PAN

Opto-Electronics Review

journal homepage: https://journals.pan.pl/opelre

Security detection method of illegal intrusion in optical transmission sensor networks based on a dual-path refinement attention mechanism

Mi Lin*, Huanyu Zhang, Xiaomin Liu, Yu Zhang, Jie Hong

Power Dispatching Control Center, Hainan Power Grid Co., Ltd., Haikou 570203, China

Article info

Article history:
Received 18 Jun. 2025
Received in revised form 28 Sep. 2025
Accepted 08 Oct. 2025
Available on-line 25 Nov. 2025

Keywords:
dual-path attention mechanism;
optical transmission sensor network;
trespassing;
safety testing;
convolutional attention module.

Abstract

This paper proposes a security detection method based on a dual-path refined attention mechanism to address the complex and variable illegal intrusion behaviours and low detection efficiency in optical transmission sensor networks. By constructing a multi-scale convolutional attention module, efficient fusion of local and global features can be achieved, combining ResNet50 structure optimisation with XGBoost classifier to improve the model ability to discriminate intrusion features and detection speed. The experimental results demonstrate that this method outperforms existing methods in terms of detection rate, real-time performance, and anti-interference capability, particularly in maintaining low network overhead under high attack densities. This study provides a reliable intrusion detection solution for optical transmission sensor networks, which is of great value in enhancing security protection capabilities in complex network environments.

1. Introduction

The research on security detection methods for illegal intrusion in optical transmission sensor networks is of far-reaching significance [1]. With the rapid development of information technology, optical transmission sensor networks are widely used in military, industrial, medical, and other fields, and their security problems are becoming increasingly prominent. Illegal intrusion may not only lead to the leakage and tampering of network data but also cause serious damage to the whole network system. Therefore, detecting illegal intrusion behaviours in optical transmission sensor networks is particularly crucial. This research is not only helpful in improving the security protection capability of optical transmission sensor networks, but it can also provide a reference for other types of network security detection. At the same time, with the rapid development of technologies such as the internet of things [2] and cloud computing [3], the application scenarios of optical transmission sensor networks will continue to expand, and their security issues will also face more complex and diversified challenges. Therefore, this study has important practical significance and strategic value for promoting the innovation and development of network security technology [4].

For the problem of sensor network intrusion detection, promising research results have been reported. Jing and Zhang [5] proposed an intrusion detection algorithm for wireless sensor networks based on blockchain technology. First, the monitoring mechanism in the blockchain is used to collect abnormal nodes in the wireless sensor network. Second, principal component analysis is used to extract the features of abnormal nodes. Then, a trust model is created based on the update and distribution of trust values. The extracted features are input into the model, and the trust value is output to complete the intrusion detection of wireless sensor networks. However, blockchain technology requires significant computing resources and storage space, especially in sensor networks, where node resources are limited. As a result, the overall system performance may be compromised because it cannot sustain the excessive computing burden. Liu *et al*. [6] proposed a wireless sensor network (WSN) intrusion detection method based on a bidirectional cyclic generation adversarial network. Adaptive learning attention detection (ALAD) is introduced

*Corresponding author at: lingmi1122@163.com

https://doi.org/10.24425/opelre.2025.156669
1896-3757/ Association of Polish Electrical Engineers (SEP) and Polish Academic of Sciences (PAS). Published by PAS

to reasonably represent high dimensional, discrete primitive features through potential spaces. Wasserstein distance and spectrum normalisation optimisation methods are introduced to improve the objective function of generative adversarial networks (GAN) to further solve the problems of pattern collapse and lack of diversity of GAN generators. Finally, since the statistical properties of the intrusion attack data change in an unforeseeable way over time, a fully connected layer network with dropout operation is built to optimise the anomaly detection results. However, the structure of the bidirectional cyclic GAN is complex and requires a lot of training data and computational resources to support its learning and optimisation process. Wang *et al*. [7] proposed an intrusion detection method for WSN based on an evolutionary game. By mapping the offensive and defensive confrontation of sensor networks to the game process, an offensive and defensive game model between malicious nodes and cluster-head nodes is established, and the traditional replication dynamic equation is improved to make cluster-head nodes consider the historical strategies of other nodes in the evolutionary game process to predict the attack strategy of malicious nodes. At the same time, the improved replication dynamic equation is applied to the intrusion detection algorithm to enhance its response time. However, the establishment of the evolutionary game model requires certain assumptions and preconditions that may differ from the actual network environment, which limits the model effectiveness. Karthic and Kumar [8] applied new intrusion detection system (IDS) to detect intruders on the wireless system communication through a complete description. Feature selection based on enhanced conditional random fields is proposed to select the features that contribute the most and an optimised hybrid deep neural network – a convolutional neural network (CNN) and a long short-term memory (LSTM) are used in the classification process. However, the training of neural networks requires a lot of labelled data and in the field of sensor network intrusion detection, the acquisition of labelled data is often difficult.

A review and analysis of existing research reveals that current detection methods have made significant progress in enhancing the performance of sensor network intrusion detection and adapting to complex network environments. Blockchain technology provides strong support for data trustworthiness and GAN have shown great potential in feature representation and anomaly detection. Evolutionary game models have opened new paths for attack, defence, and adversarial analysis, and hybrid deep neural networks have certain advantages in feature selection and classification. However, these methods also encounter many challenges. The limitations of computing resources and storage space, high-model complexity and training data requirements, deviations between assumptions and actual environments, as well as difficulties in obtaining annotated data, all pose constraints on the effective application of existing methods in illegal intrusion detection in actual optical transmission sensor networks.

The dual-path refinement attention mechanism is an effective deep learning method that can automatically learn and identify important features in input data. In the task of intrusion detection, the dual-path refinement attention mechanism can screen out key information related to intrusion from many network data, such as abnormal traffic patterns and intrusion behaviour characteristics. To this end, we propose a security detection method for illegal intrusion in optical transmission sensor networks based on the dual-path refinement attention mechanism. This method effectively captures complex features and key information in network data by designing convolutional attention modules for multi-scale spaces and channels. At the same time, through structural optimisation strategies, noise and redundant information interference are reduced and model discriminability is improved. Ultimately, combining extreme gradient boosting (XGBoost) technology to achieve efficient and accurate detection of illegal intrusion data provides an innovative and effective solution for the security protection of optical transmission sensor networks.

2. Detection model of illegal intrusion data in optical transmission sensor networks

2.1. Dual-path refinement attention mechanism

Data in optical transmission sensor networks are complex and diverse. The dual-path refinement attention mechanism is well suited to handle such complex data environments and can adapt to various network conditions and intrusion modes. Therefore, to enhance the learning ability of optical transmission sensor networks for detecting illegal intrusion feature information, an attention mechanism is employed in this paper to design a multi-scale space and channel convolution attention module [9]. The module can obtain spatial information of features at different scales, recalibrate features from the perspective of channels and spaces at multiple scales, establish long distance dependencies, and realise the interaction between local and global attention. Through a dual-path refinement, which focuses on both unique local and global features of the information in optical transmission sensor networks, the model can rapidly and accurately assess information security [10]. Local attention and global attention play different but complementary roles in feature information processing. Local attention is focused on specific regions or details of input data, capturing subtle feature changes, and is crucial for identifying local abnormal features in illegal intrusion. Global attention, on the other hand, is focused on overall features and long-range dependencies, which help to understand the overall structure and patterns of data and, thus, more accurately determine the overall security of information. The integration of these two attention mechanisms enables not only fine-grained processing of local information but also the detection of global trends, thereby collectively enhancing the model capability to learn and recognise features associated with illegal intrusion. Figure 1 shows the schematic diagram of an illegal intrusion feature extraction in the optical transmission sensor network.

Figure 1 shows the structure of the module. The specific steps are as follows:

Step 1: Input and Group Convolution.

