving key structural information, alleviating resource pressure.

(3) RBM deep feature extraction: To effectively distinguish the mixed features of network damage and malicious intrusion, a restricted Boltzmann machine (RBM) is used to perform unsupervised deep feature learning on the reduced dimensional data. By using its energy model probability distribution, abstract features that can characterize the essence of abnormal intrusion are extracted to enhance the discriminative ability of the features.

(4) Optimizing Naive Bayes classification decisions: In response to noise interference in damaged environments, perform dual optimization on the Naive Bayes classifier: first, introduce a feature weighting mechanism to highlight the contribution of key features; Secondly, implement micro conditional probability optimization to improve the robustness of the model by iteratively modifying the conditional probability estimation. Ultimately, the optimized classifier is utilized to achieve high-precision and low false positive anomaly intrusion detection.

In summary, this article constructs an end-to-end solution through a progressive technical route of "KPCA dimensionality reduction → RBM feature extraction → optimized naive Bayes classification". This solution systematically addresses the full chain challenges from data preprocessing, feature engineering to final decision-making, in order to improve the accuracy, robustness, and real-time performance of wireless sensor network communication anomaly intrusion detection under network damage conditions.

2 Data dimensionality reduction and deep feature extraction of wireless sensor network communication network under damaged state

In wireless sensor networks, in addition to network damage caused by communication anomaly intrusion, physical interference, environmental interference, and energy depletion can all lead to a damaged state of the wireless sensor network. In order to still achieve accurate detection of communication anomaly intrusion in the wireless sensor network under the damaged state, it is necessary to ensure that the entire wireless sensor network is in a perceivable state, that is, each node in the network can be effectively monitored and detected [18]. Through the design of the networking model, ensure the coverage area and communication quality of the sensor network, so as to provide a reliable data source for the subsequent automatic identification of abnormal nodes [19]. In this context, this study focuses on three core objectives: firstly, to verify whether the nonlinear dimensionality reduction method based on kernel principal component analysis can significantly reduce data dimensionality and computational complexity while preserving key information, thereby improving detection real-time performance; The second is to explore the ability of restricted Boltzmann machines to extract deep features from reduced dimensional data to distinguish between network damage and malicious intrusion behavior; The third is to evaluate the performance of the

Naive Bayes classifier with feature weighting and micro conditional probability optimization in maintaining high detection accuracy and low false alarm rate in network damaged environments, and compare its advantages and disadvantages with traditional and deep learning methods. Therefore, this article constructs an end-to-end detection framework that integrates global perception data acquisition, KPCA dimensionality reduction, RBM feature extraction, and optimized Naive Bayes classification, aiming to improve the accuracy, robustness, and real-time performance of anomaly intrusion detection in complex damage scenarios.

2.1 Data acquisition of wireless sensor network under damaged state

To ensure accurate anomaly intrusion detection even in the event of network damage, it is first necessary to ensure that the entire wireless sensor network (WSN) is in a globally perceptible state, where every node in the network can be effectively monitored by the monitoring system. Therefore, this article constructs a geometric perception-based node identifiability model to evaluate the monitoring coverage of each node in the event of network damage. For the convenience of theoretical modeling and analysis, this study simplifies the network deployment area into a rectangular region. Let the entire wireless sensor network be within the rectangle $M \times M$. If the sensing coordinate of a certain wireless sensor network node i within $M \times M$ is (x_i, y_i), whether it can be recognized when abnormal communication occurs in this wireless sensor network node depends on whether it is located within the optimal perception radius of the central node J, regardless of whether it has a logical association with the central node. Let (x, y) represent the coordinates of the automatic identification node. The formula for the condition for the abnormal node i of the wireless sensor network communication to be automatically identified is:

$$P(i, j) = 1, |i, j| < r \tag{1}$$

In the formula, $P(i, j)$ is the automatic identification probability, where a value of 1 indicates that it can be recognized and 0 indicates that it cannot be recognized, $|i, j|$ is the physical distance between node i and j, reflecting the spatial relationship between nodes, and r is the optimal sensing radius of the central node j, which is determined by the node's communication capability, channel quality, and environmental interference. It can usually be estimated through actual measurements or link budget models, representing the maximum effective range that the node can reliably perceive and communicate under specific network and environmental configurations.

The expression of $|i, j|$ is:

$$|i, j| = \sqrt{|x_i - x|^2 + |y_i - y|^2} \tag{2}$$

Through formula (1) and formula (2), it is possible to judge whether any node i can be successfully automatically identified when abnormal. If the automatic identification probability is 1 for all nodes in the wireless sensor network after the operation of formula (1), it means that the entire wireless sensor network is perceivable, and the communication data of each node in the wireless sensor network can be obtained. Otherwise, it indicates that there are coverage blind spots in the network, and it is necessary to partition the network and arrange automatic identification nodes in each partition to ensure that the entire wireless sensor network maintains a perceivable state and realize the acquisition of wireless sensor network communication data under the damaged state.

The above node identifiability model provides theoretical criteria for evaluating the global perceptibility of the network. To apply it to actual data collection, this study instantiated the model as follows: the physical coordinates of nodes and central nodes were derived from pre deployment network topology mapping; The optimal perception radius is determined through field link measurement, which tests the packet reception rate of the central node and surrounding nodes at different distances in the deployment environment. The farthest reliable communication distance that meets the minimum communication quality requirements is defined as this radius. In this experimental environment, the value of each cluster head node is distributed between 80 meters and 120 meters. The recognition probability is integrated into network management software as a binary decision function in practice, which determines whether a node can be monitored by calculating the distance between nodes in real-time and comparing it with the corresponding optimal perception radius. In this experimental deployment, by optimizing the node layout, the recognition probability of all 150 nodes was ensured to be 1, thus meeting the prerequisite of "global perceptibility" and providing a complete data foundation for subsequent analysis. Based on this network, all communication data is collected through the actual protocol stack to form the initial high-dimensional dataset; The simulation of network damage state is achieved through software injection of damage on this normal data stream, in order to obtain a controllable dataset of damage state.

In the actual data collection process, this study is based on the above model to guide network deployment and optimization, ensuring that the global perceptible conditions are met as much as possible in the actual physical topology. All communication data (including normal and abnormal traffic) are collected through this actual network, and the data collection process follows standard communication protocols, recording multi-dimensional information such as communication

timing, packet content, and signal strength of each node, forming the original high-dimensional dataset for subsequent dimensionality reduction and feature extraction.

2.2 Data dimensionality reduction of wireless sensor network communication network under damaged state based on kernel principal component analysis

The wireless sensor network networking model can achieve global state awareness of wireless sensing. Obtaining the communication data of each node in the wireless sensor network not only involves a huge amount of data, but also has a very high data dimension. In this state, data transmission will consume a large amount of communication resources. However, due to factors such as packet loss, channel congestion, and environmental interference in the network damaged state, it will cause great difficulties in the communication of the wireless sensor network, making it difficult to transmit data. Therefore, it is necessary to reduce the dimension of the communication data of the wireless sensor network in the network damaged state. By reducing the data dimension of the wireless sensor network in the damaged state, reducing data complexity, improving data calculation speed, occupying less communication resources in the damaged state, and improving the communication anomaly intrusion detection speed of the wireless sensor network in the network damaged state [20]. In order to quickly and accurately reduce the dimension, the kernel method is introduced based on the principal component analysis method to form the kernel principal component analysis method for data reduction [21].

The basic principle of the kernel method is as follows: The communication data of the wireless sensor network in the damaged state in the input data space is mapped to a high-dimensional feature space through a non-linear function, and data processing is carried out in the feature space. In this process, a kernel function is introduced to convert the inner product operation in the feature space after non-linear transformation into the calculation of the kernel function in the original space, thereby reducing the computational amount. The process of using kernel principal component analysis for dimensionality reduction of wireless sensor network communication data is shown in Figure 1.

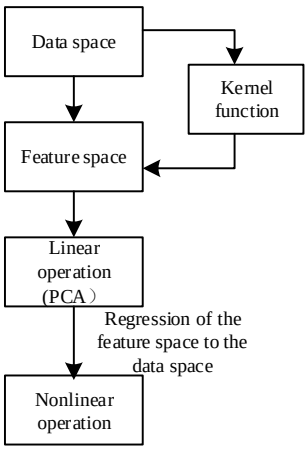


Figure 1: Kernel method framework

Based on the kernel method framework shown in Figure 1, the KPCA dimensionality reduction process achieves nonlinear feature extraction of high-dimensional data through four key stages: in the kernel function mapping stage, the original high-dimensional data is projected into a high-dimensional feature space through a nonlinear mapping function. This process uses kernel functions to implicitly calculate the inner product of samples in the feature space, avoiding complex high-dimensional explicit calculations. In the linear operation stage, data in the feature space is processed through standard principal component analysis. By calculating the eigenvalues and eigenvectors of the covariance matrix, determine the direction of maximum data variance and establish a low dimensional orthogonal coordinate system. In the feature space data reconstruction stage, the projection coordinates of the original data on the principal components of the feature space are obtained through mathematical transformations. These projection coordinates form the reduced dimensional dataset, preserving the key nonlinear features of the original data. Finally, through the organic combination of the above stages, nonlinear dimension reduction was achieved, resulting in a low dimensional data representation with discriminative power, providing an effective data foundation for subsequent anomaly intrusion detection. The specific process is as follows:

The nuclear method is combined with the principal component analysis to form the kernel principal component analysis method. The wireless sensor network communication obtained in Section 2.1 above. The trusted data is set as Π wireless sensor network communication data samples $\pi_k \left(k=1,2,3,\cdots,\Pi\right)$ in the input data space, $\pi_k \in R^N$, such that $\sum_{k=1}^{\Pi} \pi_k = 0$, and its covariance matrix $\boldsymbol{C}$ is:

$$\boldsymbol{C} = \frac{\sum_{k=1}^{\Pi} \pi_k \pi_k^T}{\Pi} \quad (3)$$

In the formula, T is the transpose.

