ingegneria sismica
International Journal of Earthquake Engineering
Anno XLIII - Num. 2 - 2026

Deep Learning-Based Multi-Modal Image Damage Detection and Cybersecurity Co-Optimization in Industrial IoT

Quntao Ma[1], *Shizhu Wu*[2,*], *Mingwei Liu*[3], *Chenyang Bu*[4] *and Xingda Gao*[4]

[1] Solution Expert, Yunding Technology Co., Ltd., Jining, 250000, Shandong, China
[2] Information Technology Department,Shandong Sunshine Digital Technology Co., Ltd., Binzhou, 256600, Shandong, China
[3] Information Technology Department,Shandong Jiuzhou Xintai Information Technology Co., Ltd., Jinan, 250000, Shandong, China
[4] The Network Security Lab,Yunding Technology Co., Ltd, Jinan, 250000,Shandong, China

SUMMARY: *In the industrial Internet of Things, deep learning-based multimodal image damage detection has been widely used in production quality inspection and safety assurance. Aiming at the problems of low real-time performance, high cost and incomplete coverage in current subway tunnel monitoring methods, this paper presents an improved LSGAN model to generate GPR images of tunnel damage and integrate a detection algorithm to identify tunnel defects, so as to realize high-precision detection of underground structural targets and concealed diseases.To resist the risks of network attacks and data tampering in subway tunnel damage detection systems, an ISSA-BiLSTM-based network security situation prediction model is proposed to predict the system security state in a fixed future period and provide decision support for network managers.Experimental results show that the proposed damage detection method achieves an average accuracy of over 70%. In terms of network security situation prediction, ISSA-BiLSTM has higher prediction accuracy than CNN-DBO-BiLSTM-Attention, CNN-IPSO-BiLSTM-Attention, IPSO-BiLSTM-Attention and BiLSTM models.*

KEYWORDS: *LSGAN model; GPR image; ISSA-BiLSTM; damage detection; cybersecurity*

1 Introduction

In recent years, the rise of the Industrial Internet of Things (IIoT) has brought profound changes to traditional industrial sectors. By embedding high-level connectivity and intelligent technologies into manufacturing links, IIoT platforms integrate large-scale interconnected equipment and sensors to realize efficient monitoring and management of industrial production activities [1]. This transformation has greatly boosted production efficiency while also posing new demands for structural and equipment damage detection.Damage detection aims to identify anomalies that deviate from normal working conditions, which may imply potential faults, external intrusions or other abnormal events [2, 3]. It supports the transformation from regular maintenance to predictive maintenance, thus reducing unexpected downtime, optimizing operational efficiency and improving system reliability. Nevertheless, with the deepening of digital transformation, the continuous growth of connected devices and sensing nodes in IIoT environments has significantly increased the difficulty of full-scenario damage detection [4].

*13365318522@163.com
https://doi.org/10.65102/is2026648
Published: 30 April, 2026

Industrial Internet of Things structures integrate a big number of monitoring terminals and sensors to support the smooth data sharing among staff, devices, and platform systems, thus enabling the real-time collection of data which reflect industrial production and running situation. On account of the complicated property of industrial working procedures and the complicacy of IIoT data, the recognition of abnormal states is exceedingly hard, and abnormal occurrences themselves are by nature infrequent. Therefore, carrying out labeling and annotation work for abnormal examples in large-scale IIoT data sets brings about extremely high costs [5-7]. In actual engineering usage scenarios, it is frequently hard or even not possible to get sufficient labeled abnormal samples from actual IIoT environments. Hence, the majority of current research work concentrates mainly on methods of unsupervised learning[8].

Traditional damage detection methods normally use a two-step tactic: firstly extracting very many hand-crafted features from industrial data, then utilizing outlier detection algorithms like clustering, one-class SVM and isolation forest to recognize abnormal conditions[9]. Zhou et al. [10]have made design of an intrusion detection system that combines kernel principal component analysis and extreme learning machine, in which KPCA is utilized for conducting dimension reduction on feature matrices. Experiment results indicate that this mixed model has higher efficiency and faster operating speed than the systems which only separately use ELM or SVM. In like manner, Gao and other researchers [11] have proposed a method which fuses incremental extreme learning machine together with adaptive principal component analysis, which can carry out adaptive screening of key features and therefore further increase the accuracy of detection.Alanazi and Aljuhani [12] presented an intrusion detection framework for IIoT networks consisting of data preprocessing, feature selection and classification modules. By using the X-IIoTID dataset, this method attains high detection accuracy and low false alarm rate. Nevertheless, these methods fail to compress the original feature dimension, leading to high overall computational cost. Other scholars have attempted feature selection strategies such as genetic algorithm and max-relevance min-redundancy algorithm. Kang and Kim [13] regarded feature selection as a combinatorial optimization issue and presented a local search optimization algorithm to select effective feature subsets for distinguishing normal and abnormal data. Although the selected feature subset performs better than the full feature set in terms of detection rate and accuracy, it brings a higher false alarm rate. Deng et al. [14] developed an enhanced one-class SVM method optimized by genetic algorithm for unsupervised anomaly detection in sensor data of large-scale IIoT systems. This method improves detection accuracy and efficiency while retaining the inherent structural characteristics of data.

One-Class Support Vector Machine (OCSVM) is a widely adopted anomaly detection approach that has been successfully applied in various fields. It constructs a decision boundary using normal samples and treats any points lying outside this boundary as anomalous events [15, 16]. Diez-Olivan et al. [17] introduced an OCSVM-based anomaly detection strategy that determines anomaly scores by measuring the separation distance between samples and the decision hyperplane, thereby detecting abnormal fluctuations in sensor data. For the further promotion of the detection performance of OCSVM, the hyperparameters of it were optimized by Yang and Zhou[18] through adoption of the Cloud Grey Wolf Optimization (CGWO) algorithm. This optimized model obtains a goodish balance between whole scope search and local refinement, hence enabling high detection rates and low false-positive rates, hence does not need additional feature engineering work. Zhang et al. [19] have made use of an Extended Boundary-based One-Class SVM (EB-OCSVM) for the detection of abnormal situations inside industrial control systems. This method can catch the cause-effect connections between variables, hence it permits correct abnormal thing finding and origin position confirming. Qu et al. [20]put together a Variational Autoencoder (VAE) and OCSVM to put forward a new

anomaly detection framework (VAE-OCSVM) that is made for IIoT cybersecurity. Contrast experiments have proven that its ability of distinguishing unusual points is better than basic algorithms. Guo and other researchers[21] have put OCSVM together with the CLOF clustering-based local outlier factor method, for the purpose of optimizing the decision boundary, and hence further enhancing the whole detection performance.However, traditional detection approaches still depend heavily on manual feature engineering, which becomes difficult under the high dimensionality and dynamic variability of IIoT data. For this reason, deep learning methods have been widely applied to IIoT anomaly detection in recent years.

Deep learning, as a branch of machine learning, refers to a class of intelligent algorithms with powerful autonomous learning abilities [22]. Since it does not rely on manual feature engineering, adapts well to dynamic industrial environments, and performs excellently in mining patterns from high-dimensional data, it has gradually become a mainstream technical solution to overcome the defects of traditional methods.A variety of deep learning models have been successfully applied to anomaly detection in Industrial Internet of Things scenarios, including convolutional neural networks (CNNs) [23], recurrent neural networks (RNNs) [24], long short-term memory networks (LSTM) [25], and others.For example, Yin et al. [26] combined CNN and recurrent autoencoders to detect anomalies in IoT systems, and designed a two-stage sliding window mechanism for the encoder to strengthen feature extraction effects.Khacha et al. [27] presented an anomaly detection scheme that fuses CNN and LSTM, which was verified on the Edge-IIoTset dataset. Experimental results demonstrated that the proposed method surpassed conventional machine learning algorithms in terms of accuracy, precision, false alarm rate and detection cost for both binary classification and multi-class classification tasks. Likewise, Nizam et al.[28] developed an end-to-end deep fusion detection framework for multivariate time series anomalies in IIoT. By integrating CNN and LSTM-based autoencoders, the method improves detection efficiency and accuracy while reducing manual intervention in model training.Anuradha et al. [29] built a deep learning detection framework based on CNN and RNN for large-scale industrial data, aiming to capture spatial and temporal correlations, alleviate model overfitting, and enhance the accuracy of intelligent anomaly detection.Laiq et al. [30] studied DDoS attack detection in edge IIoT networks using an integrated strategy combining decision trees, XGBoost, naive Bayes and SVM. Tests indicated that the XGBoost model achieved the best detection performance on the Edge-IIoT dataset.