Enter the intrusion feature graph $X(H \times W \times \mathrm{C})$ where $(H \times W \times \mathrm{C})$ is the size of each sub-feature graph. The first group convolution is carried out by a different size convolution kernel and different size group. Different convolution kernel sizes can obtain feature information [11]

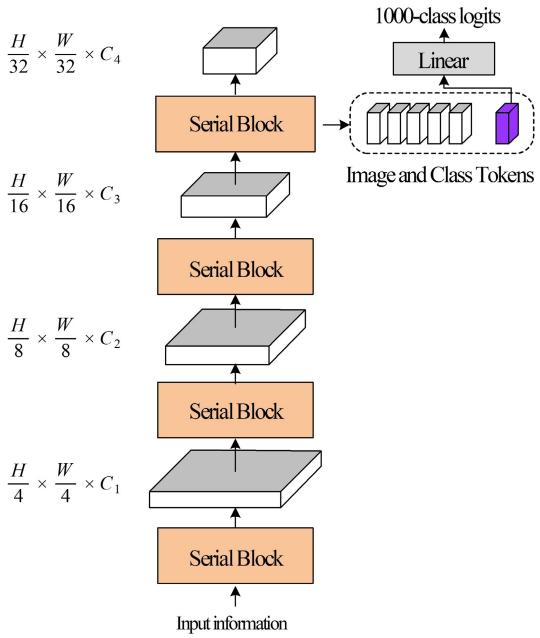


Fig. 1. Schematic diagram of an illegal intrusion feature extraction in the optical transmission sensor network.

and grouping convolution can reduce the number of parameters. Specifically, traditional convolutional layers apply the same convolution kernel to the entire input feature map, while grouped convolution limits each convolution kernel to apply only to a subset of the feature map (i.e., a group), resulting in a corresponding reduction in the number of parameters for each convolution kernel because their receptive field is limited to a smaller range. In addition, different sizes of convolution kernels can capture feature information at various scales and the introduction of grouped convolution further enhances the model flexibility and efficiency, significantly reducing its complexity and computational cost while maintaining feature extraction capabilities. Select convolution kernel $K(3, 5, 7, 9)$ to correspond to a group size $G(1, 4, 8, 16)$. The feature graph $X(H \times W \times \mathrm{C})$ is divided into four sub-feature graphs through segmentation of convolution layers with different convolution kernel sizes. The generation formula of multi-scale sub-feature graphs is as follows:

$$Q_i = X \cdot \mathrm{Conv}\left(K_i, G_i\right). \tag{1}$$

Step 2: Calculating Channel and Spatial Attention.
After obtaining each scale feature after segmentation, the weights W_c and W_s are obtained by channel attention and space attention, respectively, for different scale sub-feature graphs. Channel attention in the sub-feature graph is compressed along the channel direction through the global maximum pooling layer and the global maximum average layer. Different information is compressed through the connection layer, and then the vector length is restored to increase the network nonlinearity. Finally, the sigmoid function is activated to obtain the attention weight of the feature channel. The spatial attention module weights $H \times W$ pixels along the channel C to obtain the feature space attention weight. The use of a global max pooling layer and an average pooling layer can more comprehensively extract feature information, enhance the accuracy and effectiveness of attention. Compressing various types of information in the connection layer is necessary because the information extracted by different pooling operations varies and is relatively scattered. The connection layer can fuse and interact with information from different pooling paths achieving information reintegration and refinement during the compression process. It removes redundant information while retaining key features, providing more valuable input for subsequent vector length recovery and network nonlinearity enhancement. This enables the network to learn richer feature representations. The attention weight formula is as follows:

$$\begin{aligned} W_{ci} &= \mathrm{ChannelA}(Q) \\ W_{si} &= \mathrm{SpatialA}\left(Q_i\right) \end{aligned}, \tag{2}$$

where W_{ci} and W_{si} represent the channel and spatial attention weights.
Step 3: Feature Weight Fusion and Recalibration.
The spatial attention branch and channel attention branch are connected in parallel to obtain the feature weights extracted by the two-way attention and then fused and spliced to obtain the pixel-level feature weight vector W_i at different scales as follows:

$$W_i = W_{ci} \oplus W_{si}, \tag{3}$$

where $\oplus$ stands for the concatenation operation. In order to establish long-term channel attention dependence and spatial attention dependence and realise the information interaction between multi-scale attention, the Softmax function is further used to re-calibrate the weight of channel and spatial attention information. The weight assignment function F_i is as follows:

$$F_i = \mathrm{Softmax}\left(W_i\right) = \frac{e\left(W_i\right)}{\sum_{i=0}^{3} e\left(W_i\right)}. \tag{4}$$

Step 4: Feature Map Weighting and Splicing.
Multiply the sub-feature graph Q_i of each scale and the corresponding feature map Q_i after weight recalibration to obtain the attention-weighted sub-feature graph U_i, as shown below:

$$U_i = Q_i \odot Q_i^{'}, \tag{5}$$

where $\odot$ represents the channel multiplication operation. By splicing the sub-feature maps obtained by the attention weighting of dual-path refinement, the feature map F with richer feature information is obtained without destroying the original feature information, as follows:

$$F = F_i \times \mathrm{Cat}\left(U_i\right) = F_i \times \mathrm{Cat}\left[\left(U_0, U_1, U_2, U_3\right)\right]. \tag{6}$$

Through the detailed design and implementation steps mentioned above, the dual-path refined attention mechanism can effectively enhance the learning ability of optical transmission sensing networks for illegal intrusion feature information, providing stronger support for subsequent illegal intrusion detection.

2.2. Structure optimisation

With the increase in feature map information, rich feature maps may contain a lot of noise and redundant information, which can interfere with model extraction and recognition of key features. Without an effective mechanism for processing information, the model performance can degrade. To this end, the impact of noise and redundant information on model performance is reduced by simplifying the model structure and selectively focusing on the most important features. The specific operations are:
For the dual-path refinement attention mechanism, its network structure is usually the ResNet50 network structure, which contains four stages and the number of residual blocks in each stage is {3,4,6,3}. The size of the low-level feature information output in the first two stages is relatively large. Increasing the number of these two residual blocks will increase the richness of feature extraction to a certain extent, but it will also significantly increase the computational load and training time of the model. In practical applications, the increase in computational complexity and training time can lead to low-model training efficiency, and even the inability to complete training within a limited time. Although the size of the feature information extracted at the fourth stage is relatively small, there is less feature information in space, and deepening the layers does not allow for the extraction of useful information about the features related to illegal intrusion [12, 13]. In addition, the fourth stage extracts a relatively large number of feature information channels. If we continue to add deeper layers, it will further increase the number of parameters in the model, making it more complex and increasing the risk of overfitting. Therefore, to enhance the network ability to distinguish features extracted from illegal intrusion information without adding numerous additional parameters, the proportion of residual blocks in the third stage is increased and the feature extraction work of the third stage is deepened. In particular, the order of residual blocks was changed to {3,3,9,3}. After this adjustment, the third stage can extract more complete feature information and improve the model ability to capture illegal intrusion features.

In CNN, the down-sampling layer, located at the first layer of the model, shrinks the input information to a suitable size and performs feature extraction at various degrees of feature information [14, 15]. The first layer of the ResNet50 model is a down-sampling layer with a convolution kernel size of 7×7. Larger convolutional kernels have stronger feature extraction capabilities and can extract more complex features from information. However, this powerful feature extraction capability comes at the cost of increasing the number of model parameters. An excessive parameter count not only makes model training more difficult but also leads to overfitting of the model on the training data, thereby reducing its generalisation ability. Although smaller convolution kernels have fewer parameters, the model complexity is lower. However, small-sized convolution kernels can lose a significant amount of feature information during the feature extraction process, which affects the model ability to recognise illegal intrusion features. Therefore, in this paper, to balance model complexity and feature representation ability, the first layer of the residual network is replaced with a convolutional layer having a kernel size of 4×4 and a stride of 4. This substitution can reduce the number of model parameters to some extent, simplify the model, and retain sufficient feature information to ensure the effective extraction of illegal intrusion features by the model.