In the PCA algorithm, a non - linear mapping function ϕ is introduced to transform the communication data sample points $\pi_1,\pi_2,\pi_3,\cdots,\pi_\Pi$ of the wireless sensor network in the damaged state in the input data space into the communication data sample points $\phi(\pi_1),\phi(\pi_2),\phi(\pi_3),\cdots,\phi(\pi_\Pi)$ of the wireless sensor network in the damaged state in the feature space. Assume:

$$\sum_{k=1}^{\Pi}\phi(\pi_k)=0 \qquad (4)$$

In the feature space G, the covariance matrix is:

$$\bar{\boldsymbol{C}}=\frac{\sum_{k=1}^{\Pi}\phi(\pi_k)\phi(\pi_k)^T}{\Pi} \qquad (5)$$

Therefore, the formula for solving the communication data value and vector of the wireless sensor network in the feature space G is:

$$\gamma\boldsymbol{\nu}=\bar{\boldsymbol{C}}\boldsymbol{\nu},\boldsymbol{\nu}\in G\neq\{0\} \qquad (6)$$

Where, γ and $\boldsymbol{\nu}$ are the wireless sensor network communication data values and vectors in the feature space G, respectively.

Thus, it can be obtained that:

$$\gamma\left(\phi(\pi_k)\boldsymbol{\nu}\right)=\phi(\pi_k)\bar{\boldsymbol{C}}\boldsymbol{\nu} \qquad (7)$$

The linear representation formula of the communication data vector $\boldsymbol{\nu}$ of the wireless sensor network in the feature space G is:

$$\boldsymbol{\nu}=\sum_{i=1}^{\Pi}\boldsymbol{\delta}_i\phi(\pi_i) \qquad (8)$$

In the equation, $\boldsymbol{\delta}_i$ is the eigenvector.

According to formulas (5), (7), and (8), we can obtain:

$$\gamma\sum_{\substack{i=1\\k=(1,2,3,\cdots,\Pi)}}^{\Pi}\boldsymbol{\delta}_i\left(\phi(\pi_k)\cdot\phi(\pi_i)\right)=\frac{\sum_{i=1}^{\Pi}\boldsymbol{\delta}_i\left(\phi(\pi_k)\cdot\sum_{i=1}^{\Pi}\phi(\pi_k)\right)\left(\phi(\pi_j)\cdot\phi(\pi_i)\right)}{\Pi} \qquad (9)$$

Define the matrix $\boldsymbol{K}$ of $\Pi\times\Pi$:

$$\boldsymbol{K}_{i,j}=\phi(\pi_i)\cdot\phi(\pi_j) \qquad (10)$$

Then formula (9) can be transformed into:

$$\Pi\gamma\boldsymbol{\delta}=\boldsymbol{K}\boldsymbol{\delta} \qquad (11)$$

By solving formula (11), the communication data value γ and vector $\boldsymbol{\nu}$ of the wireless sensor network in the mapping space can be obtained. Arrange $\gamma_1,\gamma_2,\gamma_3,\cdots,\gamma_n$ in descending order and adjust $\boldsymbol{\nu}_1,\boldsymbol{\nu}_2,\boldsymbol{\nu}_3,\cdots,\boldsymbol{\nu}_n$ to correspond to the sorted $\gamma_1,\gamma_2,\gamma_3,\cdots,\gamma_n$. Using the Gram Schmidt orthogonal method to normalize vectors, ensuring that the extracted principal components are orthogonal to each other, thus constructing a non redundant and discriminative feature representation in a low dimensional space, and obtaining $\boldsymbol{\delta}_1,\boldsymbol{\delta}_2,\boldsymbol{\delta}_3,\cdots,\boldsymbol{\delta}_n$. Then the projection of the communication data test sample of the wireless sensor network on the vector $\boldsymbol{\nu}^k$ in the feature space G is:

$$y=\sum_{i=1}^{n}\boldsymbol{\delta}_i\,\boldsymbol{K}\left(\pi_i,\pi_j\right) \qquad (12)$$

If the communication data of the wireless sensor network in the feature space does not meet the centering condition, the matrix needs to be corrected. Replace $\boldsymbol{K}$ in formula (12) with $\bar{\boldsymbol{K}}$, and the formula is:

$$\bar{\boldsymbol{K}}_{i,j}=\boldsymbol{K}_{i,j}-\frac{\sum_{m=1}^{\Pi}o_{i\Pi}\boldsymbol{K}_{\Pi j}}{\Pi}-\frac{\sum_{n=1}^{\Pi}o_{in}\boldsymbol{K}_{nj}}{\Pi}+\frac{\sum_{\Pi,n=1}^{\Pi}o_{im}\boldsymbol{K}_{mn}o_{nj}}{\Pi^2} \qquad (13)$$

In formula (13), i , $j=1$, and $o_{i,j}$ are correction coefficients.

The specific process of dimensionality reduction of the communication data of the wireless sensor network by the kernel principal component analysis method according to the above content is as follows:

(1) Suppose Π data records are obtained from the communication data of the wireless sensor network sensed by the wireless sensor network networking model (each record has n attribute components), and represent it as a $\Pi\times n$ -dimensional matrix:

$$\boldsymbol{\pi}_k = \begin{bmatrix} \pi_{11} & \cdots & \pi_{1n} \\ \vdots & \ddots & \vdots \\ \pi_{\Pi 1} & \cdots & \pi_{\Pi n} \end{bmatrix} \quad (14)$$

(2) Select an appropriate kernel function and calculate the kernel matrix $\boldsymbol{K}$. Since the Gaussian radial basis function (RBF) kernel function can implicitly map data to a high-dimensional space to achieve nonlinear modeling, with few parameters, strong adaptability, and relatively efficient calculation, the Gaussian radial basis function is selected as the kernel function of kernel principal component analysis. The formula of the Gaussian radial basis function is:

$$\boldsymbol{K}\left(\pi_i, \pi_j\right) = \exp\left(-\frac{\left\|\pi_i - \pi_j\right\|^2}{\sigma^2}\right) \quad (15)$$

In the formula, $\left\|\pi_i - \pi_j\right\|^2$ is the square of the Euclidean distance between two communication data of the wireless sensor network in the feature space; σ is the kernel function width.

(3) Correct the kernel matrix $\boldsymbol{K}$ to obtain $\bar{\boldsymbol{K}}$, as shown in formula (13).

(4) Calculate the value $\gamma_1, \gamma_2, \gamma_3, \cdots, \gamma_n$ of $\bar{\boldsymbol{K}}$ and the vector $\boldsymbol{\nu}_1, \boldsymbol{\nu}_2, \boldsymbol{\nu}_3, \cdots, \boldsymbol{\nu}_n$.

(5) Arrange $\gamma_1, \gamma_2, \gamma_3, \cdots, \gamma_n$ in descending order and adjust $\boldsymbol{\nu}_1, \boldsymbol{\nu}_2, \boldsymbol{\nu}_3, \cdots, \boldsymbol{\nu}_n$ to correspond to the sorted $\gamma_1, \gamma_2, \gamma_3, \cdots, \gamma_n$.

(6) Use the Gram-Schmidt orthogonal method to normalize the vector and obtain $\boldsymbol{\delta}_1, \boldsymbol{\delta}_2, \boldsymbol{\delta}_3, \cdots, \boldsymbol{\delta}_n$.

(7) Calculate the cumulative contribution rate $B_1, B_2, B_3, \cdots, B_n$ of the sorted $\gamma_1, \gamma_2, \gamma_3, \cdots, \gamma_n$ values. According to the given extraction efficiency p , if $B_i \geq \rho$, then extract i principal components $\delta_1, \delta_2, \delta_3, \cdots, \delta_i$.

(8) Calculate the projection $y = \bar{\boldsymbol{K}}\boldsymbol{\delta}$ of the corrected kernel matrix $\bar{\boldsymbol{K}}$ on the extracted corresponding vectors, where $\boldsymbol{\delta} = \boldsymbol{\delta}_1, \boldsymbol{\delta}_2, \boldsymbol{\delta}_3, \cdots, \boldsymbol{\delta}_i$; the obtained projection y is the data obtained after the data is reduced in dimension by KPCA.

After reducing the dimension of the wireless sensor network communication data in the network damaged state by the KPCA method, a certain degree of compression is performed, redundant information is removed, and the complexity of the data is reduced, so that the data can be transmitted using fewer communication resources. Occupying fewer communication resources in the network damaged state can transmit data faster, so the wireless sensor network communication anomaly intrusion detection can be completed faster.

2.3 Feature extraction of wireless sensor network communication data in the damaged state based on the restricted boltzmann machine

After completing the dimension reduction of the wireless sensor network communication data in the network damaged state by the KPCA method, the Restricted Boltzmann Machine (RBM) is used to extract the data features of the data after dimension reduction in the network damaged state. RBM is a probability distribution function based on energy [22], and its energy function $E(\mathrm{y}, h)$ formula is:

$$E(\mathrm{y}, h) = -\sum_{i=1}^{n_y} \alpha_i y_i - \sum_{j=1}^{n_h} \beta_j y_j - \sum_{i=1}^{n_y}\sum_{j=1}^{n_h} h_j \boldsymbol{\omega}_{j,i} y_i \quad (16)$$

Where: $h = \left(h_1, h_2, h_3, \cdots, h_m\right)^T$ represents the values of the neurons in the RBM hidden layer, $y = \left(y_1, y_2, y_3, \cdots, y_n\right)^T$ represents the values of the neurons in the visible layer, that is, the wireless sensor network communication data after dimension reduction, α_i is the bias value of the visible layer neuron i , β_j is the bias value of the hidden layer neuron j , and $\boldsymbol{W} = \left(\boldsymbol{\omega}_{ij}\right)_{m \times n}$ is the connection weight matrix from the visible layer to the hidden layer.