Data in the Industrial Internet of Things and cybersecurity fields often comes from multiple modalities, each with different expression forms, data distributions, value scales and sample densities [31]. For example, industrial sensor data mainly includes temperature, pressure and other operating indicators collected by various sensing devices on the production site [32], while network traffic data is obtained through packet parsing and records key information such as source and destination addresses during transmission. These differences bring great difficulties to multimodal data fusion.To solve such problems, Jiang et al. [33] proposed a dedicated multimodal data analysis framework for IIoT scenarios. The framework adopts collaborative training and efficient inference mechanisms to optimize the training process of deep learning models and realize fast and low-resource inference. Considering the weak correlation between IIoT multimodal data and the lack of consistency constraints across modalities, Xiao et al. [34] used spatial trajectories to extract stay points, which were then transformed into feature vectors combined with surrounding points of interest. Through hierarchical clustering, these vectors form a tree structure to characterize user location history and support similarity measurement based on hierarchical graphs.Nagrani et al. [35] proposed an attention-guided bottleneck fusion method as an optimization strategy for multimodal interaction. By transferring information through a small number of bottleneck latent variables,

the model strengthens early fusion, improves fusion performance and reduces computational overhead. Nevertheless, current methods still face problems such as information redundancy or feature loss in feature-level fusion, and the model has insufficient ability to adapt to dynamic attack behaviors and emerging anomaly types.

This paper presents an intelligent monitoring system dedicated to subway tunnel safety. To overcome the shortage of labeled GPR samples for deep learning training, it adopts the LSGAN loss function combined with a convolutional neural network to generate high-quality GPR images. Furthermore, an intelligent detection algorithm based on the YOLOP framework is designed to identify tunnel structural damage, realizing efficient, non-destructive, and full-section intelligent inspection of subway tunnels.To ensure the cyber security of the entire monitoring system, a security situation prediction model is constructed. The model uses an improved BiLSTM structure with double stacked BiLSTM layers to enhance information extraction ability and improve prediction accuracy. Aiming at the shortcomings of the standard Sparrow Search Algorithm, the improved version integrates opposition-based learning and the Lévy flight mechanism to enhance optimization performance.The modified Sparrow Search Algorithm then optimizes multiple parameters of the BiLSTM neural network, thereby enhancing the accuracy of security posture prediction.

2 Design of a Damage Detection System for Subway Tunnels

This system is structured around three core functional modules: data collection and preprocessing, wireless data communication, and an intelligent monitoring and management platform. Within each shield tunnel segment, the sensor network is arranged at an optimized spacing of 2.5 kilometers. Meanwhile, the layout can be dynamically adjusted according to specific geological and structural conditions: for example, groundwater level monitoring is intensified near tunnel entrances and exits, while additional sensors for rock mass internal force and surrounding soil pressure are installed in sections with high bearing demands. Sensors are mainly installed on the tunnel lining and invert, focusing on six key indicators: groundwater level, surface cracking, peripheral displacement, surrounding earth pressure, internal force of surrounding rock, and linear settlement. The sensor models corresponding to each monitoring indicator are detailed in Table 1.

Table 1: The sensor models used for the six monitoring quantities

Name	Type
Internal force sensor	Bgk4200 concrete strain gauge
Peripheral soil pressure sensor	Bgk-4810 soil pressure box
Groundwater sensor	Bgk-4500s pressure sensor
Peripheral displacement monitoring sensor	Bgk-a3 multi-point displacement meter
Tunnel surface fracture sensor	Bgk-4420 surface crack meter
Tunnel linear sedimentation observation sensor	Two-dimensional laser array surface sensor

2.1 Data Collection and Processing

Multiple wireless sensors are employed to gather structural deformation and environmental monitoring data of the tunnel. On the sensor node controller, the STM32 microcontroller performs region-aware compressed data fusion. By integrating error elimination strategies, weighted data fusion algorithms, and threshold judgment mechanisms between cluster members and cluster heads, the scheme effectively improves data reliability, cuts down data transmission

traffic, and reduces the power consumption of sensor nodes. In this way, it enables more precise evaluation and early warning of potential safety hazards in subway tunnels.

2.2 Wireless Data Transmission

Data collected by sensor nodes is first transmitted to multiple aggregation nodes through LoRa wireless communication, then forwarded to wireless gateways via relay transmission. Ultimately, the gateways send all sensor data wirelessly to the remote monitoring and management platform. In the hardware and software design of each sensor node, energy efficiency is taken as a core indicator, so as to maximize the service life of nodes and realize the low-power operation of the entire safety monitoring system.

2.3 Data Intelligence Monitoring Management Platform

The intelligent monitoring and management platform allows real-time uploading of data acquired by automatic, semi-automatic and manual monitoring means. It supports functions such as abnormal data troubleshooting, visual data display, trend variation analysis, automatic report generation and SMS alarm notification once the preset early-warning thresholds are triggered.

2.4 Dual-Layer Wireless Sensor Monitoring Network

Considering the enclosed, long-strip and multi-line layout of subway tunnels, this design makes full use of the strengths of wireless sensor networks by dividing the tunnel into multiple monitoring areas, forming a dedicated network structure suitable for tunnel scenarios. Sensor nodes adopt a two-level deployment scheme: lower-level nodes collect data and send it to relay nodes, which then filter redundant information and forward effective data to gateways. This reduces data traffic, eases network load and prolongs network lifetime, improving the reliability, fault tolerance and stability of the monitoring network. To avoid network breakdown caused by single-point failure, each sensor node is covered by at least two relay nodes.

2.5 Key Technologies for Damage Detection

Once a subway tunnel is constructed, its underground placement leads to continuous interactions between the tunnel structure and the surrounding soil and groundwater. As a result, identifying and locating structural damage using measured data becomes considerably more complicated and difficult.

2.5.1 Ground Penetrating Radar Detection Technology

Ground penetrating radar detects underground structures by emitting high-frequency electromagnetic pulse signals through a transmitting antenna into the tunnel lining.When these electromagnetic waves encounter interfaces with dielectric differences within the lining, the soil behind the lining, or other surrounding media, reflected signals are generated. A receiver antenna captures these reflected signals and transmits them to the host computer for signal processing. Ultimately, through image reconstruction techniques, the distribution of underground structures is identified. The dielectric differences in the subsurface media determine variations in the intensity of the reflected signals. By analyzing information such as the amplitude, frequency, and phase of these reflected signals, characteristics of the subsurface target—including its shape, size, and material—can be determined [36]. When the transmission and reception distances of the GPR antenna are significantly shorter than the burial depth of the target, the following formula can be used to calculate the burial depth of the target:

$$h = \frac{ct}{2\sqrt{\varepsilon_r}} \tag{1}$$

In the equation, h represents the burial depth of the target object. c denotes the speed of electromagnetic waves in a vacuum. t indicates the round-trip propagation time of the GPR signal within the medium. ε_r signifies the relative permittivity of the subsurface background medium.