In the feature extraction stage, the optimised model first adjusts the ResNet50 structure, primarily by increasing the proportion of residual blocks in the third stage, to more fully extract feature information from the input data. The dual-path refinement attention mechanism plays a key role in this process. Through the convolutional attention module of multi-scale space and channels, the feature map is finely processed to obtain feature space information of different scales and the features are recalibrated to establish long-range dependencies. In this way, the model can more effectively capture key features related to illegal intrusion.

In the classification stage, the model inputs the extracted feature information into the classifier for processing, using the XGBoost technique. XGBoost consists of multiple weak learners (decision trees) to form a strong learner, which iteratively optimises the objective function, minimises the sum of the loss function and regularisation factor and obtains the optimal classification result. In the model presented in this article, the feature information processed by the dual-path refined attention mechanism is input into the XGBoost classifier. After being judged by the classifier, each data category is output to detect illegal intrusion data.

After optimising the dual-path refinement attention mechanism, a new and efficient network mechanism model is designed, as shown in Fig. 2.

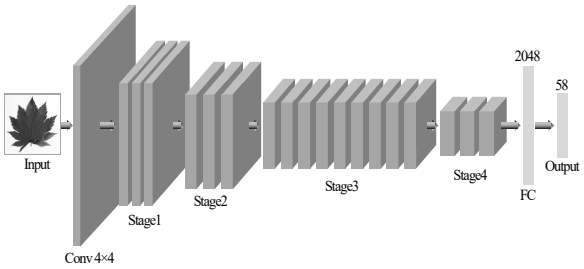


Fig. 2. Optimised structure of the attention mechanism.

The optimised model not only reduces noise and redundant information interference but also enhances the ability to extract illegal intrusion feature information, which is expected to achieve better detection results in practical applications.

To address the issue of high computational overhead and time consumption caused by the use of multiple convolutions and attention weights in the proposed model, depth-wise separable convolutions can be used instead of traditional convolutions to reduce parameter and computational complexity. Meanwhile, the attention mechanism should be streamlined by reducing the number of attention heads to lower its computational complexity. In addition, using model pruning techniques to compress the model size further improves computational efficiency and effectively reduces computational overhead and time while maintaining model performance.

2.3. Implementation of unauthorised intrusion data detection

Through the above steps, the dual-path refinement attention mechanism designed in this paper can weigh the feature information of channels and spaces at different scales of input information. Better information interaction between local and global attention enables the network model to extract richer information features and identify illegal intrusions more accurately.

Because XGBoost offers a fast classification speed and high precision, it is selected for classification to detect illegal intrusion data [16–18]. XGBoost consists of several weak learners (decision trees) that are combined to form a strong learner, arranged in the order of each weak learner. Generation of the latter weak learner will consider the judgment result of the previous weak learner, and the deviation of the previous weak learner will be taken into account to improve the classification accuracy of the decision tree [19]. The specific process is as follows:

(1) XGBoost classifier initialisation, using XGBoost to build s tree, using these trees to judge the category of each data, namely:

$$\hat{y}_{i_1} = F\sum_{j_1}^{s} f_{j_1}\left(x_{i_1}\right), \quad f_{j_1} \in \varepsilon, \tag{7}$$

where j_1 represents the certain tree; $f_{j_1}(\cdot)$ represents the leaf fraction of j_1, ε represents the set of decision trees and the solution process is as follows:

$$\varepsilon = \left\{ f\left(x^*\right) = w_q\left(x^*\right) \right\}, \tag{8}$$

where $f(x^*)$ represents the tree function, $w_q(x^*)$ represents the weight of leaf nodes and each leaf node represents the intrusion attack type of optical transmission sensor network [20].

(2) In order to optimise the prediction performance of the classification model, the minimum objective function is used to optimise the judgment results, namely:

$$Q^{(r)} = \sum_{i_1=1}^{n_2} Q\left(\hat{y}_{i_1}, y_{i_1}\right) + \sum_{j_1=1}^{s} Z\left(f_{i_1}\right), \tag{9}$$

where r represents the certain leaf, y_{i_1} represents the actual category to which x_1 belongs, $\left(\hat{y}_{i_1}, y_{i_1}\right)$ represents the loss function, i.e., the error between $\hat{y}_{i_1}$ and x_1, Z represents the regularisation factor, and the calculation process of Z is

$$Z(f) = \chi + \lambda \sum_{j_1=1}^{T} w_{j_1}, \tag{10}$$

where χ stands for the hyperparameter, λ represents the penalty factor and w_{j_1} represents the weight value of j_1.

(3) If the tree structure $q(x_{i_1})$ is fixed, the optimal weight w_{j_1} and q of the leaf j_1 are solved. In other words, the tree model iteration is regarded as an iteration of leaf nodes and the corresponding score of the best leaf node is obtained, namely:

$$w_{j_1}^* = \frac{g_{i_1}}{h_{i_1} + \lambda}, \tag{11}$$

Bring $w_{j_1}^*$ into $Q^{(r)}$ to obtain the final objective function value $Q^{(r)*}$, namely:

$$Q^{(r)^*} = \chi + \sum_{i_1=1}^{T} \frac{g_{i_1}}{h_{i_1} + \lambda}. \tag{12}$$

(4) Determine the termination conditions. If the number of iterations is equal to the limit value of model training iterations or the optimal classification result is found, the model training is ended, the classification result is output, and the illegal intrusion data is detected.

Based on the above content, the pseudo-code of the illegal intrusion data detection model for optical transmission sensor networks is as follows:

```
# Pseudo-code for Optical Transmission Sensor Network Illegal Intrusion Data Detection Model
# Define the Double-Path Refinement Attention Mechanism
function DoublePathRefinementAttention(input_feature_map):
    # Step 1: Input and Grouped Convolution
    grouped_feature_maps = []
    for kernel_size in [small_kernel, medium_kernel, large_kernel]:
        grouped_conv_output = GroupedConvolution(input_feature_map, kernel_size, corresponding_group_size)
        grouped_feature_maps.append(grouped_conv_output)
    # Step 2: Channel and Spatial Attention Calculation
    attention_weights = []
    for sub_feature_map in grouped_feature_maps:
        channel_weight = ChannelAttention(sub_feature_map)
        spatial_weight = SpatialAttention(sub_feature_map)
        attention_weights.append((channel_weight, spatial_weight))
    # Step 3: Feature Weight Fusion and Re-calibration
    fused_feature_weights = []
    for i in range(len(grouped_feature_maps)):
        channel_weight, spatial_weight = attention_weights[i]
        combined_weight = Concat(channel_weight, spatial_weight)
        recalibrated_weight = Softmax(combined_weight)
        fused_feature_weights.append(recalibrated_weight)
    # Step 4: Feature Map Weighting and Concatenation
    enhanced_feature_maps = []
    for i in range(len(grouped_feature_maps)):
        sub_feature_map = grouped_feature_maps[i]
        weight = fused_feature_weights[i]
        weighted_feature_map = ElementWiseMultiply(sub_feature_map, weight)
        enhanced_feature_maps.append(weighted_feature_map)
    final_feature_map = Concatenate(enhanced_feature_maps)
    return final_feature_map

# Define the Structure Optimization
function StructureOptimization():
    # Modify the ResNet50 structure
    original_stages = [3, 4, 6, 3]  # Original number of residual blocks in each stage
    optimized_stages = [3, 3, 9, 3]  # Optimized number of residual blocks in each stage
    # Replace the first convolutional layer
    original_first_layer = ConvLayer(kernel_size=7, stride=2)
    optimized_first_layer = ConvLayer(kernel_size=4, stride=4)
    return optimized_stages, optimized_first_layer

# Define the XGBoost-based Illegal Intrusion Data Detection
function XGBoostDetection(feature_data):
    # Initialize XGBoost classifier
    num_trees = 100
    xgboost_model = InitializeXGBoost(num_trees)
```

```
    # Define the objective function for optimization
    def objective_function(predictions, actual_labels):
        loss = CalculateLoss(predictions, actual_labels)
        regularization = CalculateRegularization(xgboost_model.trees)
        return loss + regularization
    # Train the XGBoost model
    for iteration in range(max_iterations):
        predictions = xgboost_model.Predict(feature_data)
        gradient = CalculateGradient(objective_function, predictions,
actual_labels)
        xgboost_model.Update(gradient)
        # Check termination condition
        if iteration == max_iterations - 1 or IsOptimal(predictions,
actual_labels):
         break
    # Output the classification result
    classification_result = xgboost_model.Predict(feature_data)
    return classification_result

# Main function to run the detection model
function Main(input_data):
    # Step 1: Apply Double-Path Refinement Attention Mechanism
    enhanced_feature_map =
DoublePathRefinementAttention(input_data)
    # Step 2: Apply Structure Optimization (conceptually, as actual
structure change is model-specific)
    optimized_stages, optimized_first_layer = StructureOptimization()
# This would be used in model construction
    # Step 3: Use XGBoost for Illegal Intrusion Data Detection
    detection_result = XGBoostDetection(enhanced_feature_map)
    return detection_result
```