According to the energy function, the joint probability distribution $P(y, h)$ of y and h can be obtained as:

$$P(y, h) = \frac{1}{Z} e^{-E(y,h)} \quad (17)$$

Where, Z is the partition function (normalization factor):

$$Z = \sum_{y,h} e^{-E(y,h)} \qquad (18)$$

Formula (17) gives the "energy - probability" relationship, from which the feature μ of the wireless sensor network communication data after dimension reduction extracted by the hidden layer can be obtained, and the formula is:

$$\mu = P(y_i = 1 \mid h) = \sigma\left(\alpha_j + \sum_i h_j \omega_{ij}\right) \qquad (19)$$

In the equation, σ is the Sigmoid function.

According to formula (20), the dimensionality-reduced wireless sensor network communication data features μ extracted by the hidden layer of the RBM [23], that is, the communication features of the wireless sensor network in the network damaged state.

When the RBM algorithm is applied to the process of extracting wireless sensor network communication data features, an unsupervised learning method is adopted to train the RBM feature extraction model. The purpose of training the RBM is to make the distribution $p(y)$ of the visible layer nodes y best fit the distribution $q(y)$ of the sample space where the input dimensionality-reduced wireless sensor network data samples are located. From the perspective of information entropy, it is to make the *KL* (Kullback-Leibler, relative entropy) distance between p and q the smallest, so that the two distributions are closer. The formula is:

$$\begin{aligned} KL(q \| p) &= \sum_{y \in Y} \ln \frac{q(y)}{p(y)} \\ &= \sum_{y \in Y} q(y) \ln q(y) - \sum_{y \in Y} q(y) \ln p(y) \end{aligned} \qquad (20)$$

Since the input of the visible layer is the communication data information in the wireless sensor network, $q(y)$ is a determined item. To ensure the smallest *KL* distance, $\sum_{y \in Y} q(y) \ln p(y)$ needs to be maximized. Since the sample space Y of the wireless sensor network communication data is unknown, the Monte Carlo method is used to find the approximate value of $\sum_{y \in Y} q(y) \ln p(y)$. The formula is:

$$\sum_{y \in Y} q(y) \ln p(y) \approx \frac{\sum_{\psi=1}^{\Psi} \ln p\left(y^{\psi}\right)}{\Psi} \qquad (21)$$

In the formula: Ψ is the assumed number of training samples; y^{ψ} represents the ψ th training sample.

To find the optimal RBM parameter $\theta = \{W, \alpha, \beta\}$, the logarithmic loss function is adopted. The formula is:

$$Loss = -\sum_{i=1}^{\psi} \ln p\left(y^{(i)}\right) \qquad (22)$$

Thus, the training of the RBM feature extraction model is completed, and the feature extraction of the dimensionality-reduced wireless sensor network communication data is realized based on the trained RBM.

To ensure the effectiveness and reproducibility of the RBM feature extraction model, this study specifically designed its network structure and training process. In terms of network structure, the number of visible layer neurons remains consistent with the dimensionality of KPCA reduced data; The number of hidden layer neurons has been experimentally verified to be 128, in order to achieve a balance between feature compression and information preservation. The model training adopts the Contrastive Divergence (CD-1) algorithm, which performs one-step Monte Carlo simulation through Gibbs sampling to efficiently approximate the negative phase gradient of the data. Specifically, during the training process, Gibbs sampling is used to quickly generate visible and hidden layer samples from the current distribution of RBM in order to approximate the expected term of the model in formula (21). This Monte Carlo sampling method avoids the huge computational overhead of directly calculating the partition function, and approximates the true gradient direction through finite step sampling, making it possible to maximize the logarithmic likelihood function through the random gradient ascent method. The key hyperparameters are set as follows: learning rate of 0.01, training epochs of 100, and batch size of 64. This set of parameter combinations has been experimentally verified to effectively ensure the stable convergence of the model and extract deep features with high discriminative power.

3 Abnormal intrusion detection of wireless sensor network communication in the damaged state based on Naive Bayes Classifier

The naive Bayes classifier ensures that the posterior probability of a class is higher than that of other classes according to the maximum posterior probability rule, so as to achieve accurate classification [24]. The extracted wireless sensor network communication data feature vector $\boldsymbol{\mu}$ is used as the input of the naive Bayes network for abnormal intrusion detection of wireless sensor network communication [25]. Since the normal wireless sensor network in the network damaged state will also be affected by different factors, resulting in certain communication anomalies, but there are differences in the performance of the abnormal feature vector $\boldsymbol{\mu}$ between the communication anomalies caused by the network damaged state and those caused by intrusions. Therefore, the abnormal intrusion detection of communication in the network damaged state can be realized through the abnormal feature vector $\boldsymbol{\mu}$.

First, set or adjust the weight vector $\boldsymbol{\varepsilon}$ of the prior probability. The formula is:

$$p\left(\boldsymbol{\varepsilon}\mid\kappa\right)=\prod_{1}^{\vartheta}N\left(0,\partial_{i}^{-1}\right) \qquad (23)$$

In the formula: ϑ is the hyperparameter vector described by ∂.

Use $S=\left[s_1,s_2,s_3,\cdots,s_n\right]$ to describe the set of wireless sensor network communication data. Use $\boldsymbol{U}=\left[\boldsymbol{\mu}_2,\boldsymbol{\mu}_2,\boldsymbol{\mu}_3,\cdots,\boldsymbol{\mu}_n\right]$ to describe the set of wireless sensor network communication data feature vectors. Adopt the $s=f\left(\boldsymbol{\mu}_i\right)$ mapping criterion for description, where f is a classifier, which can make a random $s_i\in S$ uniquely correspond to a $\boldsymbol{\mu}_i\in\boldsymbol{U}$, satisfying $s=f\left(\boldsymbol{\mu}_i\right)$. The naive Bayes classification method is to establish a naive Bayes classifier, and the probability $p\left(s_e\mid\boldsymbol{\mu}\right)$ that the set of homogeneous data feature vectors $\boldsymbol{\mu}$ of wireless sensor network nodes that need to be classified as normal or abnormal belongs to the s_e class. The formula is:

$$p\left(s_e\mid\boldsymbol{\mu}\right)=\frac{p\left(\boldsymbol{\mu}\mid s_e\right)p\left(s_e\right)}{p\left(\boldsymbol{\mu}\right)} \qquad (24)$$

In the formula: $p\left(\boldsymbol{\mu}\right)>0$; $p\left(s_e\right)>0$, $e=1,2,3,\cdots,m$.

In formula (24), for different wireless sensor network states, the denominator $p\left(\boldsymbol{\mu}\right)$ is fixed, so maximizing the numerator is sufficient. If the wireless sensor network communication data in the network damaged state in the training set follows a specific probability distribution or is parameter-free, when dealing with continuous data, it is assumed that this data follows a normal distribution. For a certain continuous attribute in the training set, represented by b , first classify it, and then calculate the mean and variance of each class. Use η_{s_1} to represent the variance of b in the s_1 class. The communication abnormal intrusion probability $p\left(\boldsymbol{\mu}=z\mid s_1\right)$ for any wireless sensor network node is:

$$p\left(\boldsymbol{\mu}=z\mid s_1\right)=\frac{p\left(s_e\boldsymbol{\mu}\right)e}{p\left(\boldsymbol{\varepsilon}\middle|k\right)\sqrt{2\pi\eta_{s_1}^2}} \qquad (25)$$

In the formula, η_{s_1}、z are respectively used to describe the normal distribution and the variance with the mean at s_1, $p\left(\boldsymbol{\varepsilon}\mid\kappa\right)$ is a naive Bayes classifier.

Since normal network communication in the network damaged state will also be interfered and generate certain anomalies, a threshold is set based on formula (25), adjusted according to the actual situation based on a 60% probability. When the abnormal probability exceeds this threshold, it is determined that there is a communication abnormal intrusion in this wireless sensor network, and there is a node being invaded in the wireless sensor network.

Since the network damaged state will bring great interference to the intrusion detection of the naive Bayes classifier, the features of the naive Bayes classifier are weighted and the micro conditional probability is optimized.

(1) Feature Weighting Optimization

The formula of the naive Bayes classifier based on feature weighting optimization is:

$$p\left(\boldsymbol{\varepsilon}\mid\kappa\right)=\arg\max p\left(\boldsymbol{\varepsilon}\right)\prod_{1}^{\vartheta}N\left(\varsigma_i\mid\boldsymbol{\varepsilon}\right)^{\omega_\tau}\prod_{1}^{\vartheta}N\left(\varsigma_i\mid\boldsymbol{\varepsilon}\right)^{\omega_t} \qquad (26)$$

In the formula, the weight vectors $\boldsymbol{\varepsilon}=\left\{\omega_\tau,\omega_t\right\}$, ω_τ is the qualitative weight calculated based on the mutual information between features and categories, reflecting the correlation between features and abnormal intrusion. ω_t is the quantitative weight obtained based on the

inverse normalization of feature variance, used to balance the impact of differences in different feature value ranges. The specific calculation of weights is determined on the training set through cross validation.