For calculating the round-trip propagation time, assume an ideal point scatterer is located at coordinate point (x, z), where x represents the antenna scan direction and z represents the subsurface depth direction. The transmit and receive antennas are positioned at coordinates Tx and Rx, respectively. In a homogeneous subsurface medium, the round-trip propagation time from the transmit antenna to any imaging point underground is:

$$t(x, z) = \frac{L_{Tx} + L_{Rx}}{v} = \frac{\sqrt{(x_T - x)^2 + z^2} + \sqrt{(x_R - x)^2 + z^2}}{v} \tag{2}$$

Here, v denotes the propagation velocity of electromagnetic waves within the subsurface medium, L_{Tx} and L_{Rx} represent the signal reflection paths from the transmit antenna to the imaging point and from the imaging point to the receive antenna, respectively, while x_T and x_R denote the horizontal coordinates of the transmit and receive antennas, respectively. The intensity of electromagnetic wave reflection at an interface primarily depends on the reflection coefficient R, expressed as:

$$R = \frac{\sqrt{\varepsilon_1} - \sqrt{\varepsilon_2}}{\sqrt{\varepsilon_1} + \sqrt{\varepsilon_2}} \tag{3}$$

Here, ε_1 and ε_2 represent the permittivities of the boundary material and the propagation medium, respectively. The reflection coefficient mainly describes the correlation in phase and amplitude between the incident wave and the reflected wave. A positive coefficient indicates that the reflected wave is in phase with the incident wave, while a negative value means the two waves are out of phase.

After completing GPR detection, the collected GPR data requires preprocessing to enhance the signal-to-noise ratio and highlight reflections from concealed defects behind subway tunnel walls. The specific steps for data preprocessing are as follows:

(1) DC Removal. Various noises and system biases may occur during data acquisition, leading to DC drift in the data. Removing DC improves the signal-to-noise ratio, reduces noise interference, and enhances data quality. This is achieved by subtracting the mean value (DC component) of the entire GPR profile from each sample point, as shown in the following equation:

$$X(n) = X_0(n) - \frac{1}{N}\sum_{n=1}^{N} X(n) \tag{4}$$

In the equation, X_0 and $X(n)$ represent the GPR signal before and after DC removal, respectively. N denotes the number of sampling points during detection, and n is the number of acquired channels.

(2) Time Gain. Linear time gain is applied to enhance the GPR reflection signal from voids behind the tunnel wall. Its expression is:

$$Y(t) = Y_0(t) \times vt \exp(\beta t) \tag{5}$$

In the equation, v represents the propagation velocity of electromagnetic waves within the tunnel, $Y_0(t)$ denotes the time-domain signal before gain amplification, t is the round-trip transit time from emission to reception, and β represents the attenuation coefficient.

(3) Bandpass Filtering (BPF). A BPF employing a trapezoidal window function is applied to suppress low signal-to-noise ratio frequency components in GPR data:

$$Y(f) = \begin{cases} 0, & f < f_1 \\ \sin^2 \dfrac{\pi}{2}\left(\dfrac{f - f_1}{f_2 - f_1}\right), & f_1 \le f \le f_2 \\ 1, & f_2 < f < f_3 \\ \sin^2 \dfrac{\pi}{2}\left(\dfrac{f_4 - f}{f_4 - f_3}\right), & f_3 \le f \le f_4 \\ 0, & f > f_4 \end{cases} \tag{6}$$

In the equation, f_1, f_2, f_3, and f_4 represent the filter threshold frequencies. For the BPF in this section, the threshold frequencies are $0.1f_c$, $0.3f_c$, $1.2f_c$, and $1.6f_c$ (f_c denotes the center frequency of the GPR antenna). Additionally, the BPF is further employed in this paper to mitigate the impact of noise from subway shield tunnel segment joints on GPR data.

(4) Zero-time correction. In the zero-time correction process described in this chapter, the starting time of the GPR profile is adjusted to align with the surface of the subway tunnel lining. Specifically, the zero-time value is set to the first positive peak of each A-scan direct wave.

2.5.2 Improved Least Squares Generative Adversarial Network (LSGAN)

Traditional GANs exhibit relative instability during image generation and are prone to non-convergence during training, resulting in suboptimal image convergence outcomes. Furthermore, the instability of GANs can lead to underfitting or overfitting when generating GPR images. Therefore, generating high-precision GPR images using GAN networks necessitates adjusting the network parameters and implementing improvements.

LSGAN improves the cross-entropy loss function by incorporating the discriminator D's least-squares loss function, enabling it to generate GPR images that more closely resemble reality than traditional GANs. The loss functions for LSGAN's generator and discriminator are defined as follows:

$$\min_{D} V_{LSGAN}(D) = \frac{1}{2} E_{x \sim P_{data}} [D(x) - b]^2 + \frac{1}{2} E_{z \sim P_z} \left[(D(G(z)) - a)^2 \right] \tag{7}$$

$$\min_{G} V_{LSGAN}(G) = \frac{1}{2} E_{z \sim P_z} \left[(D(G(z)) - c)^2 \right] \tag{8}$$

Here, a represents the label of the generated data, b denotes the label of the actual GPR data, and c is the threshold set by the generator G for the discriminator D to determine whether the generated GPR image approximates the real data.

In this part, in order to promote the accuracy of GAN-produced GPR pictures, the LSGAN network frame is changed. When one compares with traditional GANs, the improved LSGAN uses CNNs for the smoothing of generator gradients, and for the enhancement of the stability of adversarial training. Therefore, this reduces pattern collapse in the training process, and hence increases the diversity of generated GPR images. In addition, the training that uses LSGAN's loss function can make the speed of model convergence become faster.

2.5.3 YOLOP Model

YOLOP is one detection algorithm which is based on convolution nerve network, it can make multi-task identification in one single model. When we use it to find hidden flaws in subway tunnel GPR pictures, the YOLOP framework can at the same time achieve flaw checking and concrete lining thickness cutting division. The model which this study uses is made up of a shared encoder structure that is followed by two independent decoders[37].

(1) Encoder

The sharing coder of the YOLOP model is composed by a backbone network and a neck network. The skeleton network, which is built on the CSP-Darknet structure, undertakes the task of extracting features from the input GPR images. This backbone network is able to effectively reduce the problem of gradient vanishing that appears during the optimization process, hence it can enhance both the convergence speed and the stability of training work. In order to make feature representation have stronger ability, the neck component carries out the integration of the SPPF module and the FPN module. The SPPF module carries out multi-scale characteristic drawing and combination, while the FPN module combines semantic messages from characteristic drawings at different layers. All these modules together promote the feature extraction ability for GPR images that have internal defects, therefore therefore increasing the accuracy of the detection and segmentation branches which come after.

(2) Decoder

In this network segment, two independent decoders are adopted to perform detection and segmentation tasks separately. For the concealed defect detection branch, a Path Aggregation Network (PANet) is utilized to propagate semantic and location features in a bottom-up FPN structure, which further enhances the feature fusion performance.The detection module adopts an anchor-based multi-scale detection strategy similar to YOLOv4, and directly extracts multi-scale fused features from PANet for the identification of concealed defects.For the segmentation of lining thickness, a special segmentation branch based on FPN is designed. To boost computational efficiency, we replace deconvolution upsampling with nearest-neighbor interpolation. This interpolation strategy not only cuts down computational overhead but also retains high-precision outputs, enabling rapid and accurate prediction of concrete lining thickness.

3 Performance Analysis of Damage Detection Methods

The models in this chapter are validated using the public RDDC2022 dataset, which contains annotated markings for approximately 55,000 damage instances across different types.All annotation information is stored in XML files following the PASCAL VOC specification.To assess the experimental outcomes quantitatively, this chapter uses precision, recall, F1 score (the harmonic mean of precision and recall), and average precision (AP) as key evaluation indicators to reflect model detection accuracy and overall performance.The effectiveness of the model is evaluated by aligning the predicted bounding boxes output by the detection model with the manually annotated ground-truth boxes in the dataset, so as to verify the accuracy and dependability of detection.