Due to the structural optimisation in this article, the method reduces noise and redundant information and enhances the ability to extract illegal intrusion feature information. However, specific adjustments to the model structure may limit its flexible application in tasks of different scales and complexities, making it difficult to extend it directly to broader or more complex scenarios. Therefore, the method proposed in this article enables the design of a dual-path refined attention mechanism as an independent module, making it easy to embed into various neural network architectures and adapt to tasks of different scales and complexities. The introduction of configurable parameters in model design enables users to adjust the model structure according to specific task requirements, thereby achieving the optimal balance between performance and efficiency. Meanwhile, by using transfer learning techniques, pre-trained model parameters on large-scale datasets are used as initialisation parameters for fine-tuning specific tasks, thereby improving the model generalisation ability and scalability. Through these improvements, the model proposed in this article has better scalability while maintaining high performance and can adapt to a wider and more complex range of scenarios.

In the illegal intrusion data detection model proposed in this article for optical transmission sensor networks, overfitting is a crucial issue that needs attention. Due to the use of multiple convolutional layers and attention mechanisms, as well as a complex XGBoost classifier, the model has many parameters and is prone to overfitting on both training and testing data. In order to avoid overfitting, this paper takes various measures to reduce unnecessary parameters, especially adjusting the stacking mode of residual blocks in the ResNet50 network to avoid excessively deepening the network layers. At the same time, model pruning techniques are employed to further compress the model size and reduce its complexity. In addition, during the training process, regularisation methods are used to effectively monitor and prevent overfitting, ensuring that the model has good generalisation ability.

3. Experimental design and result analysis

To comprehensively verify the effectiveness and robustness of the proposed method, multiple sets of comparative experiments are designed in this paper to evaluate it from multiple dimensions, including detection accuracy, real-time performance, network overhead, and generalisation ability. The experimental platform was built using the ns-3 network simulator and simulated optical transmission sensing network environments of varying scales. The experimental data include normal traffic and various types of abnormal intrusion traffic, simulating real intrusion behaviour by injecting different types of attack packets.

3.1. Experimental setup

The optical transmission sensing network studied in this article is a hybrid network architecture based on the combination of fibre-optic sensing and wireless transmission. It has a characteristics of high bandwidth, low latency, and strong anti-interference ability, and is suitable for scenarios with extremely high-security requirements such as military, industrial monitoring, and smart cities. The network structure primarily consists of the following components: sensor nodes are deployed in the monitoring area, responsible for collecting changes in optical signals, such as vibration, temperature, and pressure, and converting them into electrical signals. The fibre-optic transmission link uses a single-mode fibre as the backbone transmission medium, supporting long-distance and high-capacity data transmission. Some wireless access points access the network through the IEEE 802.11b protocol, simulating real-life mobile terminals. The control centre is responsible for data aggregation, analysis, and intrusion detection tasks.

An optical transmission sensor network terminal with 80 nodes was constructed using the ns-3 platform. Within the identification range, 30 fixed routes were laid out on average, and 60 mobile terminals were placed arbitrarily. The initial time of the data flow experiment is 0 s and the remaining experimental parameters are shown in Table 1.

Table 1.
Experimental parameters.

Experimental parameter	Numerical value
Abnormal intrusion risk type	Random trespass
Transmission range	500 m
Packet size	1024 bytes
MAC type	The IEEE 802.11 b
Mobility model	Random waypoint model
Packet sending speed	300 kbps
Business type	User datagram protocol
Experiment time	120 s

To simulate abnormal intrusion behaviours of different intensities, this article classifies intrusion attacks based on indicators such as attack frequency, data volume, and node coverage, and sets simulation methods. Low-intensity attacks are used to simulate probing intrusions, with a set attack frequency of 1 to 5 abnormal data packets per second, and the number of target nodes does not exceed 10% of the total nodes. Medium-intensity attacks are used to simulate early or collaborative distributed denial-of-service (DDoS) attacks, with a set attack frequency of 5 to 20 abnormal data packets per second, and a target node coverage range of 10% to 30% of the total nodes. High-intensity attacks are used to simulate large-scale DDoS or network flooding, with a set attack frequency of at least 20 abnormal data packets per second, a target node coverage of at least 30% of the total nodes, and significant abnormal data traffic. The simulated attack types include data tampering, signal interference, illegal access, and replay attacks.

In addition to the above parameters, the parameters of the proposed optical transmission sensor network illegal intrusion security detection method based on the dual-path refinement attention mechanism are presented in Table 2. The reason for choosing these specific parameters is that they can comprehensively simulate the actual operating environment of optical transmission sensing networks and optimise the performance of detection models. The 80-node network and terminal layout built on the ns-3 platform, combined with parameters such as random waypoint models, can simulate real network scenarios and dynamic characteristics. The dual-path refinement attention mechanism module parameters include 3×3 and 1×1 convolution kernels, 64 output feature maps, and ReLU activation function, which can effectively capture multi-scale spatial and channel features. XGBoost classifier parameters, including 0.1 learning rate, 5 maximum tree depths, and 100 weak learners, can balance model complexity and generalisation ability. The training process parameters, including 64 batch sizes, 100 training epochs, and Adam optimiser, ensure stable convergence of the model. The early stop mechanism can prevent overfitting. The illegal intrusion classification label clarifies the detection target, jointly guaranteeing the accuracy and efficiency of illegal intrusion detection.

Table 2.
Algorithm parameters of the dual-path attention refinement mechanism.

Parameter class	Parameter name	Set value
Data set partitioning	Proportion of training sets	0.7
	Verify the set proportion	0.15
	Proportion of test sets	0.15
Dual refinement attention mechanism module	Spatial attention convolution kernel size	3×3
	Channel attention convolution kernel size	1×1
	Output the number of feature maps	64
	Activation function	ReLU
	Number of feature extraction stages	3
XGBoost classifier	Learning rate (eta)	0.1
	Maximum tree depth (max_depth)	5
	Number of weak learners (n_estimators)	100
	Objective function optimisation strategy	Minimise cross-entropy loss
Training process	Batch size (batch_size)	64
	Training rounds (epochs)	100
	Optimiser	Adam optimiser
	Initial value of learning rate	0.001
	Learning rate decay strategy	Decay 0.1 per 10 rounds
Early shutdown mechanism	Verification set performance did not improve the number of consecutive rounds	5
Trespassing label	Lawful act	0
	Trespassing	1

3.2. Verification process

Firstly, data collection and preprocessing are carried out to generate normal and abnormal data streams in the optical transmission sensing network through the ns-3 simulation. Multi-dimensional features, including packet size, transmission frequency, source/destination nodes, signal strength, etc., are extracted and standardised. Subsequently, the dataset was divided into training, validation, and testing sets in a ratio of 7:1.5:1.5.: training the dual-path refined attention mechanism model using the training set, using the validation set for parameter tuning and early stopping strategy and using the test set for final performance evaluation. For fair comparison, reference [7] (WSN intrusion detection method based on evolutionary game theory) and reference [8] (method based on a hybrid deep neural network) were selected as comparison benchmarks and run in the same experimental environment. The performance evaluation mainly uses detection rate, accuracy, F1 score, and running time as indicators, and draws receiver operating characteristic (ROC) curves to analyse the comprehensive performance.