(2) Micro Conditional Probability Optimization

In the training phase, first learn the estimated information and the Naive Bayes classifier, and then predict the training set to obtain the misclassified training samples. In the fine-tuning phase, modify the conditional probabilities corresponding to all misclassified samples in each round. Increase the conditional probability of each feature under the true class by a certain step size and decrease the conditional probability of each feature under the predicted class by a certain step size, so as to improve the accuracy of classifying the training set in the next round. Otherwise, stop the iteration. The optimal conditional probability is the conditional probability modified in the previous round. The formula is:

$$p(s_e \mid \boldsymbol{\mu}) = \frac{p(\boldsymbol{\mu} \mid s_e)\, p(s_e)}{p(\boldsymbol{\mu})} + \varpi_t(TC)$$
$$p(s_e \mid \boldsymbol{\mu}) = \frac{p(\boldsymbol{\mu} \mid s_e)\, p(s_e)}{p(\boldsymbol{\mu})} + \varpi_t(PC) \quad (27)$$

Among them, TC and PC are the true class and the predicted class of the training samples of the communication data of the wireless sensor network respectively. ϖ_t is the conditional probability of the t -th round of iteration, and t is the number of iterations.

In the fine-tuning phase, an iterative optimization strategy is adopted to adjust the conditional probability estimates, specifically implemented through the following algorithm:

Input: Training dataset, initial Naive Bayes classifier, maximum iteration count *T*, convergence threshold ε

Output:Optimized conditional probability table

1)Initialization:

Set the current iteration round t=0, train using the training dataset to obtain the initial conditional probability table.

2)Iterative Optimization:

for t=1 to T do

Step 1: Use the current conditional probability table to predict the training set and collect the set of misclassified samples.

Step 2: Check convergence criteria:

if the number of misclassified samples stops decreasing and the decrease magnitude is less than threshold ε then

Terminate the iteration, jump to Step 5.

end if

Step 3: For each misclassified sample:

Obtain the sample's true class and predicted class.

for each feature do

Increase the conditional probability of this feature under the true class (increase by step size δ).

Decrease the conditional probability of this feature under the predicted class (decrease by step size δ).

end for

Step 4: Perform normalization to ensure the sum of all conditional probabilities is 1.

end for

3)Output Result:

Step 5: Return the final optimized conditional probability table.

The core idea of this optimization process is: for each misclassified sample, increase the conditional probabilities of its features under the true class, while simultaneously decreasing them under the incorrectly predicted class. Through this bidirectional adjustment, the model can gradually correct initial estimation biases and better adapt to the true data distribution.

During optimization, the adjustment step size δ for conditional probabilities is typically set to a small positive number, such as 0.01 or 0.05, to ensure a smooth and convergent optimization process. Additionally, the algorithm incorporates dual convergence criteria: firstly, the number of misclassified samples ceases to decrease, and secondly, the decrease magnitude falls below a preset threshold. These two conditions together ensure the optimization process terminates at an appropriate point, preventing overfitting.

By performing feature weighting on the Naive Bayes classifier and optimizing the conditional probabilities through fine-tuning, the influence of key features on classification can be highlighted, the weights of features with a high degree of association with the target category can be enhanced, the interference of irrelevant features can be suppressed, and at the same time, the probability estimation deviation caused by assuming feature independence, data sparsity, etc. can be corrected, making the model more adaptable to the actual distribution of the data, and increasing the accuracy of detecting abnormal intrusions in the wireless sensor network communication under the network damaged state.

4 Experimental analysis

4.1 Experimental object

The experiment selected a wireless sensor network used in a company, which covers over 1000 square meters of production, warehousing, and transportation areas, with a total of 150 sensor nodes covering various types such as vibration, temperature and humidity, pressure, etc. It is used for real-time monitoring of equipment production and environmental parameters for intelligent control. The topology structure of the wireless sensor network is shown in Figure 2.

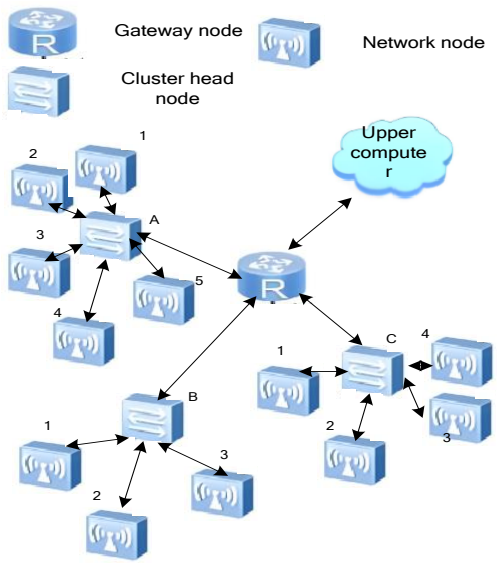


Figure 2: Topology structure of wireless sensor network

Figure 2 illustrates the topology structure of the Wireless Sensor Network (WSN) employed in the experiments. This network is deployed in an industrial environment, covering production, storage, and transportation areas for real-time monitoring of equipment operating status and environmental parameters. A hybrid topological structure is adopted, combining the advantages of star and mesh topologies to enhance communication reliability and coverage. The network comprises multiple cluster head nodes (CHs) (e.g., Cluster Head A, B, C), which are responsible for coordinating data aggregation and transmission from ordinary sensor nodes within their respective regions. Utilizing a multi-hop communication mechanism, data is relayed through the cluster head nodes to a gateway node, and ultimately uploaded to the cloud or a control center. To verify the anomaly intrusion detection capability of the proposed method under network damage conditions, communication damage was artificially introduced in the experiment: a random packet loss rate of 30% was set between cluster head C and the gateway to simulate channel quality deterioration; Limit the communication bandwidth of cluster heads A and B to 40% of their original value, simulating a resource constrained scenario. The dataset used for training and testing was actually collected through the network, containing a total of 50000 communication data records, including 35000 normal communication data and 15000 abnormal data. Abnormal data is generated by simulating ten typical attack behaviors, including Sinkhole attack, wormhole attack, denial of service attack, replay attack, disguised node attack, selective forwarding attack, flooding attack, data tampering attack, key leakage attack, and topology destruction attack. Each type of attack generates approximately 1500 instances to ensure class balance in the dataset, and each type of attack is injected into specific nodes through scripts, with corresponding timestamps and traffic characteristics recorded. The ratio of normal and abnormal samples in the dataset is 7:3, ensuring that the model still has good generalization ability even in cases of class imbalance. All data are anonymized during the collection process and feature sequences are constructed using time window slicing to support subsequent dimensionality reduction and feature extraction operations.

The parameters of the wireless sensor network used are shown in Table 2.

Table 2: Parameters of wireless sensor network

Attribute	Parameters
Topological structure	Hybrid topological structure
Communication standard	IEEE 802.15.4g
Working frequency band	2.4GHz
Network capacity	Support concurrent access of over 2000 nodes
Sensor type	Vibration sensor, temperature and humidity sensor, RFID reading and writing module, pressure sensor
Battery life	Lithium thionyl chloride battery, with a 5-year battery life (in low-power mode)
Protection grade	IP67
Computing power	8-bit microcontroller, supporting edge lightweight computing
Transmission distance	Single jump 150 meters
Data rate	250kbps
Encryption protocol	AES - 128
Deployment method	Guide rail installation + ceiling mounting + pole clamping installation

Gateway interface	Ethernet (1Gbps), 4G/5G modules
Working temperature	-20℃ ~ 70℃

The selection of kernel functions and their parameters has a decisive impact on the dimensionality reduction performance of KPCA. This study uses Gaussian radial basis function (RBF) kernel function, whose parameter kernel width σ controls the flexibility and locality of the model. To evaluate the robustness of parameter selection and determine the optimal value, a sensitivity analysis experiment was designed: on the same dataset, all other conditions were fixed, and the value of σ was systematically changed to observe its impact on the performance of reduced dimensional data in subsequent anomaly intrusion detection tasks (with F1 score as the core indicator).

Table 3: Sensitivity analysis results of KPCA parameter σ

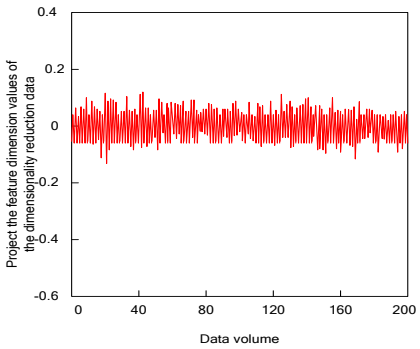
Kernel width	Data dimension after dimensionality reduction	Abnormal intrusion detection F1 score
0.01	28	0.71
0.10	19	0.84
0.50	15	0.92
1.00	13	0.87
5.00	10	0.78

According to the results in Table 3, the performance of KPCA is more sensitive to changes in the value of σ. When σ =0.50, the reduced dimensional data achieved the highest F1 score (0.92) in subsequent classification tasks, indicating that under this parameter, KPCA can most effectively extract the nonlinear features that are most beneficial for distinguishing normal and abnormal communication modes. Meanwhile, when σ is within the range of [0.10, 1.00], the F1 scores remain above 0.84, indicating that the method has good robustness within this parameter range. All subsequent experiments in this study were conducted using the optimal parameter determined by this experiment, σ =0.50.