In the comparative experiments, several representative object detection models are selected as benchmarks, including the YOLO family (YOLOv5s, YOLOv6s, YOLOv8n), Faster R-CNN, RetinaNet, SSD, FCOS, and EfficientDet. The experimental results are analyzed both qualitatively and quantitatively.The dataset divides tunnel distress into three categories: D00 longitudinal cracks, D20 network cracks, and D40 potholes. The dataset is split into training, validation, and test sets at a ratio of 8:1:1, containing 400, 50, and 50 samples respectively.

Tables 2 and 3 respectively present the comparative test outcomes on the RDD2022_USA and RDD2022_Japan damage datasets. As reflected in the results, the model proposed in this study holds clear advantages across the three types of defect detection tasks. Its detection accuracy remains above 70%, and the overall performance is comparable to that of mainstream detection frameworks. This fully verifies the reliability and validity of the damage detection method proposed in this section.

Table 2: Comparative experimental results on the RDD2022_USA injury dataset

Algorithm	mAP@50	D00 AP@50	D20 AP@50	D40 AP@50
YOLOv5-s	51.5	67.4	58.4	27.3
YOLOv6-s	51.5	70.8	62.6	22
YOLOv8-n	49	68.4	59.7	23.5
Faster R-CNN	39	47.5	46.5	26.4
RetinaNet	49.1	57.8	63	29.6
SSD	44.8	48.3	47.5	34.6
FCOS	52.7	72.5	62.3	21.1
EfficientDet	45.1	61.7	61	2.3
Ours	84.3	74.8	73	72.4

Table 3: Comparative experimental results on the RDD2022_Japan injury dataset

Algorithm	mAP@50	D00 AP@50	D20 AP@50	D40 AP@50
YOLOv5-s	58.3	41.7	67.4	57.5
YOLOv6-s	57	46.6	63.8	56.2
YOLOv8-n	54.8	44.2	62.8	54.1
Faster R-CNN	29.3	21.5	55.5	28.4
RetinaNet	51.1	45	65.2	53
SSD	42.4	30.6	53.1	38.4
FCOS	55.2	43.2	65.8	60.3
EfficientDet	53.2	57.2	58	46.9
Ours	87.3	78.6	76.6	72.4

4 Cybersecurity Optimization for Damage Detection Systems

The subway tunnel damage detection system relies on large-scale data collection, transmission, and storage, supported by an extensive network architecture. These characteristics place higher cybersecurity demands on the system. In the event of a network intrusion or data tampering attack, serious threats may arise for the operational safety of subway trains and daily maintenance work.To defend against cyberattacks and ensure data security and detection accuracy, this paper combines an improved Sparrow Search algorithm with a BiLSTM neural network to propose a cybersecurity posture prediction model for subway tunnel damage detection systems.

4.1 ISSA Optimizes and Improves the BiLSTM Model

4.1.1 Improvements to the BiLSTM Network Architecture

The proposed cybersecurity threat prediction model based on a double-layer BiLSTM comprises a double-layer BiLSTM, a dropout layer, and a dense layer.

(1) The two-layer BiLSTM structure makes full use of the inherent information in time-series data, thereby achieving more excellent prediction performance.

(2) The dropout layer effectively suppresses overfitting and improves the model's ability to generalize to unseen data.

(3) The fully connected layer adjusts the output dimension to generate the final prediction results.

For simpler prediction targets in the past, traditional single-layer BiLSTM neural network structures could achieve relatively accurate results. However, with the diversification of cyberattacks and the increasing complexity of industrial IoT environments, the relational information within time series often becomes difficult to discern. To achieve superior prediction performance, it is necessary to learn the deep-level correlations among data points in the time series. Traditional BiLSTM neural networks may only uncover superficial data associations, resulting in suboptimal prediction accuracy. Therefore, a stacked two-layer BiLSTM neural network architecture is proposed to uncover deeper relationships within the time-series data.

Dropout is a regularization technique that randomly discards a proportion of nodes during training to mitigate overfitting. This reduces the complexity of interactions between nodes.

The fully connected dense layer plays an essential role in the structure. It maps the nonlinear features learned by the preceding layers into the final output space, enabling effective interpretation of the high-level semantic information extracted earlier. The resulting prediction represents the overall cybersecurity state of the damage detection system in the upcoming time period, which can also be regarded as a classification task in essence.

Stacking two BiLSTM layers effectively boosts prediction accuracy and enhances the overall performance of the model. However, deep multi-layer structures also introduce drawbacks including longer computing time and a sharp rise in the number of trainable parameters. Cybersecurity situation prediction for damage detection systems demands high real-time performance. A delayed prediction result may prevent security administrators from taking timely IIoT protection measures, leaving key security risks unresolved, which is not permissible in engineering practice.Accordingly, the performance of the BiLSTM-based cybersecurity threat prediction model still needs to be further optimized.

4.1.2 ISSA Optimization of BiLSTM Network Parameters

(1) Reverse Learning Strategy

The reverse learning strategy is an optimization technique frequently applied in swarm intelligence algorithms. In classical SSA, the initial population is randomly generated, with sparrows potentially clustering in one area or dispersing across multiple regions, slowing the algorithm's convergence speed. Therefore, the reverse learning strategy is introduced to generate the initial population for the Sparrow Search Algorithm, employing adversarial search instead of random search.

Assume the randomly generated initial population is:

$$X = \left[x_1, x_2, \ldots, x_n\right] \tag{9}$$

The initial population X corresponds to the inverse population $\bar{X}$ as follows:

$$\bar{X} = [\, x_1', x_2', \ldots, x_n' \,] \tag{10}$$

Definition:

$$\bar{X} = Ub + Lb - X \tag{11}$$

Ubrepresents the upper bound of the search space, while Lb stands for its lower bound. After merging populations P and Q, all N sparrow individuals are sorted in ascending order according to their fitness values, and the top N individuals with the optimal fitness are chosen as the ultimate initial population.

(2) Lévy Walk Strategy

A Lévy walk is a random walk composed of clusters of short steps and long steps. An example of a Lévy walk is shown in Figure 1. Its step length probability exhibits a “heavy tail” characteristic, meaning there is a significant probability of large jumps occurring during the random walk.

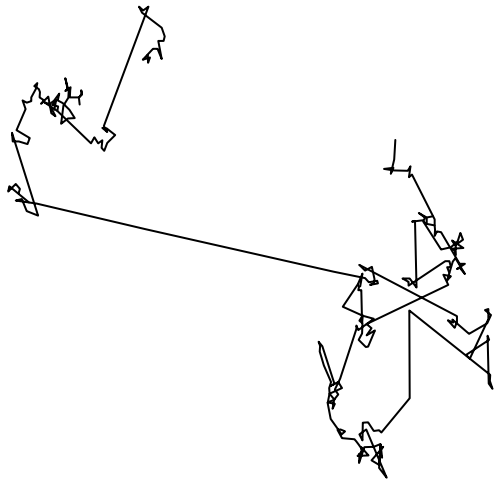

Figure 1: Lévy flight example

Standard SSA is prone to getting stuck in local optima. If a global optimum is not found, the optimization task cannot be completed. The Lévy flight strategy, while following a small-step random walk, also has a significant probability of taking large leaps. This indicates that the Lévy flight strategy is capable of balancing local exploitation and global exploration abilities. Accordingly, this study introduces the Lévy flight mechanism into the position update equation for the scrounger sparrows. Since the optimal position of the sparrow in the Sparrow Search

Algorithm is continuously updated, the improved SSA avoids getting stuck in local optima. The modified position update formula for the freeloader is as follows:

$$x_{i,j}(t+1)=\begin{cases} Q\cdot \exp\left(\dfrac{x_{worst}(t)-x_{i,j}(t)}{t^2}\right), & i>\dfrac{n}{2} \\ x_b(t+1)+x_p(t+1)\otimes Levy(d), & \text{Other} \end{cases} \tag{12}$$

where d represents the vector dimension, the Lévy flight strategy calculation formula is as follows:

$$Levy(x)=0.01\times\frac{r_3\times\sigma}{|r_4|^{\frac{1}{\xi}}} \tag{13}$$

Where r_3 and r_4 are both random numbers between 0 and 1, the value of ξ can be set to 1.5, and the formula for calculating σ is as follows:

$$\sigma=\left(\frac{\Gamma(1+\xi)\times\sin\left(\frac{\pi\xi}{2}\right)}{\Gamma\left(\frac{1+\xi}{2}\right)\times\xi\times 2^{\frac{\xi-1}{2}}}\right)^{\frac{1}{\xi}} \tag{14}$$

Among them $\Gamma(x)=(x-1)!$.