3.3. Result analysis

After the above parameters are set, the data of the simulated terminal is illegally invaded, and the indicator signal is used to give early warning, as shown in Fig. 3. An illegal intrusion risk is identified when the intrusion signal indicator is set to 1. The results indicate that abnormal intrusion attacks occurred during the following intervals: 9–25 s, 43 s, 44–62 s, 70 s, 80–95 s, and 100 s.

It can be observed from Fig. 3 that the proposed method is based on a two-path refinement attention mechanism, which can quickly focus on key features in the input data through a convolution attention module of multi-scale spaces and channels. The design of the attention mechanism enables the model to automatically learn and identify the

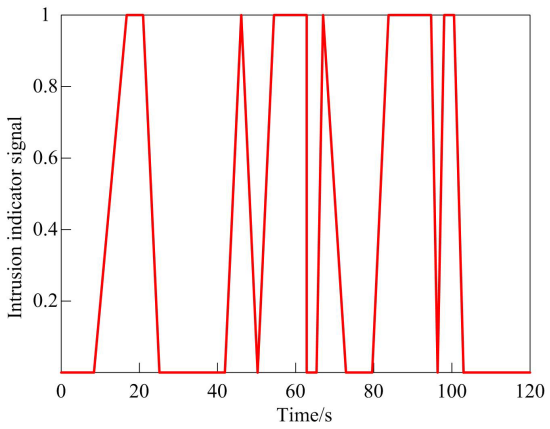


Fig. 3. Intrusion detection temporal response of the proposed method within 120 s.

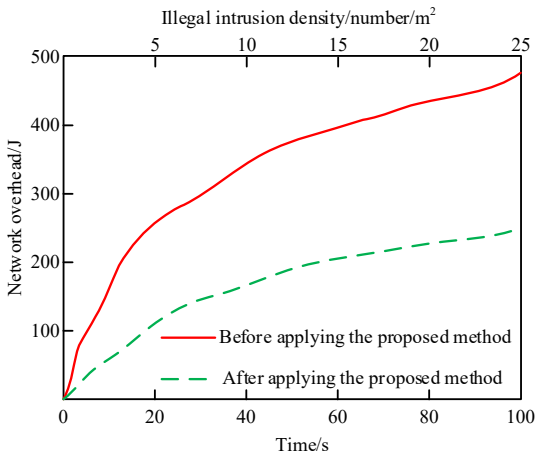


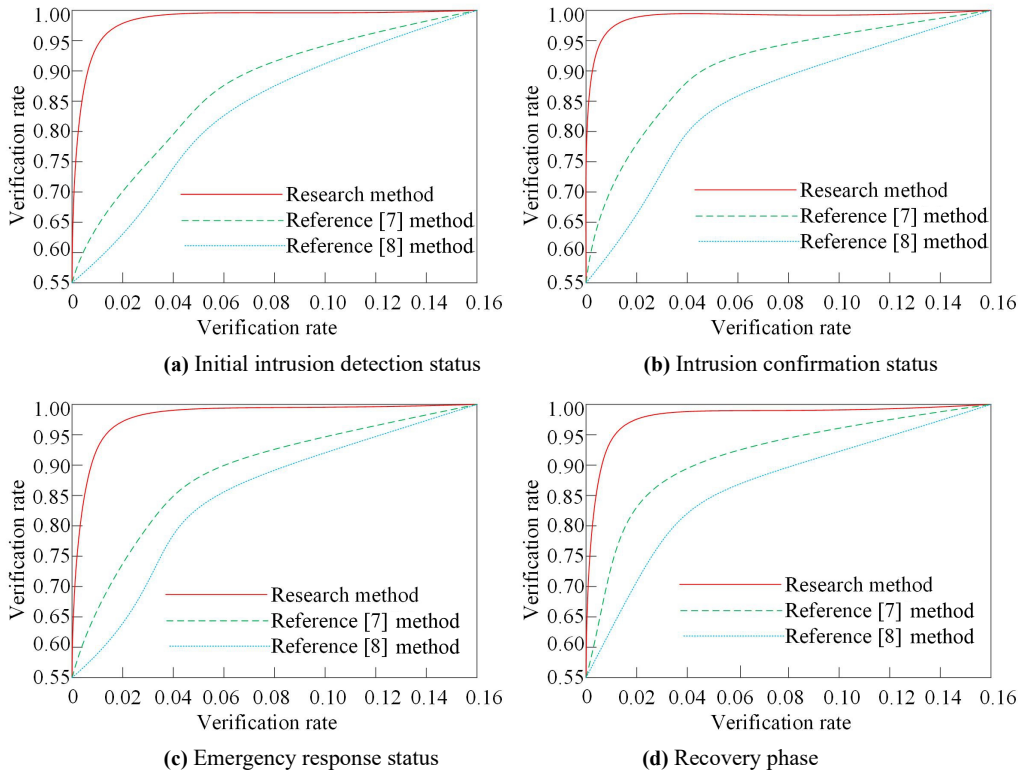
Fig. 4. Network overhead before and after the application of the proposed method.

key information related to illegal intrusion, so that the detection of intrusion can be completed in a short time. In addition, multiple weak learners (decision trees) in extreme gradient lift technology (XGBoost) are used for classification, which can quickly classify features and further shorten the detection time. Therefore, the proposed method can identify illegal intrusion attacks in a very short time.

Because terminal performance is related to intrusion density, the intrusion density determines the frequency of the original intrusion signal and interferes with signal reconstruction. Consequently, the network overhead in relation to intrusion density both before and after applying the proposed method was analysed. The results are presented in Fig. 4.

It can be seen from Fig. 4 that when the network starts running, the network intrusion density is high, and the network overhead is also high. With the continuous operation of the network, more abnormal data intrusion is identified, the intrusion density is gradually reduced, and the network cost is also reduced. A comparative analysis reveals a significant reduction in network overhead when the proposed method is applied. This improvement can be attributed to the dual-path refinement attention mechanism, which mitigates the interference from redundant information and noise through feature map optimisation, thereby reducing the computational resources required during model execution. At the same time, XGBoost algorithm itself has a high computational efficiency, and by optimising the objective function, it can further reduce the unnecessary computing overhead.

To measure the performance of different methods, they were compared with those in [7] and [8]. Two indices, accuracy rate and false alarm rate, are used. The ROC curves of the optical transmission sensor network after illegal intrusion were set as initial intrusion detection state, intrusion confirmation state, emergency response state, and recovery stage, respectively, as shown in Fig. 5 and Fig. 6.