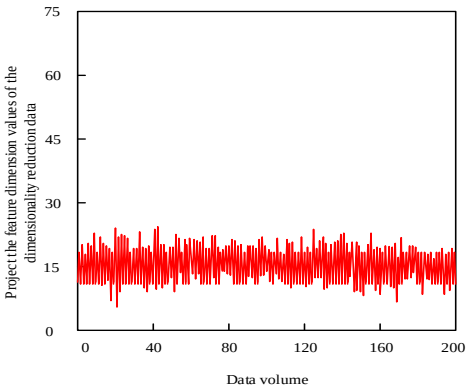
To ensure the reproducibility and scientificity of the proposed method, this study specifically set and explained the hyperparameters of the model. Firstly, in the design of a Restricted Boltzmann Machine (RBM), the number of hidden layer neurons is set to 128 to achieve a balance between feature compression and information preservation; The model training uses the Contrastive Divergence (CD-1) algorithm, with key hyperparameters including a learning rate of 0.01, 150 training epochs, and a batch size of 64. Secondly, in the process of optimizing the Naive Bayes classifier, the qualitative weights (based on mutual information) and quantitative weights (based on reciprocal variance) used for feature weighting are fused with coefficients of 0.7 and 0.3, respectively, and determined through cross validation; The adjustment step size for micro conditional probability optimization is set to 0.01, the maximum number of iterations is 50, and the convergence criterion is to stabilize the number of misclassified samples (with a change amplitude less than 0.001). In the process of determining key parameters of the model, such as the kernel width σ of KPCA, the number of hidden units in RBM, and the weight coefficients of Naive Bayes, 5-fold cross validation was used to optimize on the training set. Specifically, divide the training set into 5 equal parts, take turns using 4 parts as the training subset and the remaining 1 part as the validation subset, and loop 5 times. The final parameter selection is based on the group with the best average performance among 5 verifications. All performance metrics reported, such as F1 score and false positive rate, are the final results of the model on an independent test set.

4.2 Analysis of the effectiveness of the proposed method

To verify the effect of the KPCA method used in this article on dimensionality reduction of original wireless sensor network communication data, wireless sensor network communication data was randomly collected and dimensionality reduction was performed using the KPCA method proposed in this article. The original wireless sensor network communication dataset contains 90 features (attributes), and the reduced wireless sensor network communication data is shown in Figure 3.



(a)The distribution of original wireless sensor network communication data



(b)Data distribution of wireless sensor network communication after KPCA dimension reduction

Figure 3: Data dimensionality reduction effect of the KPCA method

From Figure 3, it can be seen that the KPCA method proposed in this paper can achieve efficient dimensionality reduction of wireless sensor network communication data. In the original state, the feature dimensions of wireless sensor network communication data without dimensionality reduction are mainly concentrated in 60-80 features, but there are also a large number of fluctuations between 10-90 features, resulting in extremely high data dimensions. In the state of network damage, the computing power of the network decreases, and it is difficult to ensure the accuracy of anomaly intrusion detection by processing high-dimensional data. After using the KPCA method in this article for data dimensionality reduction (as shown in Figure 3 (b)), the projected values of the data in the KPCA principal component space were standardized to around 15 features, which cumulatively explained about 94.7% of the original variance, indicating that the reduced features had been effectively compressed and concentrated, with slight fluctuations but almost negligible. The data fluctuation is reduced and the dimensionality is significantly reduced after dimensionality reduction using the method described in this article. In situations where the network is damaged and communication resources are tight, very few resources can be used for anomaly intrusion detection to ensure real-time detection. Moreover, the reduced dimensional data reduces interference, improves the accuracy of anomaly intrusion detection, and ensures that the proposed method can quickly and accurately detect communication anomalies in wireless sensor networks, thereby ensuring the security of wireless sensor networks.

The data fluctuates less after dimensionality reduction by this method, and the dimension is significantly reduced. In the case of network damage and tight communication resources, extremely few resources can be used for anomaly intrusion detection, ensuring the real - time performance of detection. Moreover, the dimensionality - reduced data reduces interference and improves the accuracy of anomaly intrusion detection, ensuring that the method in this paper can quickly and accurately detect the abnormal intrusion of wireless sensor network communication, thus ensuring the security of the wireless sensor network.

To quantitatively evaluate the data dimensionality reduction performance of the kernel principal component analysis (KPCA) method used in this paper, we compared it with two widely used nonlinear dimensionality reduction methods - t-distributed random neighbor embedding (t-SNE) and uniform manifold approximation and projection (UMAP). The evaluation metric is the cumulative variance contribution rate, which reflects the ability of the reduced data to retain the original data information and is a key quantitative standard for measuring the effectiveness of dimensionality reduction. The cumulative variance contribution rates of the three methods in extracting different numbers of principal components are shown in Table 4.

Table 4: Cumulative variance contribution rate of different dimensionality reduction methods (%)

Number of Principal Components	KPCA	t-SNE	UMAP
5	68.5	45.2	52.7
10	86.3	61.8	70.4
15	94.7	73.1	81.9
20	98.2	80.5	88.3
25	99.5	85.0	92.1

The following conclusion can be drawn from Table 3: The KPCA method used in this article is significantly better than the comparative method in terms of cumulative variance contribution rate. Specifically, with only 15 principal components, KPCA can retain 94.7% of the variance information in the original data; However, t-SNE and UMAP can only retain 73.1% and 81.9% of the information under the same principal component score. To achieve information retention levels similar to KPCA (approximately 94%), t-SNE and UMAP require more dimensions, which undoubtedly increases the burden of subsequent computation and communication. This result demonstrates that KPCA can capture key nonlinear structures in wireless sensor network communication data with fewer dimensions and higher

efficiency, and its dimensionality reduction performance is superior to t-SNE and UMAP. This advantage stems from the ability of kernel methods to implicitly handle inner product operations in high-dimensional feature spaces, avoiding the computational complexity of direct high-dimensional mapping while preserving key structural information of the data. In the event of network damage, KPCA not only reduces the dimensionality of the data, but more importantly, extracts more discriminative features through nonlinear mapping, providing higher quality and less noisy input data for subsequent anomaly intrusion detection, thereby improving the overall robustness and detection efficiency of the system.

4.3 Experimental comparison results

To verify the effectiveness of the RBM method used in this paper for extracting reduced dimensional wireless sensor network features, we compared our method with three feature extraction methods: CNN (Convolutional Neural Network), LSTM (Long Short-Term Memory Neural Network), and LLE (Local Linear Embedding). The features extracted by the above methods were input into a Bayesian classifier for communication anomaly intrusion detection. To ensure fairness in comparison, CNN adopts a typical structure consisting of two convolutional layers (kernel sizes of 3 and 5 respectively) and one fully connected layer; LSTM uses a single-layer network with 128 hidden units to capture temporal dependencies. All models use the Adam optimizer and learn until convergence on the same training set. All the features extracted by the methods were input into the same Naive Bayes classifier for communication anomaly intrusion detection, and the F1 score was used as the evaluation metric. The results are shown in Figure 4.

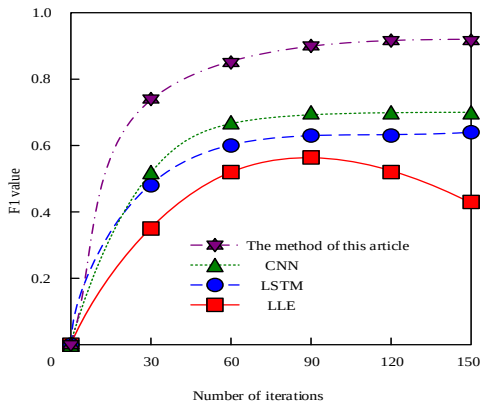


Figure 4: F1 values of different feature extraction methods under 75% network damage rate

From Figure 4, it can be seen that among the different feature extraction methods mentioned above, the RBM method proposed in this paper combines Naive Bayes classifier for anomaly intrusion detection after feature extraction, with an F1 value of 0.9, significantly higher than other methods. This indicates that the RBM method can more effectively extract key features from wireless sensor network communication data, thereby improving the accuracy of classification. This is mainly due to the fact that RBM, as an energy based unsupervised deep learning model, can effectively capture nonlinear feature distributions in high-dimensional data, especially suitable for complex and nonlinear abnormal patterns caused by network damage in wireless sensor networks. WSN communication data usually has the characteristics of high dimensionality, strong noise, and pattern mutation. The probability generation model of RBM can learn its underlying distribution well and is insensitive to noise, thus robustly extracting key features. In contrast, although CNN performs well in image and sequence data processing, its deep structure is prone to overfitting in the small sample, high noise wireless sensor network communication data used in this experiment, and the assumption of local correlation in the data may not always hold true in this task, resulting in limited feature extraction ability, with an F1 value of only about 0.6. LSTM is also difficult to learn effective long-term time dependencies due to limited data volume and noise interference, and its F1 value is similar to CNN. The LLE method has the lowest F1 value after feature extraction, and there is a decrease in F1 value during the iteration process. This may be due to the poor performance of LLE methods in processing high-dimensional and nonlinear data, resulting in extracted features that cannot effectively distinguish between normal and abnormal communication data. The above results indicate that the proposed RBM feature extraction method has significant advantages in wireless sensor network communication anomaly intrusion detection, which can more effectively extract key features and improve classification accuracy.

In order to verify the effectiveness of intrusion detection for abnormal communication in wireless sensor networks under network damage conditions, the company's wireless sensor network topology caused a certain amount of packet loss in the communication between cluster head C and gateway nodes, and reduced the bandwidth of the wireless sensor network, reducing the communication resources of cluster head A and cluster head B, simulating a network damage state. In this state, 10 attacks were carried out on random nodes in cluster heads A and B. The attack intrusion detection was performed using the method proposed in this paper, and the detection results are shown in Table 5.