(3) ISSA-Optimized BiLSTM Neural Network Parameter Process

This paper introduces a reverse learning strategy and Lévy flight strategy to optimize the Sparrow Search Algorithm (SSA), yielding an initial population with improved fitness. This mitigates SSA's tendency to get stuck in local optima, ensuring both local and global search capabilities and enhancing algorithm performance. The steps for optimizing BiLSTM neural network parameters using the improved SSA are as follows:

1) Configure the structure of the enhanced BiLSTM network and define the neuron count for both the input and output layers.

2) Configure the initial parameters of the improved sparrow search algorithm, including population size, maximum iteration count, producer ratio, scout ratio, and early warning threshold.

3) Define the dimensions of the sparrow population and their value ranges. These dimensions represent the number of model iterations, dropout rate, and the number of units in each hidden layer of the BiLSTM neural network.

4) Define the fitness function for the sparrow search algorithm. Generate the initial population randomly, compute the fitness value of each sparrow individual, adopt a reverse learning strategy to determine the final initial population, and record the current optimal solution.

5) Calculate the fitness values of sparrow individuals, update the optimal solution, and adjust the positions of leaders, followers, and sentinels according to the formula.

6) If the maximum iteration count is reached, proceed to the next step; otherwise, return to the previous step and continue iteration.

7) Obtain the optimal parameters for the BiLSTM model.

8) Perform cybersecurity situation prediction to obtain the prediction results.

The flowchart for ISSA-optimized BiLSTM network parameter adjustment is shown in Figure 2.

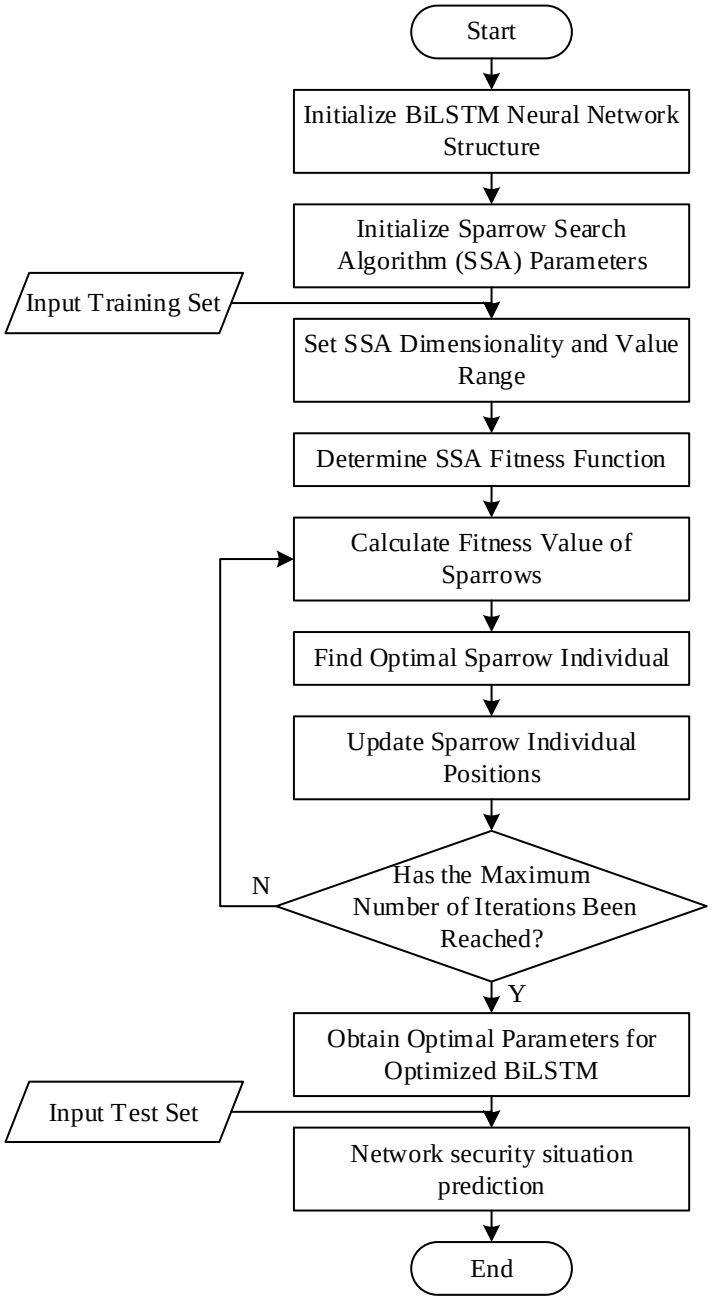

Figure 2: Flowchart of ISSA optimizing BiLSTM network parameters

4.2 Cybersecurity Situation Forecasting Model Based on ISSA-BiLSTM

Based on the aforementioned process of adopting ISSA-optimized BiLSTM network parameters, this paper constructs an ISSA-BiLSTM-based cybersecurity threat prediction model. The ISSA-BiLSTM cybersecurity threat prediction framework is illustrated in Figure 3.