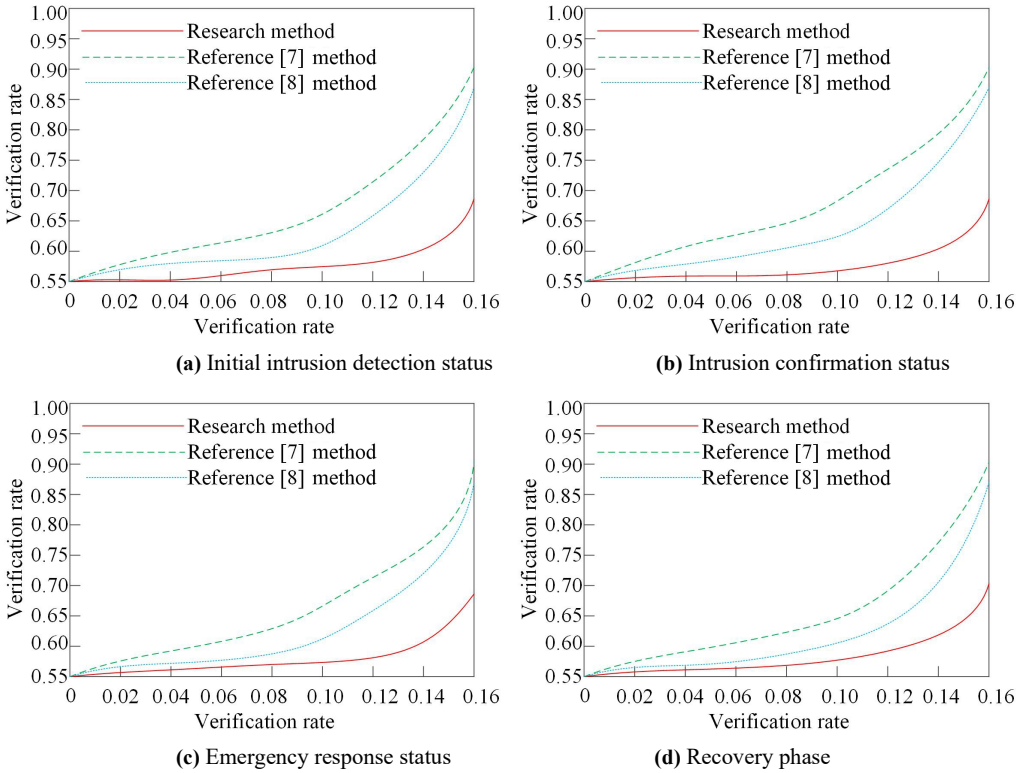
(a) Initial intrusion detection status

(b) Intrusion confirmation status

(c) Emergency response status

(d) Recovery phase

Fig. 5. ROC curve of accuracy under different network states.



(a) Initial intrusion detection status

(b) Intrusion confirmation status

(c) Emergency response status

(d) Recovery phase

Fig. 6. ROC curve of false alarm rate under different network states.

According to Figs. 5 and 6, compared with the methods in [7] and [8], the proposed optical transmission sensor network illegal intrusion security detection method, based on the dual-path refined attention mechanism, shows significant advantages in terms of accuracy rate and false alarm rate. This is because the dual-path refined attention mechanism improves the recognition ability of the model to illegal intrusion behaviour through refined feature extraction and attention allocation. At the same time, XGBoost algorithm enhances the generalisation ability and robustness of the model by integrating the prediction results of multiple weak learners. These advantages make the proposed method perform well in terms of detection rate and can accurately identify the illegal intrusion behaviour. In addition, by optimising the objective function and parameter settings, the model can reduce the possibility of miscalculation, thus reducing the false alarm rate. Therefore, the accuracy of the proposed method is high, and the false alarm rate is very low for the initial intrusion detection state, intrusion confirmation state, emergency response state, and recovery stage of the optical transmission sensor network after the occurrence of illegal intrusion.

In order to comprehensively evaluate the efficiency of the proposed method, small-, medium-, and large-scale optical transmission sensor networks were constructed using the ns-3 platform, with nodes, fixed routes, and mobile network terminals setup according to different scales. Meanwhile, low-, medium-, and high-intensity abnormal intrusion attacks were simulated in networks of different scales. The same experimental parameters as the original experiment were retained and compared with the methods in [7] and [8]. The detection rates, running times, accuracies, and F1 scores of each method were recorded in different scenarios. The experimental results are shown in Table 3.

According to the analysis in Table 3, in small-, medium-, and large-scale optical transmission sensor networks, regardless of the attack intensity being low, medium, or high, the research method exhibits significant advantages in detection rate, with detection rates reaching over 90%, which is higher than the methods in [7] and [8]. In terms of running time, the proposed method is also more efficient and can complete illegal intrusion detection in a shorter period. In addition, the research method also performs well in terms of accuracy and F1 score, indicating that it not only has high detection accuracy but also superior overall performance. In contrast, the performance of the methods in [7] and [8] is insufficient under different network sizes and attack strengths, particularly under high-intensity attacks, where their detection rates and accuracy are significantly lower than those of the research method. Therefore, the experimental results in Table 3 fully demonstrate the effectiveness and superiority of the research method in different scenarios.

To evaluate the feasibility and robustness of the proposed method in real network environments, experiments were conducted on the publicly available USTC-TFC2016 network traffic dataset. This dataset contains both malicious software traffic and normal traffic captured from real network environments, providing rich and realistic network behaviour characteristics. The results are shown in Table 4. According to Table 4, the proposed method, based on the dual-path refined attention mechanism, performs well on the real USTC-TFC2016 dataset, with an average detection rate of 98.2% and an average accuracy rate of 97.8%, significantly outperforming the comparative methods. This demonstrates that it is not only suitable for simulation environments but also capable of handling complex patterns and noise in real-world network traffic and has practical deployment potential. Statistical robustness

Table 3.
Comparison of the performance of various methods under different network sizes and attack strengths.

Network size	Attack power	Method	Detection rate (%)	Running time (s)	Accuracy (%)	F1 score
Small-scale	Low intensity	Research method	98	12.5	97	0.975
		Reference [7] method	92	15.2	91	0.915
		Reference [8] method	90	16.8	89	0.895
	Moderate intensity	Research method	96	13.8	95	0.955
		Reference [7] method	90	17.5	88	0.890
		Reference [8] method	88	19.2	86	0.870
	High strength	Research method	94	15.1	93	0.935
		Reference [7] method	86	20.5	84	0.850
		Reference [8] method	84	22.1	82	0.830
Medium-scale	Low intensity	Research method	97	18.3	96	0.965
		Reference [7] method	91	22.7	89	0.900
		Reference [8] method	89	24.5	87	0.880
	Moderate intensity	Research method	95	20.6	94	0.945
		Reference [7] method	88	26.2	89	0.870
		Reference [8] method	86	28.1	84	0.850
	High strength	Research method	96	23.2	92	0.925
		Reference [7] method	84	30.8	82	0.830
		Reference [8] method	82	32.7	80	0.810
Large-scale	Low intensity	Research method	96	25.8	95	0.955
		Reference [7] method	90	31.2	88	0.890
		Reference [8] method	88	33.5	86	0.870
	Moderate intensity	Research method	94	28.7	93	0.935
		Reference [7] method	86	36.1	84	0.850
		Reference [8] method	84	38.4	82	0.830
	High strength	Research method	92	32.3	91	0.915
		Reference [7] method	82	41.7	80	0.810
		Reference [8] method	80	44.2	78	0.790

Table 4.
Comparison based on the USTC-TFC2016 real dataset (10 cross-validation results).

Method	Detection rate (%) (mean ± standard deviation)	95% confidence interval (detection rate)	Accuracy (%) (mean ± standard deviation)	F1 score (mean ± standard deviation)	P-value compared to the proposed method
Research method	98.2 ± 0.5	[97.8, 98.6]	97.8 ± 0.6	0.980 ± 0.004	–
Reference [7] method	90.5 ± 1.8	[89.2, 91.8]	89.1 ± 2.1	0.898 ± 0.015	<0.001
Reference [8] method	92.3 ± 1.5	[91.2, 93.4]	91.0 ± 1.7	0.916 ± 0.012	<0.001

Note: p-value is calculated through a paired t-test to evaluate the statistical significance of the performance difference between the proposed method and the comparative method.

analysis shows that the detection rate of this method has a 95% confidence interval of [97.8%, 98.6%], with high repeatability and reliability. The standard deviation of various performance indicators is significantly smaller than that of the comparison method, resulting in minimal performance fluctuations, insensitivity to data sampling randomness, and excellent stability. The p-values compared with the comparative methods are all less than 0.001, indicating a highly significant and non-accidental performance advantage. In summary, this experiment strongly demonstrates that the proposed method has high detection performance and the robustness, stability, and

reliability required for deployment in practical optical transmission sensing networks, providing a key basis for its engineering application.