As can be seen from Table 5, the proposed anomaly intrusion detection method in this paper shows excellent performance under the network damaged state. For each type of attack, the proposed method in this paper can accurately detect and determine the type of attack. For example, in the Sinkhole attack, the proposed method in this paper detected the abnormal nodes and abnormal aggregated traffic and determined it as the Sinkhole attack; in the wormhole attack, it detected the abnormal

high-speed data transmission path across regions and determined it as the wormhole attack. The results show that the proposed detection method can accurately identify and defend against various wireless sensor network anomaly intrusion behaviors under the network damaged state. Facing different types of attacks, the proposed method can quickly respond and accurately judge the type of attack, providing a strong guarantee for the security protection of wireless sensor networks. It not only provides a new technical idea for the anomaly intrusion detection of wireless sensor networks in emergency situations, but also provides a valuable practical reference for the construction of network security protection systems in fields such as industrial Internet of Things and intelligent transportation. This is because the method in this article adopts a multi-level feature decoupling and adaptive decision-making mechanism. Specifically, KPCA maps raw high-dimensional data to a renewable Hilbert space using kernel techniques, effectively separating background noise features caused by network damage such as channel packet loss and bandwidth limitations from structural anomaly features generated by attack behavior. Subsequently, RBM uses an energy model to perform deep representation learning on the reduced dimensional data, and its hidden layer neurons capture the clustering distribution characteristics of different attack patterns in the feature space through probabilistic activation. For example, for Sinkhole attacks, RBM hidden layer features will highlight abnormal data aggregation patterns; For wormhole attacks, it will enhance the time synchronization anomaly characteristics of cross regional transmission paths. Finally, the Naive Bayes classifier optimized by feature weighting integrates the likelihood ratio decision boundaries of different attack types through the Bayesian probability framework, and dynamically adjusts the prior distribution estimation under network damage conditions using the micro conditional probability optimization mechanism, thereby achieving high-precision attack classification and low false alarm detection in complex damaged environments. This technical route of "feature decoupling deep learning adaptive decision-making" enables our method to effectively resist the feature confusion problem caused by network damage, providing a reliable intrusion detection solution for practical WSN deployment.

Table 5: Detection results of our method under network damage conditions

Number	Attack name	Attack time	The detection results of the method in this paper
1	Sinkhole attack	0:15:23	Abnormal node and abnormal aggregated traffic were detected and determined to be a Sinkhole attack
2	Wormhole attack	1:08:17	An abnormal high-speed data transmission path across regions was discovered and determined to be a wormhole attack
3	Denial-of-service attack	2:30:05	A large number of invalid requests were detected, causing channel congestion, and it was determined to be a DoS attack
4	Replay attack	3:12:40	Duplicate historical data packets were detected and determined as replay attacks
5	Disguised node attack	4:45:32	t was found that the ID of the new node conflicted with that of the normal node, and it was determined as a masquerade node attack
6	Selective forwarding attack	5:20:18	Some data packet transmission paths are abnormal and are determined to be selective forwarding attacks
7	Flood attack	6:03:55	The channel traffic surges sharply in a short period of time and is determined to be a flooding attack
8	Data tampering attack	7:10:09	Verify the abnormal hash value of the data packet content and determine it as a data tampering attack
9	Key leakage attack	8:33:21	Unauthorized decryption data packets were discovered and determined to be a key leakage attack
10	Topological structure destruction attack	9:17:44	A large number of node connection interruptions were detected and determined to be a topological structure failure attack

First of all, in the case of network damage, the communication efficiency of wireless sensor network nodes is greatly reduced. This situation is very similar to that of nodes after being invaded. Therefore, the detection method is very likely to produce false alarms. To verify the sensitivity of the method proposed in this paper to abnormal intrusion detection in the case of network damage, it is compared with SVM (Support Vector Machine), association rule mining and CNN methods. The network damage rate is used to represent the degree of network damage. The effects of different methods on abnormal intrusion detection under different network damage rates are shown in Figure 5. In the experimental setup, to ensure the physical feasibility of the simulated scene and its compatibility with the actual industrial environment, this study set the upper limit of network damage rate to 75%. This setting is based on the following considerations: In actual industrial wireless sensor networks, when the link packet loss rate or bandwidth limitation exceeds 75%, the basic

communication functions of the network are almost paralyzed, and the regular monitoring data flow will be interrupted. At this time, discussing intrusion detection based on communication traffic is no longer practically meaningful. Therefore, a 75% damage rate represents the extreme pressure conditions that the system faces while maintaining a minimum operational state.

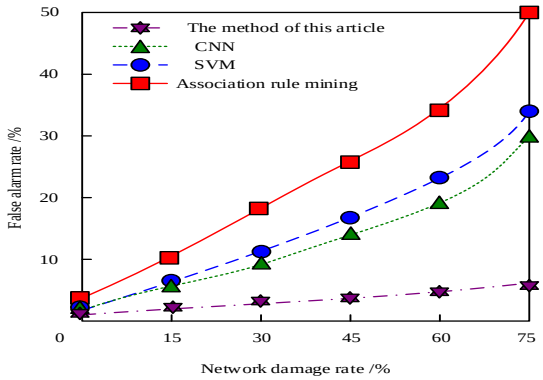


Figure 5: shows the abnormal intrusion detection effects of different monitoring methods under the condition of network damage

From Figure 5, it can be seen that as the degree of network damage increases, the false alarms of abnormal intrusion detection in wireless sensor networks under damaged conditions will correspondingly increase. The reason for this situation is that the state of network damage is similar to that under abnormal intrusion, and the difficulty of information transmission increases in network damage, making it more likely for detection results to be inconsistent with the actual state. Among them, the performance of anomaly intrusion detection through association rule mining is the worst. This method maintains the highest false alarm rate for anomaly intrusion detection under different network damage rates, and the false alarm rate significantly increases with the increase of network damage rate, reaching a final false alarm rate of 50%. At the same time, the false alarm rates of SVM and CNN reached 33% and 28%, respectively. On the other hand, although the false alarm rate of our method is also increasing, the degree of increase is not significant. In the case where the final network damage rate reaches the highest 75%, the false alarm rate of abnormal intrusion detection is only 5%. This result is derived from the multi-level anti-interference mechanism constructed by the method in this paper: KPCA achieves structural separation of noise and attack features in a high-dimensional feature space through kernel mapping, reducing feature confusion caused by network damage; The deep features extracted by RBM based on probability generation models have robust representation ability for damages such as random packet loss and bandwidth fluctuations; The optimized naive Bayes classifier enhances the discriminative contribution of attack related features through feature weighting, and dynamically adapts to changes in network state by combining micro conditional probability optimization, thereby maintaining stable decision boundaries in extremely damaged environments. These 5% false positives are mainly due to brief communication interruptions caused by extreme network congestion, which were mistakenly identified as denial of service attacks by the model. In practical WSN applications, this type of false alarm can be effectively filtered by setting a short time window for secondary verification, thereby avoiding unnecessary system alerts. From this, it can be seen that the method proposed in this paper can still maintain extremely high accuracy in anomaly intrusion detection under network damage, with excellent robustness and detection accuracy, further verifying the effectiveness and practicality of the method proposed in this paper.

To further verify the effectiveness of the method proposed in this paper, accuracy and recall were used as evaluation indicators to compare the detection performance of different methods. The comparison results of accuracy and recall of different detection methods under different degrees of network damage are shown in Table 6.

Table 6: Comparison of accuracy and recall rates of different detection methods under different degrees of network damage

Network Impairment Rate	Method	Precision	Recall
0%	Proposed Method	0.96	0.93
	SVM	0.89	0.85
	Association Rule Mining	0.75	0.70
	CNN	0.88	0.87
25%	Proposed Method	0.95	0.91
	SVM	0.85	0.80
	Association Rule Mining	0.70	0.65
	CNN	0.84	0.82
50%	Proposed Method	0.94	0.88
	SVM	0.78	0.72

Network Impairment Rate	Method	Precision	Recall
75%	Association Rule Mining	0.62	0.55
	CNN	0.77	0.75
	Proposed Method	0.94	0.86
	SVM	0.68	0.60
	Association Rule Mining	0.50	0.42
	CNN	0.65	0.63

According to the analysis of the results in Table 5, it can be concluded that our method outperforms the comparative methods in terms of accuracy and recall. To scientifically verify the statistical significance of this advantage, paired sample t-tests were conducted on the performance indicators of four methods on the same test set. The results showed that under different degrees of network damage, the accuracy and recall of our method were significantly different from those of SVM, association rule mining, and CNN methods (p values were all less than 0.01). Specifically, under the harsh condition of 75% network damage rate, our method (accuracy=0.94 ± 0.01, recall=0.86 ± 0.02) has a t-test statistic of t=15.73 ($p<0.001$) for accuracy and t=12.45 ($p<0.001$) for recall compared to the suboptimal CNN method (accuracy=0.65 ± 0.03, recall=0.63 ± 0.04). This proves that the performance advantage of the method proposed in this article is not accidental, but stems from its unique technical architecture. This architecture effectively decouples damage noise and intrusion features through KPCA nonlinear dimensionality reduction, extracts deep representations with strong discriminative power through RBM, and finally achieves robust decision-making through a Naive Bayes classifier optimized by feature weighting and micro conditional probability. In contrast, when the feature quality of SVM and CNN methods deteriorates due to network damage, the optimization objectives they rely on (such as classification interval and convolution kernel response) are prone to shift, resulting in significant performance degradation; However, association rule mining is completely ineffective in complex damage environments due to its inability to adapt to the dynamic changes in association relationships between features. In summary, statistical testing and mechanism analysis jointly confirm that the method proposed in this paper not only has higher detection accuracy under network damage conditions, but also has statistically significant performance advantages, providing a more reliable solution for practical wireless sensor network security protection.

To further evaluate the performance trade-off of the proposed method under extreme damage conditions, the method proposed in this paper was adopted at a 75% network damage rate SVM、CNN、 Association rule mining is used for intrusion detection, and the confusion matrix results of different methods are shown in Figure 6.