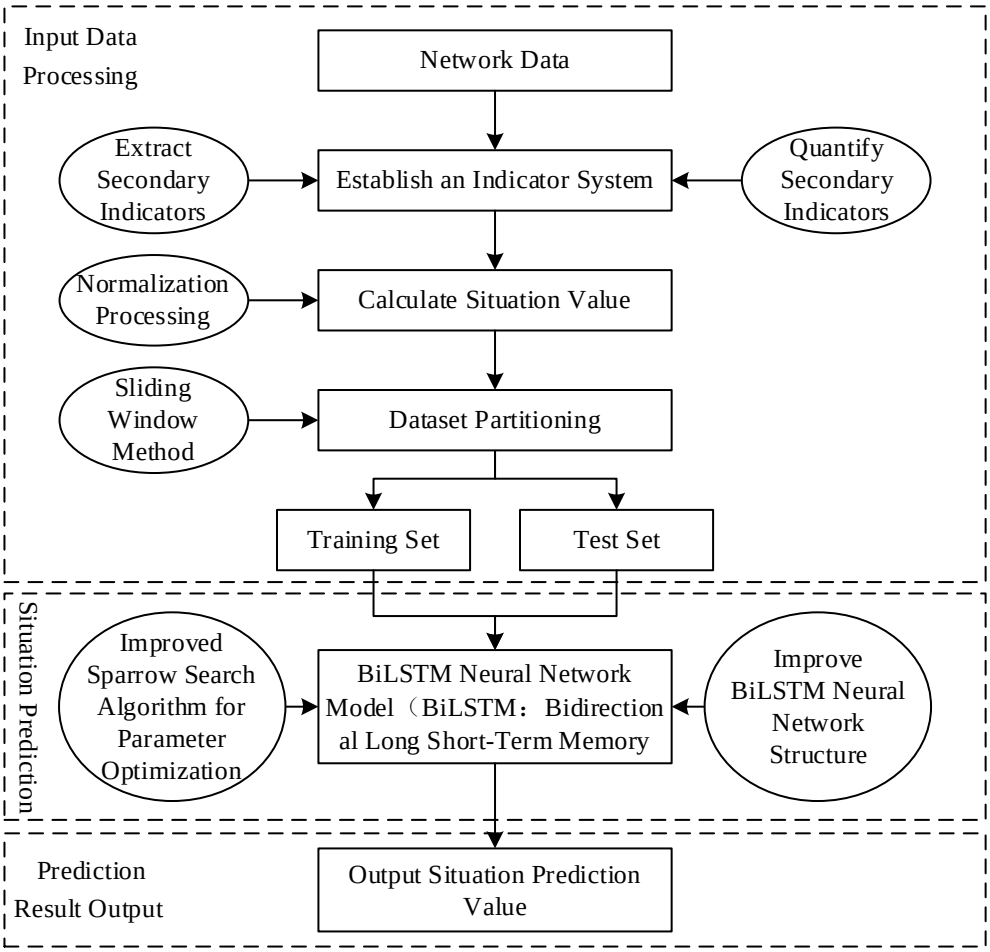

Figure 3: Network security situation prediction based on ISSA-BiLSTM

(1) Input Data Processing

This study uses a sliding window method to divide the dataset into training and test subsets. Following preprocessing, the network security dataset contains 215 samples with a selected sliding window size. The composition of the sample set is presented in Table 4. The neuron counts in the input and output layers of the BiLSTM network match the dimensions of the input features and output points accordingly. As a result, the input layer is set with 1 neuron, and the output layer is defined as 1 neuron.

Table 4: Sample set structure

Sample number	Input data	Output data
1	$(x_1, x_2, \ldots, x_m)$	x_{m+1}
2	$(x_2, x_3, \ldots, x_{m+1})$	x_{m+2}
…	…	…
$n-m$	$(x_{n-m}, x_{n-m+1}, \ldots, x_{n-1})$	x_n

(2) Cybersecurity Situation Prediction

The aforementioned sample set is input into the BiLSTM model proposed in this paper for training. The ISSA algorithm is introduced to optimize the parameters of the BiLSTM model, thereby enhancing the model's prediction accuracy.

(3) Prediction Result Output

The cybersecurity situation values predicted by the cybersecurity situation prediction model are output.

5 Analysis of Experimental Results for Cybersecurity Situation Forecasting

5.1 Cybersecurity Situation Value

Based on the temporal sequence of the dataset samples, every 2000 consecutive samples form a time period. The state values across all time periods are mapped to the range [0,1], generating a total of 155 state value sequence samples. The state values for these 155 time periods are shown in Figure 4.

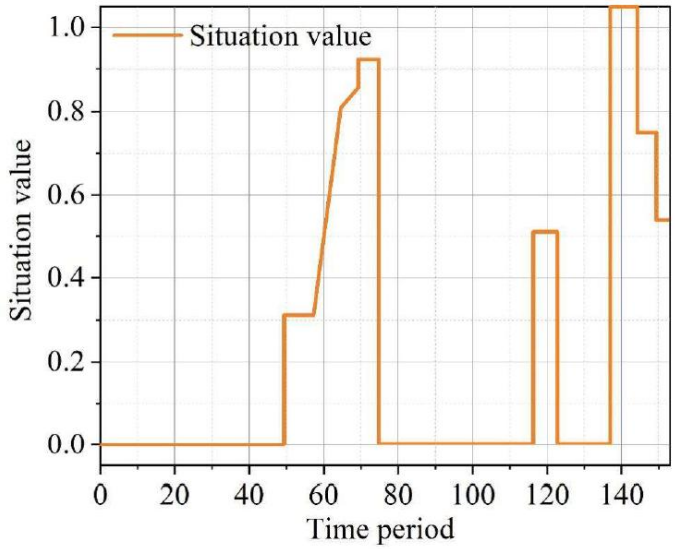

Figure 4: The situation value of the dataset.

5.2 Analysis of Experimental Results

To verify the prediction performance of the proposed models, four regression indicators are adopted in the experiment to evaluate each method: mean squared error (MSE), mean absolute error (MAE), root mean squared error (RMSE), and coefficient of determination. The calculation formulas for these metrics are given as follows:

$$MSE = \frac{1}{n}\sum_{i=1}^{n}(y_i - \hat{y}_i)^2 \tag{15}$$

$$MAE = \frac{1}{n}\sum_{i=1}^{n}\left|y_i - \hat{y}_i\right| \tag{16}$$

$$RMSE = \sqrt{MSE} = \sqrt{\frac{1}{n}\sum_{i=1}^{n}(y_i - \hat{y}_i)^2} \tag{17}$$

$$R^2 = 1 - \frac{\sum_{i=1}^{n} (y_i - \hat{y}_i)^2}{\sum_{i=1}^{n} (y_i - \bar{y})^2} \tag{18}$$

Where n stands for the number of samples, y represents the actual state value, \hat{y} denotes the predicted state value, and \bar{y} refers to the mean of the actual state values. Lower error values correspond to stronger model performance. For the coefficient of determination, a value approaching 1 indicates a higher fitting accuracy of the model.

To assess the prediction performance of different models, tests were carried out using window sizes of 6 and 3. With a window size of 6, the proposed ISSA-BiLSTM model is compared with several benchmark algorithms. The prediction outcomes of each model are illustrated in Figure 5, and the absolute errors between predicted and actual values are displayed in Figure 6.

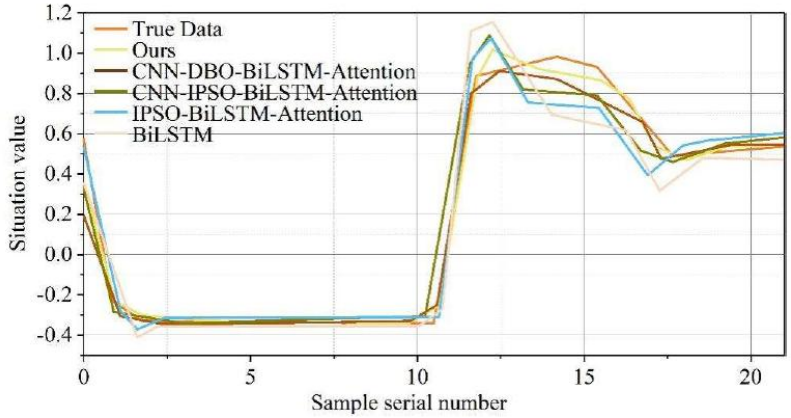

Figure 5: Comparison of prediction results

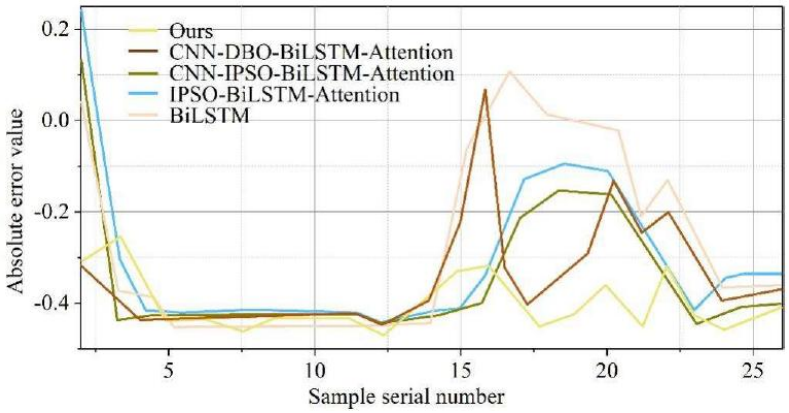

Figure 6: Absolute error comparison

As shown in the two figures above, the ISSA-BiLSTM model exhibits smaller fitting errors in its predicted situation values compared to the other four models.