To conduct a more comprehensive and rigorous evaluation of the proposed method, the USTC-TFC2016 dataset from a real network environment was introduced for cross-domain validation based on the ns-3 simulation environment to evaluate the generalisation ability of the method. At the same time, expanding the scope of comparison benchmarks, in addition to including the original references [7] and [8], two representative deep learning models from recent times are also introduced, namely the transformer-based intrusion detection model (which embodies cutting-edge sequence modelling capabilities) and the lightweight MobileNetV2-based model (which embodies efficient computing). In addition, all results are based on statistics from 10 independent experiments, reported in the form of mean plus minus standard deviation and 95% confidence interval to verify their robustness. In terms of performance indicators, the number of new model parameters and the average inference time per sample are added to evaluate computational efficiency quantitatively. The results are shown in Table 5 and Table 6 .According to Table 5 and Table 6, the proposed method achieved the highest average detection rate of 98.2% and F1 score of 0.980 on the ns-3 simulation dataset. The extremely low standard deviation of ± 0.5 % and narrow 95% confidence interval [97.8, 98.6] demonstrate its high robustness, and its superiority is not accidental. In comparison with cutting-edge deep learning models (transformers), the proposed method has a more efficient advantage in capturing feature dependencies due to its designed dual-path refinement attention mechanism. Compared with the lightweight model (MobileNetV2), the detection accuracy is 5.7 percentage points higher, showing significant advantages. However, the parameter count, and inference time are higher, indicating that this study prioritises the pursuit of ultimate detection performance and provides solutions for nodes with certain computing power. It also suggests that in the future, lightweight backbone networks can be combined to strike a balance between performance and efficiency. The cross-domain validation on the USTC-TFC2016 dataset shows that the proposed method maintains the highest detection rate of 93.5% with a narrow confidence interval, demonstrating its strong feature representation generalisation ability and providing key evidence for practical deployment. The analysis of computational efficiency reveals that the proposed method achieves a lower inference time of 5.8 ms, compared to the complex transformer model at 12.3 ms and the traditional CNN-LSTM method at 8.1 s. The structural optimisation is effective, although not as good as MobileNetV2, the performance advantage is acceptable for most application scenarios. In the future, hardware testing can focus on verifying its real-time performance on embedded platforms equipped with GPUs or NPUs. In summary, this method not only performs robustly and optimally in simulation environments but also establishes advantages in extensive comparisons and has strong generalisation ability on real datasets.

To quantitatively evaluate the theoretical basis and relative contribution of key design choices in the method proposed in this article, rigorous ablation experiments were conducted. The experiment is divided into two parts: 1) Optimisation analysis of backbone network structure: By changing the stacking strategy of residual blocks ({3,4,6,3}, {3,3,9,3}) and the size of the first layer convolution kernel (7×7, 4×4), to verify its impact on feature discriminability and model efficiency; 2) Classifier selection analysis: Comparing the performance of XGBoost with mainstream classifiers such as *support vector machines* (SVM), random forest (RF), and lightweight gradient boosting machine (LightGBM) framework under the same dual-path refined attention feature extractor to demonstrate the advantages of XGBoost in this task. All experiments were conducted on the same training/validation/ testing set and the results were taken as the average ± standard deviation of 10 runs. The results are shown in Table 7.

Table 5.
Comparative analysis of comprehensive performance and efficiency.

Method	Detection rate (%) (mean ± standard deviation [95% confidence interval])	F1 score (mean ± standard deviation)	Model parameter quantity (million)	Single sample inference time (ms)
Research method	98.2 ± 0.5[97.8, 98.6]	0.980 ± 0.004	25.1	5.8
Transformer-based	95.1 ± 1.2[94.3, 95.9]	0.947 ± 0.010	38.5	12.3
MobileNetV2-based	92.5 ± 1.0[91.8, 93.2]	0.921 ± 0.008	3.2	1.5
Reference [8] method	92.3 ± 1.5[91.2, 93.4]	0.916 ± 0.012	15.7	8.1
Reference [7] method	90.5 ± 1.8[89.2, 91.8]	0.898 ± 0.015	–	2.0

Table 6.
Cross-domain validation results.

Method	Results
Research method	93.5 ± 1.0[92.8, 94.2]
Transformer-based	91.8 ± 1.5[90.8, 92.8]
MobileNetV2-based	88.9 ± 1.8[87.6, 90.2]

Note: "–" indicates that the method is a non-parametric model.

Table 7.
Analysis of ablation experiment results (performance indicators are mean ± standard deviation).

Experiment no.	Model configuration	Detection rate (%)	F1 score	Parameter quantity (M)	Inference time (ms)
A-1	Full model (Ours) (ResNet-{3,3,9,3} + first-layer 4×4 convolution + XGBoost)	98.2 ± 0.5	0.980 ± 0.004	25.1	5.8
A-2	Residual blocks {3,4,6,3} (original) + first-layer 4×4 convolution + XGBoost	96.5 ± 0.7	0.963 ± 0.006	23.9	5.5
A-3	Residual blocks {3,3,9,3} + first-layer 7×7 convolution (original) + XGBoost	97.8 ± 0.6	0.976 ± 0.005	38.6	7.2
A-4	Residual blocks {3,4,9,2} + first-layer 4×4 convolution + XGBoost (exploratory configuration)	97.1 ± 0.8	0.969 ± 0.007	22.5	5.3
B-1	Feature extractor (Ours) + LightGBM	97.8 ± 0.5	0.977 ± 0.004	–	4.1
B-2	Feature extractor (Ours) + Random Forest	96.0 ± 1.0	0.958 ± 0.009	–	3.5
B-3	Feature extractor (Ours) + SVM (RBF kernel)	94.3 ± 1.2	0.939 ± 0.012	–	6.0

According to Table 7, in terms of the rationality of optimising the backbone network structure, comparing the complete model A-1 with the original residual block configuration A-2, after adjusting the residual block from {3,4,6,3} to {3,3,9,3}, the detection rate significantly increased by 1.7% and the F1 score increased by 0.017, which strongly proves that concentrating computing resources in the third stage of the network can more effectively extract distinguished information of illegal intrusion from the mesoscale feature map. In the original configuration, the first and second stages introduce redundancy due to excessive deep numbers, and the fourth stage feature abstraction and insufficient spatial information result in limited benefits from deepening the layers. Comparing A-1 with A-3 using the original 7×7 convolution, the performance of both is comparable, but A-1 reduces the number of parameters by about 35% and improves inference speed by 19%. This indicates that replacing the first layer convolution kernel from 7×7 to 4×4 significantly reduces model complexity and computational overhead without sacrificing feature extraction capability, achieving an excellent balance between performance and efficiency. It is crucial for intrusion detection systems that require fast response. Exploratory configuration A-4 has lower performance than A-1, further indicating that {3,9,3} is a carefully considered optimal configuration. In terms of classifier selection criteria, when using the same feature extractor, A-1 achieves the highest detection rate and F1 score with XGBoost, outperforming B-1, which uses LightGBM. This is because XGBoost uses precise greedy algorithms, regularised targets, and deep capture of feature interactions to construct more discriminative models when processing features weighted by attention mechanisms and with complex dependencies. Compared with B-2 using RF, the XGBoost mechanism can more effectively reduce bias, obtain higher accuracy, and provide more stable results. Compared to B-3 using SVM, XGBoost does not require complex kernel function tuning, is insensitive to feature scales, is easier to train and deploy, and typically performs better in handling tabular feature data. Choosing XGBoost instead of LightGBM reflects the design philosophy of prioritising the maximisation of detection performance in this study. Although LightGBM has advantages in efficiency, XGBoost leads in accuracy and robustness, making it more valuable for security-critical intrusion detection tasks. This ablation experiment fully demonstrates the correctness of the core design selection from an empirical perspective. The targeted optimisation of the ResNet50 backbone network achieves the best balance between feature discriminability and model efficiency. The XGBoost classifier outperforms other mainstream alternative solutions in processing high-quality features generated by this method, which is a crucial link to achieving high-precision detection goals and provides solid data support for the methodology presented in the paper.