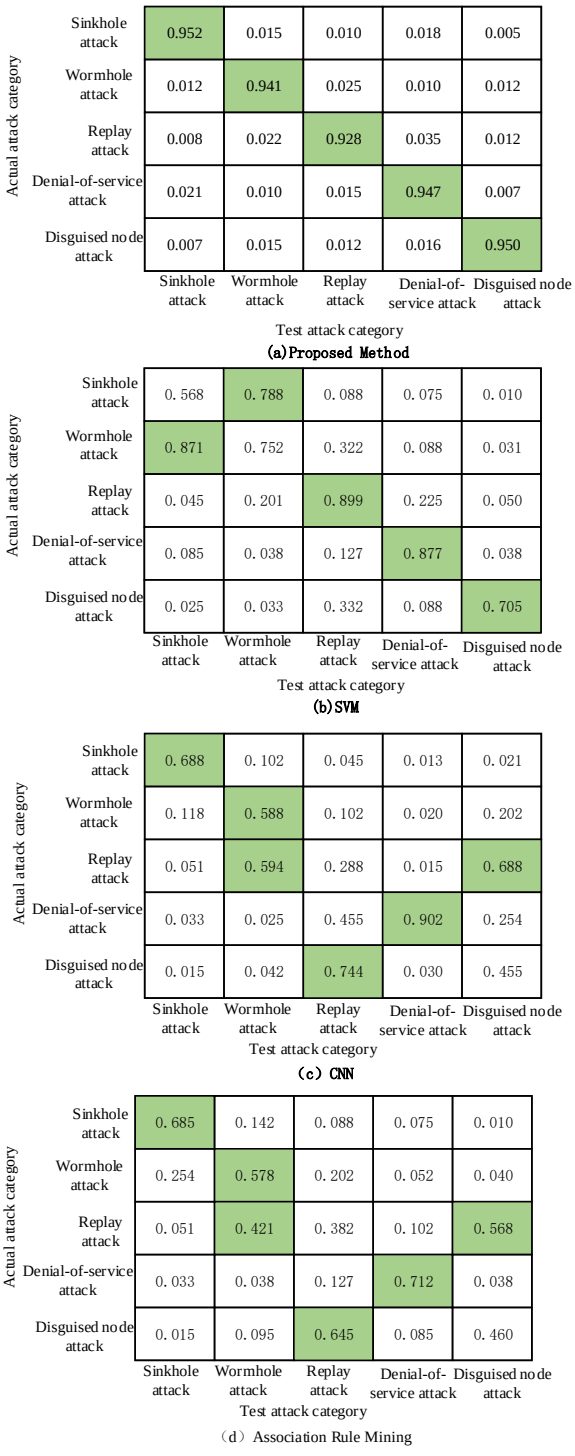


Figure 6: Confusion matrix results of different methods

From Figure 6, it can be seen that the average main diagonal value of the confusion matrix in this method reaches 0.944, and the recognition accuracy of various types of attacks is above 92.8%, and the inter class misjudgment rate is generally lower than 5.0%. In contrast, the attack recognition accuracy of the comparative method is lower. This is because the method in this article adopts a targeted technical architecture of "KPCA nonlinear dimensionality reduction → RBM deep feature extraction → optimized naive Bayes classification": KPCA maps damaged data to a high-dimensional feature space through kernel techniques, effectively removing channel noise and attack features; RBM enhances the discriminative differences between different attack modes by extracting deep representations based on energy models; The Naive Bayes classifier, which has undergone feature weighting and micro conditional probability optimization, has constructed an adaptive decision boundary. This system systematically overcomes the problem of feature confusion caused by network damage, enabling the model to maintain high accuracy even under extreme damage conditions.

The specific AUC curves of the above four methods are shown in Figure 7.

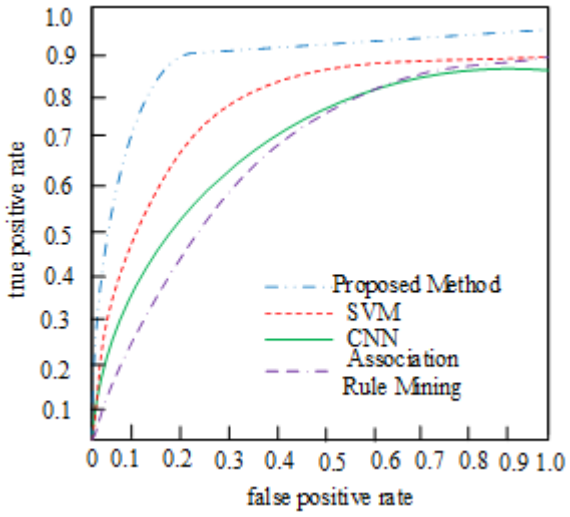


Figure 7: Comparative analysis of AUC curves of four methods

As shown in Figure 7, the AUC curve of our method and the area enclosed by the coordinate axis are higher than other methods, which effectively verifies the performance of our design method and the accuracy of its estimation results is relatively high. This is because the method proposed in this article constructs a complete robustness link from feature decoupling to adaptive decision-making: KPCA achieves structural separation of damage noise and attack features in high-dimensional space through kernel mapping, providing a pure feature base for subsequent processing; RBM extracts deep discriminative features that are insensitive to random packet loss and bandwidth fluctuations from reduced dimensional data based on probability generation models; The naive Bayes classifier, which has undergone dual optimization, enhances the contribution of key attack patterns through feature weighting and dynamically adapts to changes in network state through micro conditional probability optimization. This technical system enables the model to maintain a stable high true positive rate and low false positive rate under different decision thresholds, with a high AUC value.

Wireless sensor network (WSN) nodes typically have weak computing power, limited storage resources, and energy constraints. Therefore, intrusion detection methods must have low computational and resource consumption while ensuring detection performance. The detection pipeline (KPCA+RBM+NB) of the proposed method is designed to be executed in cluster head nodes or gateways with relatively sufficient resources, using a hierarchical deployment architecture of "edge collection aggregation analysis". The terminal sensor node is only responsible for lightweight data collection and uploading, avoiding complex calculations; And cluster heads/gateways run complete algorithms with their stronger processing capabilities, such as the ARM Cortex-A series. To evaluate the practical deployment feasibility of the proposed methods, a quantitative comparison of the computational complexity and resource consumption of all methods was conducted on the same experimental platform, and the results are shown in Table 7.

Table 7: Comparison of computational overhead under 75% network impairment rate

Method	Training Time (s)	Inference Time per Sample (ms)	Peak Memory Usage (MB)
Proposed Method	52.3	0.21	45.7
SVM	189.5	1.85	210.4
CNN	425.6	3.42	550.1
Association Rule Mining	510.2	4.15	480.3

The result analysis shows that the method proposed in this paper has significant advantages in computational efficiency. Its training time (52.3 seconds) and single sample prediction time (0.21 milliseconds) are much lower than the comparison method, and its peak memory

usage (45.7 MB) is also at the lowest level. This is mainly due to its cascaded lightweight design: KPCA dimensionality reduction significantly compresses the data scale and reduces the computational load of subsequent processing; Although RBM feature extraction involves unsupervised learning, its efficiency is higher compared to the divergence algorithm; Optimizing the Naive Bayes classifier itself has the characteristic of low computational complexity. Therefore, this method ensures high detection accuracy while achieving low cost and low latency characteristics that meet the resource constraints of wireless sensor networks, making it feasible for edge deployment.

To verify the necessity and contribution of each component in the proposed technical route of "KPCA dimensionality reduction → RBM feature extraction → optimized naive Bayes classification", a systematic ablation experiment was designed. Under extreme conditions of 75% network damage rate, the performance of the model was observed by removing or replacing key components one by one, and the results are shown in Table 8.

Table 8: Performance comparison of different model variants under 75% network impairment rate

Variant ID	Model Variant	Precision	Recall
A	KPCA + RBM + Optimized NB (Full Model)	0.94	0.86
B	Raw Data + RBM + Optimized NB	0.71	0.65
C	KPCA + Raw Features + Optimized NB	0.82	0.78
D	KPCA + RBM + Standard NB	0.85	0.80
E	KPCA + RBM + SVM	0.88	0.83
F	PCA + RBM + Optimized NB	0.79	0.72

Analysis of ablation experiment results: The complete model (A) maintains the highest performance among all variants, verifying the necessity of collaborative design among various components. Removing KPCA (variant B) resulted in a significant decrease in performance (accuracy dropped from 0.94 to 0.71), proving that non-linear dimensionality reduction using kernel methods is crucial for separating network damage noise and attack features; After removing RBM (variant C), the performance also significantly decreased, indicating that deep feature extraction can capture more essential attack pattern discrimination information; Replacing the optimized classifier with standard naive Bayes (variant D) or SVM (variant E) resulted in a decrease in performance, confirming that feature weighting and micro conditional probability optimization effectively improved the model's adaptability to damaged environments; The use of linear PCA (variant F) instead of KPCA resulted in a decrease in performance, further demonstrating the superiority of nonlinear mapping in this scenario. All components together form a complete enhancement chain from noise robustness, feature discriminative power to decision adaptation.