When the window size is set to 3, this experiment compares the ISSA-BiLSTM model with the other four models. The prediction results of each model are shown in Figure 7, while the absolute errors between the predicted values and the actual values are presented in Figure 8.

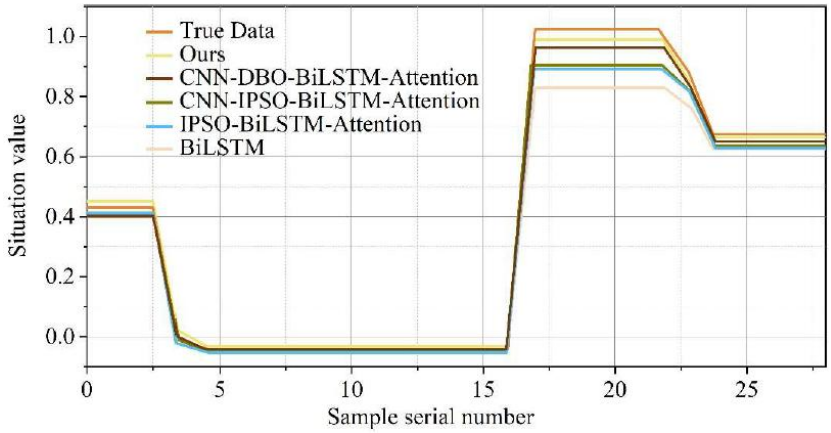

Figure 7: The prediction results are compared

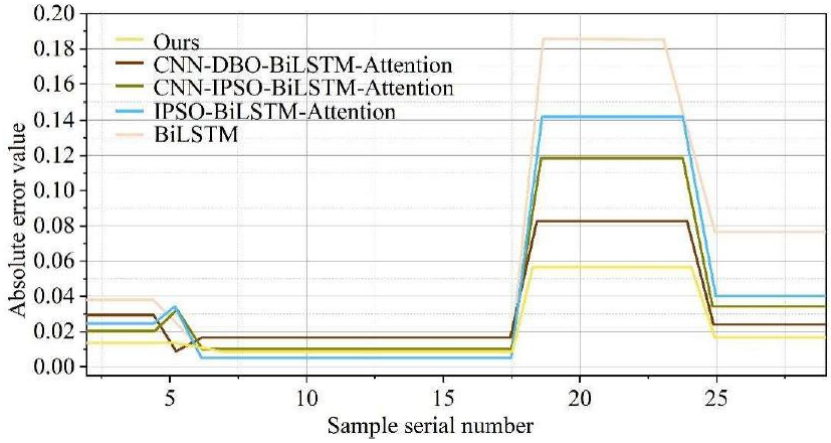

Figure 8: Absolute error comparison

As shown in the two figures above, the ISSA-BiLSTM model achieves better fitting performance than the other four models. The evaluation metrics for each model with window sizes of 6 and 3 are presented in Tables 5 and 6, respectively.

Table 5: Different model evaluation index comparison (window value is 6)

Evaluation model	MSE	MAE	RMSE	R2
Ours	0.000551	0.010552	0.019731	0.995257
CNN-DBO-BiLSTM-Attention	0.003295	0.061668	0.056198	0.953563
CNN-IPSO-BiLSTM-Attention	0.003659	0.061259	0.061237	0.969326
IPSO-BiLSTMAttention	0.005654	0.069565	0.076234	0.960261
BiLSTM	0.010139	0.069658	0.101165	0.936217

Table 6: Comparison of Evaluation Indicators of different models (window value is 3)

Evaluation model	MSE	MAE	RMSE	R2
Ours	0.000323	0.023376	0.022425	0.997367
CNN-DBO-BiLSTM-Attention	0.002228	0.026723	0.033263	0.982793
CNN-IPSO-BiLSTM-Attention	0.003282	0.036282	0.036626	0.972329
IPSO-BiLSTMAttention	0.006323	0.072356	0.066787	0.986262
BiLSTM	0.009282	0.063582	0.092362	0.933369

When the window size is set to 6 and 3, the MSE, MAE, and RMSE values of the ISSA-BiLSTM model are lower than those of the CNN-DBO-BiLSTM-Attention, CNN-IPSO-BiLSTM-Attention, IPSO-BiLSTM-Attention, and BiLSTM models, respectively. Additionally, its R^2 fit is higher than that of the other four models. Specifically, with a window size of 6, ISSA-BiLSTM achieved an average increase of 4.04% in R^2 fit quality, a reduction of 0.00514 in MSE, and a decrease of 0.05499 in MAE. When the window size was 3, ISSA-BiLSTM achieved an average increase of 2.87% in goodness-of-fit, a reduction of 0.00496 in MSE, and a decrease of 0.02636 in MAE. Accordingly, the ISSA-BiLSTM model achieved superior performance over the other four comparison models. The fitting degree between the predicted results and actual values for different models is depicted in Figure 9.

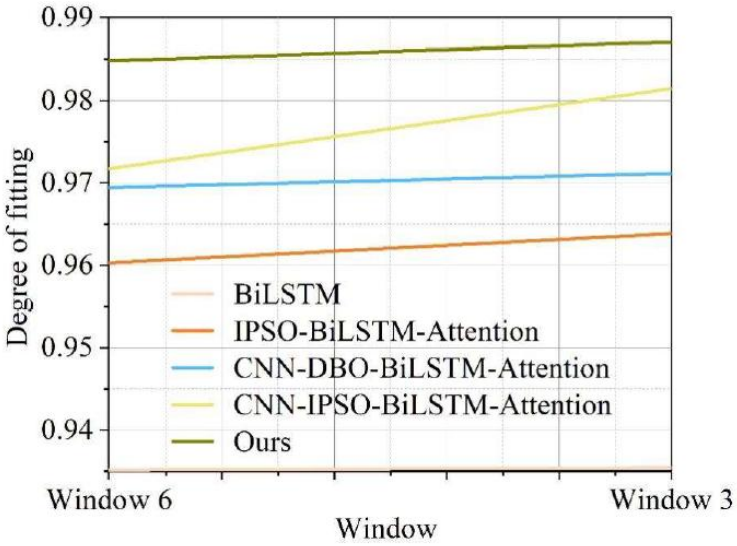

Figure 9: Comparison of the fitting degrees of different models.

Experimental result comparisons show that under a fixed sliding window setting, the ISSA-BiLSTM model achieves higher prediction accuracy than the other four models. When the sliding window size is variable, using two historical state values to forecast the subsequent state value produces more reliable prediction outcomes.

6 Conclusion

This paper establishes a damage detection platform for subway tunnels and develops damage detection algorithms alongside high-precision imaging algorithms. Compared with existing mainstream detection models, the method proposed in this paper shows obvious advantages, with higher recognition accuracy for tunnel defects and more reliable overall performance. Against the background of increasingly complex network environments and diversified cyber threats, system security risks and network vulnerabilities are becoming more prominent.For this reason, the ISSA-BiLSTM model is used to strengthen the network security situation awareness ability of the whole system.Experimental results show that, compared with other comparable prediction models, ISSA-BiLSTM improves the fitting accuracy by 4.04% and 2.87% on average under the window settings of 6 and 3 respectively.

Overall, the application of deep learning-driven multimodal image damage detection technology within the Industrial Internet of Things offers substantial potential for the operation and maintenance management of subway systems.By utilizing the damage detection methods

presented in this study, subway operating units can realize more efficient, reliable, and secure operational and maintenance management.

References

[1] Qin, W., Chen, S., & Peng, M. (2020). Recent advances in Industrial Internet: insights and challenges. Digital Communications and Networks, 6(1), 1-13.

[2] Malik, S., Rouf, R., Mazur, K., & Kontsos, A. (2020). The industry Internet of Things (IIoT) as a methodology for autonomous diagnostics in aerospace structural health monitoring. Aerospace, 7(5), 64.