4. Conclusions

This article proposes a security detection method for illegal intrusion in optical transmission sensor networks based on the dual-path refined attention mechanism. Through multi-scale feature extraction and attention weighting mechanism, combined with structural optimisation and XGBoost classifier, the efficient and accurate identification of illegal intrusion behaviour is achieved. The experimental results demonstrate that this method outperforms existing mainstream methods in terms of detection speed, accuracy, and robustness. Especially when the attack density increases, it can still maintain low network overhead, demonstrating good practical potential.

However, the method proposed in this article still has certain limitations. Firstly, the model has a strong dependence on annotated data, and in practical deployment, the lack of sufficiently diverse annotated samples may affect its generalisation ability. Secondly, although the computational complexity has been reduced through structural optimisation, the combination of dual attention mechanism and XGBoost still requires certain computing resources, which may pose challenges when deployed on resource constrained edge nodes. Additionally, the adaptive ability of the proposed method in the face of new and unknown attack types requires further verification. Compared with unsupervised and self-supervised intrusion detection methods that have emerged in recent years (such as detection frameworks based on anomaly scoring or generative models), the adaptability in zero-sample or small-sample scenarios is weaker.

Compared to recent research, this method offers significant advantages in feature representation ability and classification accuracy, particularly with the introduction of a multi-scale spatial channel attention mechanism, which is innovative. However, compared with some intrusion detection methods based on transformer or graph neural networks, this method still has room for improvement in capturing long sequence dependencies or complex topological relationships. Future research can be conducted in the following directions: first, exploring the combination of lightweight attention mechanism and model compression technology to adapt to resource limited optical transmission sensing nodes; second, introducing semi-supervised or self-supervised learning strategies to reduce dependence on annotated data; third, integrating dynamic update mechanisms into the model to enhance online learning and adaptability to new types of attacks; fourth, expanding the ability of multimodal data fusion, combining optical signal characteristics with network traffic behaviour, and building a more comprehensive security perception system.

In summary, the method proposed in this article provides an effective technical approach for securing optical transmission sensor networks. In the future, it will be further optimised and expanded to promote its practical application in more complex and dynamic network environments.

Authors' statement

Writing – original and draft, writing – review and editing, M.L. and H.Z.; conceptualisation, methodology, project administration, data curation, formal analysis, resource, X.L., Y.Z., J.H.

Acknowledgements

This work was supported by science and technology projects of Hainan Power Grid Co., Ltd. research on 'Image analysis of breast histopathology based on deep learning method' (Project no. 070000KK52190020).

References

[1] Reyes-Vera, E. *et al*. Machine learning applications in optical fiber sensing: A research agenda. *Sensors* **24**, 2200 (2024). https://doi.org/10.3390/s24072200

[2] Jin, S. B. & Zhang, L. Detection of false data injection attack in internet of things based on Bayesian. *Comput. Simul.* **39**, 406–410 (2022). https://doi.org/10.3969/j.issn.1006-9348.2022.11.080 (in Chinese)

[3] Wang, Y., Bao, Q., Wang, J., Su, G. & Xu, X. Cloud computing for large-scale resource computation and storage in machine learning. *J. Theory Pract. Eng. Sci.* **4**, 163–171 (2024). https://doi.org/10.53469/jtpes.2024.04(03).14

[4] Kumar, N., Kasbekar, G. S., & Manjunath, D. Application of data collected by endpoint detection and response systems for implementation of a network security system based on zero trust principles and the Eigen Trust algorithm. *Perform. Eval. Rev.* **50**, 5–7 (2023). https://doi.org/10.48550/arXiv.2203.09325

[5] Jing, W. & Zhang, J. Wireless sensor network intrusion detection algorithm based on blockchain technology. *Chin. J. Sensor. Actuator.* **36**, 978–983 (2023). https://doi.org/10.3969/j.issn.1004-1699.2023.06.019 (in Chinese)

[6] Liu, Y. M., Yang, Y. J., Luo, H. Y., Huang, H. & Xie, T. Q. Intrusion detection method for wireless sensor network based on bidirectional circulation generative adversarial network. *J. Comput. Appl.* **43**, 160–168 (2023). https://www.joca.cn/CN/10.11772/j.issn.1001-9081.2021112001 (in Chinese)

[7] Wang, X. Y., Xing, H. Y., Hou, T. H. & Zheng, J. C. Research on wireless sensor network intrusion detection based on evolutionary game. *J. Electron. Meas. Instrum.* **37**, 97–105 (2023). https://doi.org/10.13382/j.jemi.B2306568 (in Chinese)

[8] Karthic, S. & Kumar, S. M. Hybrid optimized deep neural network with enhanced conditional random field based intrusion detection on wireless sensor network. *Neural Process. Lett.* **55**, 459–479 (2023). https://doi.org/10.1007/s11063-022-10892-9

[9] Chang, J. *et al*. Multi-scale attention network for building extraction from high-resolution remote sensing images. *Sensors* **24**, 1010 (2024). https://doi.org/10.3390/s24031010

[10] Mady, A., Gupta, S. & Warkentin, M. The effects of knowledge mechanisms on employees' information security threat construal. *Inf. Syst. J.* **33**, 790–841 (2023). https://doi.org/10.1111/isj.12424

[11] Yin, Z. *et al*. Deep CSI compression for massive MIMO: A self-information model-driven neural network. *IEEE Trans. Wirel. Commun.* **21**, 8872–8886 (2022). https://doi.org/10.1109/TWC.2022.3170576

[12] Mohy-Eddine, M., Guezzaz, A., Benkirane, S., Azrour, M. & Farhaoui, Y. An ensemble learning based intrusion detection model for industrial IoT security. *Big Data Min. Anal.* **6**, 273–287 (2023). https://doi.org/10.26599/BDMA.2022.9020032

[13] Rajalakshmi, R., Sivakumar, P., Prathiba, T. & Chatrapathy, K. An energy efficient deep learning model for intrusion detection in smart healthcare with optimal feature selection mechanism. *J. Intell. Fuzzy Syst* .**44**, 2753–2768 (2023). https://doi.org/10.3233/JIFS-223166

[14] Nayak, K. V., Arunalatha, J. S., Vasanthakumar, G. U. & Venugopal, K. R. Design of deep convolution feature extraction for multimedia information retrieval. *Int. J. Intell. Unmanned Syst.* **11**, 5–19 (2023). https://doi.org/10.1108/IJIUS-11-2021-0126

[15] Wang, S., Lin, S. & Yang, R. A lightweight convolutional neural network for multipoint displacement measurements on bridge structures. *Nonlinear Dyn.* **112**, 11745–11763 (2024). https://doi.org/10.1007/s11071-024-09673-x

[16] Majidian, Z., TaghipourEivazi, S., Arasteh, B. & Babai, S. An intrusion detection method to detect denial of service attacks using error-correcting output codes and adaptive neuro-fuzzy inference. *Comput. Electr. Eng.* **106**, 108600 (2023). https://doi.org/10.1016/j.compeleceng.2023.108600

[17] Guo, Z. Criminalisation of the illegal use of personal data: comparative approaches and the Chinese choice. *Humanit. Soc. Sci. Commun.* **12**, 782 (2025). https://doi.org/10.1057/s41599-025-05141-y

[18] Vladov, S. *et al*. Neural network method of analysing sensor data to prevent illegal cyberattacks. *Sensors* **25**, 5235 (2025). https://doi.org/10.3390/s25175235

[19] Choudhury, A., Mondal, A. & Sarkar, S. Searches for the BSM scenarios at the LHC using decision tree-based machine learning algorithms: a comparative study and review of random forest, AdaBoost, XGBoost and LightGBM frameworks. *Eur. Phys. J. Spec. Top.* **233**, 2425–2463 (2024). https://doi.org/10.1140/epjs/s11734-024-01308-x

[20] Attou, H., Guezzaz, A., Benkirane, S., Azrour, M. & Farhaoui, Y. Cloud-based intrusion detection approach using machine learning techniques. *Big Data Min. Anal.* **6**, 311–320 (2023). https://doi.org/10.26599/BDMA.2022.9020038