5 Conclusion

This article proposes a detection method that combines kernel principal component analysis (KPCA), restricted Boltzmann machine (RBM), and optimized naive Bayes classifier to address the core challenges of highly confused features and significantly reduced data quality in anomaly intrusion detection of wireless sensor networks under network damage. This method uses KPCA nonlinear dimensionality reduction to remove damage noise, extracts deep discriminative features robust to packet loss and interference using RBM, and achieves high-precision decision-making with the help of a Naive Bayes classifier optimized by feature weighting and micro conditional probability. Experiments have shown that the proposed method can maintain an accuracy of 0.94 and a recall of 0.86, with a false positive rate of less than 5%, even at a network damage rate of up to 75%. Its comprehensive performance (F1 value 0.90, AUC 0.96) is significantly better than traditional machine learning and deep learning methods, verifying its effectiveness and robustness in extreme damage environments. However, this study also has several limitations, and based on this, future directions are indicated. Firstly, the experiment is based on the WSN topology and data of a single industrial scenario. In the future, its universality needs to be verified in more heterogeneous and large-scale networks, and more complex damage models such as time-varying fading and mobile intermittent connections need to be included. Secondly, although it covers ten mainstream attacks, the defense capabilities against unknown attacks and adaptive attackers need further evaluation. In order to promote the actual deployment, the current "edge collection gateway analysis" architecture can be extended in depth: explore the deployment of lightweight KPCA or

RBM feature extraction modules on cluster head nodes to achieve early threat awareness on the edge side, so as to deeply integrate with the edge computing framework; At the same time, blockchain technology can be introduced to store and trace the detection logs and model updates, in order to enhance the system's resistance to tampering and credibility. In the face of continuously evolving threats, future work can introduce deep reinforcement learning frameworks to dynamically adjust feature weights and classification thresholds, enabling the system to have online learning and adaptive defense capabilities, thus completing the evolution from static detection to dynamic adversarial. In summary, this work provides an effective solution to the security monitoring problem in damaged networks, and through the analysis of its limitations and the prospect of integrating edge intelligence, blockchain, and adaptive learning, lays the foundation for building the next generation of robust, trustworthy, and adaptive IoT security protection system.

Funding

This work was supported by the 2025 Soft Science Research Plan Project of Henan Province "Research on the Optimization Path of New Quality Productive Forces Empowering Enterprise-led Industry-University-Research Collaborative Innovation" (Grant No. 252400410121).

References

[1] M. Altuwairiqi. “An optimized multi-hop routing protocol for wireless sensor network using improved honey badger optimization algorithm for efficient and secure qos,” Computer communications, vol. 214, no. 1, pp. 244-259, 2024. https://doi.org/10.1016/j.comcom.2023.08.011

[2] A. Shilpi, & Kumar. “Application of jaya algorithm for solving localization problem in a distributed wireless sensor network,” Journal of Supercomputing, vol. 80, no. 5, pp. 6017-6041, 2024. https://doi.org/10.1007/s11227-023-05683-5

[3] E. Elmahfoud, S. Elhajla, Y. Maleh, & S. Mounir, “Machine learning algorithms for intrusion detection in iot prediction and performance analysis,” Procedia Computer Science, vol. 236, no. 1, pp. 460-467, 2024. https://doi.org/10.1016/j.procs.2024.05.054

[4] A. Souri, M. Norouzi, & Y. Alsenani, “A new cloud-based cyber-attack detection architecture for hyper-automation process in industrial internet of things.” Cluster computing, vol. 27, no. 3, pp. 3639-3655, 2024. https://doi.org/10.1007/s10586-023-04163-y

[5] M. S. Korium, M. Saber, A. Beattie, A. Narayanan, S. Sahoo, Pedro H. J. Nardelli, “Intrusion detection system for cyberattacks in the internet of vehicles environment,” Ad hoc networks, vol. 153, no. 2, pp. 1.1-1.16, 2024. https://doi.org/10.1016/j.adhoc.2023.103330

[6] M. Poongodi, & M. Hamdi, “Intrusion detection system using distributed multilevel discriminator in gan for iot system,” Transactions on Emerging Telecommunications Technologies, vol. 34, no. 11, pp. 1-18, 2023. https://doi.org/10.1002/ett.4815

[7] Yogesh, & L. M. Goyal, “Deep learning-based network intrusion detection system: a systematic literature review and future scopes,” International Journal of Information Security, vol. 23, no. 6, pp. 3433-3463, 2024. https://doi.org/10.1007/978-3-031-78255-8_13

[8] Gupta, Amara S. A. L. G. Gopala, S. P. Gudapati , and P. Tumuluru . "Securing wireless sensor network from node capture attack using an efficient optimization defense strategy model." Journal of Discrete Mathematical Sciences and Cryptography vol. 26, no. 5, pp. 1457-1472, 2023. http://doi.org/10.47974/jdmsc-1771

[9] S. Amaouche, A. Guezzaz, S. Benkirane, & M. Azrour, “A robust model for predicting abnormal behavior in vehicular networks using adaboost and chi-square,” Wireless Personal Communications, vol. 138, no. 4, pp. 2583-2611, 2024. https://doi.org/10.1007/s11277-024-11615-0

[10] B. Niccolò, F. Aromolo, L. T. X. Phan, & G. Buttazzo, “A convolutional autoencoder architecture for robust network intrusion detection in embedded systems,” Journal of Systems Architecture, vol. 156, no. 11, pp. 103283-103296, 2024. https://doi.org/10.1016/j.sysarc.2024.103283

[11] A. Karrothu, G. V. Sriramakrishnan, & V. Ragavi, “Gazelle - dingo optimization and ensemble classification: a hybrid approach for intrusion detection in fog computing,” Transactions on Emerging Telecommunications Technologies, vol. 36, no. 3, pp. 70084-70087, 2025. https://doi.org/10.1002/ett.70084

[12] A. S. Arkan, & M. Ahmadi, “An unsupervised and hierarchical intrusion detection system for software-defined wireless sensor networks,” Journal of supercomputing, vol. 79, no. 11, pp. 11844-11870, 2023. https://doi.org/10.1007/s11227-023-05117-2

[13] I. Mutambik, “An efficient flow-based anomaly detection system for enhanced security in iot networks,” sensors, vol. 24, no. 22, pp. 7408-7431, 2024. https://doi.org/10.3390/s24227408

[14] B. Zhang, X. Zhao, H. Wen, J. Wu, X. Wang, N. Dong, X. Yu, “The role of convolutional kernels in automated welding defect detection using t-sne and dbscan clustering,” Welding in the World, vol. 69, no. 5, pp. 1267-1275, 2025. http://doi.org/10.1007/s40194-025-01984-w.

[15] Z. Shen, X. Zeng, J. Wang, J. Liu, J. Lu, J. Ma, Y. Zhang, B. Fan, “Investigation of impairments separability in direct detection optical performance monitoring based on umap technique,” Optical

Review, vol. 31, no. 3, pp. 329-344, 2024. http://doi.org/10.1007/s10043-024-00878-4.

[16] MS. Alshehri, O. Saidani, WA. Malwi, F. Asiri, S. Latif, AA. Khattak, J. Ahmad, “A Hybrid Wasserstein GAN and Autoencoder Model for Robust Intrusion Detection in IoT,” CMES-COMPUTER MODELING IN ENGINEERING & SCIENCES, vol. 143, no. 3, pp. 3899-3920, 2025. https://doi.org/10.32604/cmes.2025.064874.

[17] W. Brian, SR. Raja, “An integrated hybrid model for cyber threat intrusion detection for satellite ground station networks using transformers and random forest,” International Journal of Scientific Research in Science, Engineering and Technology, vol. 11, no. 6, pp. 368-379, 2024. https://doi.org/10.32628/ijsrset2411463.

[18] H. M. S. Hatamleh, “Optimizing multi-tier scheduling and secure routing in edge-assisted software-defined wireless sensor network environment using moving target defense and ai techniques,” Future Internet, vol. 16, no. 11, pp. 386-413, 2024. https://doi.org/10.3390/fi16110386

[19] M. Bourdeau, J. Waeytens, & P. N. E. Aouani, “A wireless sensor network for residential building energy and indoor environmental quality monitoring: design, instrumentation, data analysis and feedback,” sensors, vol. 23, no. 12, pp. 5580-5608, 2023. https://doi.org/10.3390/s23125580

[20] Y. Xie, S. M. Beram, B. Kaur, R. Neware, M. Rakhra, & D. Koundal, “Research on visualization of large-scale user association feature data based on nonlinear dimension reduction method,” Journal of mobile multimedia, vol. 19, no. 2, pp. 587-602, 2023.

[21] Soegiharto, Irwin Santoso, and A. S. Girsang . "NoSQL Injection Detection Using Deep Neural Network and Principal Component Analysis of Injection Feature Vectors." International Conference on Computer, Control, Informatics and its Applications (IC3INA), pp. 7408-7431, 2024.https://doi.org/10.1109/ic3ina64086.2024.10732284

[22] R. Kirubahari, & A. S. M. Joe. “An improved restricted boltzmann machine using bayesian optimization for recommender systems,” Evolving Systems, vol. 15, no. 3, pp. 1099-1111, 2024. https://doi.org/10.1007/s12530-023-09520-1

[23] E. Park, S. Jang, G. Noh, Y. Jo, D. K. Lee, & I. S. Kim, et al., “Indium–gallium–zinc oxide-based synaptic charge trap flash for spiking neural network-restricted boltzmann machine,” Nano Letters, vol. 23, no. 20, pp. 9626-9633, 2023. https://doi.org/10.1021/acs.nanolett.3c03510

[24] E. Chappidi, & A. Singh, “A hyper-heuristic-based approach with naive bayes classifier for the reliability p-median problem,” Applied Intelligence, vol. 53, no. 22, pp. 27269-27289, 2023. https://doi.org/10.1007/s10489-023-04983-w

[25] X. Chen, G. Zhang, “Simulation of Fuzzy Random Mining of Big Data Based on Naive Bayes,” Computer Simulation, vol. 40, no. 11, pp. 428-432, 2023. https://doi.org/10.1515/jisys-2018-0020