[3] Altan, G. (2021). SecureDeepNet-IoT: a deep learning application for invasion detection in industrial internet of things sensing systems. Transactions on Emerging Telecommunications Technologies, 32(4), e4228.

[4] Misra, S., Roy, C., Sauter, T., Mukherjee, A., & Maiti, J. (2022). Industrial Internet of Things for safety management applications: A survey. IEEE Access, 10, 83415-83439.

[5] Yang, Y., Yang, X., Heidari, M., Khan, M. A., Srivastava, G., Khosravi, M. R., & Qi, L. (2022). ASTREAM: Data-stream-driven scalable anomaly detection with accuracy guarantee in IIoT environment. IEEE Transactions on Network Science and Engineering, 10(5), 3007-3016.

[6] Zhou, L., & Guo, H. (2018, July). Anomaly detection methods for IIoT networks. In 2018 IEEE International Conference on Service Operations and Logistics, and Informatics (SOLI) (pp. 214-219). IEEE.

[7] Rodriguez, M., Tobon, D. P., & Munera, D. (2025). A framework for anomaly classification in Industrial Internet of Things systems. Internet of Things, 29, 101446.

[8] Hore, U. W., & Wakde, D. G. (2022). An effective approach of IIoT for anomaly detection using unsupervised machine learning approach. J. IoT Soc. Mob. Anal. Cloud, 4, 184-197.

[9] Kim, J., Shin, J., Park, K. W., & Seo, J. T. (2022). Improving Method of Anomaly Detection Performance for Industrial IoT Environment. Computers, Materials & Continua, 72(3).

[10] Zhou, Y., Yu, L., Liu, M., Zhang, Y., & Li, H. (2018, October). Network intrusion detection based on kernel principal component analysis and extreme learning machine. In 2018 IEEE 18th International Conference on Communication Technology (ICCT) (pp. 860-864). IEEE.

[11] Gao, J., Chai, S., Zhang, B., & Xia, Y. (2019). Research on network intrusion detection based on incremental extreme learning machine and adaptive principal component analysis. Energies, 12(7), 1223.

[12] Alanazi, R., & Aljuhani, A. (2023). Anomaly Detection for Industrial Internet of Things Cyberattacks. Computer Systems Science & Engineering, 44(3).

[13] Kang, S. H., & Kim, K. J. (2016). A feature selection approach to find optimal feature subsets for the network intrusion detection system. Cluster Computing, 19(1), 325-333.

[14] Deng, X., Jiang, P., Peng, X., & Mi, C. (2018). An intelligent outlier detection method with one class support tucker machine and genetic algorithm toward big sensor data in internet of things. IEEE Transactions on Industrial Electronics, 66(6), 4672-4683.

[15] Shang, W., Zeng, P., Wan, M., Li, L., & An, P. (2016). Intrusion detection algorithm based on OCSVM in industrial control system. Security and Communication Networks, 9(10), 1040-1049.

[16] Pang, J., Pu, X., & Li, C. (2022). A hybrid algorithm incorporating vector quantization and one-class support vector machine for industrial anomaly detection. IEEE Transactions on Industrial Informatics, 18(12), 8786-8796.

[17] Diez-Olivan, A., Pagan, J. A., Khoa, N. L. D., Sanz, R., & Sierra, B. (2018). Kernel-based support vector machines for automated health status assessment in monitoring sensor data. The International Journal of Advanced Manufacturing Technology, 95(1), 327-340.

[18] Yang, H., & Zhou, Z. (2018, July). A novel intrusion detection scheme using cloud grey wolf optimizer. In 2018 37th Chinese Control Conference (CCC) (pp. 8297-8302). IEEE.

[19] Zhang, R. B., Xia, L. H., & Lu, Y. (2019, July). Anomaly Detection of ICS based on EB-OCSVM. In Journal of Physics: Conference Series (Vol. 1267, No. 1, p. 012054). IOP Publishing.

[20] Qu, H., Zhou, J., Qin, J., & Tian, X. (2021). Anomaly detection for industrial control networks based on improved one-class support vector machine. International Journal of Pattern Recognition and Artificial Intelligence, 35(04), 2150012.

[21] Guo, K., Liu, D., Peng, Y., & Peng, X. (2018, October). Data-driven anomaly detection using OCSVM with boundary optimzation. In 2018 Prognostics and System Health Management Conference (PHM-Chongqing) (pp. 244-248). IEEE.

[22] Li, X., Xie, C., Zhao, Z., Wang, C., & Yu, H. (2024). Anomaly detection algorithm of industrial internet of things data platform based on deep learning. IEEE Transactions on Green Communications and Networking, 8(3), 1037-1048.

[23] Omarov, B., Auelbekov, O., Suliman, A., & Zhaxanova, A. (2023). Cnn-bilstm hybrid model for network anomaly detection in internet of things. International Journal of Advanced Computer Science and Applications, 14(3).

[24] Ullah, I., & Mahmoud, Q. H. (2022). Design and development of RNN anomaly detection model for IoT networks. IEEE Access, 10, 62722-62750.

[25] Chen, Z., Li, Z., Huang, J., Liu, S., & Long, H. (2024). An effective method for anomaly detection in industrial Internet of Things using XGBoost and LSTM. Scientific Reports, 14(1), 23969.

[26] Yin, C., Zhang, S., Wang, J., & Xiong, N. N. (2020). Anomaly detection based on convolutional recurrent autoencoder for IoT time series. IEEE Transactions on Systems,

Man, and Cybernetics: Systems, 52(1), 112-122.

[27] Khacha, A., Saadouni, R., Harbi, Y., & Aliouat, Z. (2022, November). Hybrid deep learning-based intrusion detection system for industrial internet of things. In 2022 5th International Symposium on Informatics and its Applications (ISIA) (pp. 1-6). IEEE.

[28] Nizam, H., Zafar, S., Lv, Z., Wang, F., & Hu, X. (2022). Real-time deep anomaly detection framework for multivariate time-series data in industrial IoT. IEEE Sensors Journal, 22(23), 22836-22849.

[29] Anuradha, R., Swathi, B., Nagpal, A., Chaturvedi, P., Kalra, R., & Alwan, A. A. (2023, December). Deep Learning for Anomaly Detection in Large-Scale Industrial Data. In 2023 10th IEEE Uttar Pradesh Section International Conference on Electrical, Electronics and Computer Engineering (UPCON) (Vol. 10, pp. 1551-1556). IEEE.

[30] Laiq, F., Al-Obeidat, F., Amin, A., & Moreira, F. (2023, October). DDoS attack detection in edge-IIoT using ensemble learning. In 2023 7th Cyber Security in Networking Conference (CSNet) (pp. 204-207). IEEE.

[31] Elsas, R., Van Leemput, D., Hoebeke, J., & De Poorter, E. (2025). Multi-modal industrial IoT networks: Recent advances and future challenges. Wireless Personal Communications, 140(1), 1-24.

[32] Sun, S., Ma, L., Huang, H., & Fan, Y. (2024, December). Multi-Modal Big Data Modeling and Analysis Techniques for Industrial Internet of Things. In 2024 6th International Academic Exchange Conference on Science and Technology Innovation (IAECST) (pp. 775-784). IEEE.

[33] Jiang, W., Zhang, Y., Han, H., Liu, S., Duan, S., Zhang, H., & Gu, W. (2024, November). Multi-Modal Big Data Analyzing Architecture for Industrial Internet of Things. In Proceedings of the First International Workshop on IoT Datasets for Multi-modal Large Model (pp. 83-84).

[34] Xiao, X., Zheng, Y., Luo, Q., & Xie, X. (2014). Inferring social ties between users with human location history. Journal of Ambient Intelligence and Humanized Computing, 5(1), 3-19.

[35] Nagrani, A., Yang, S., Arnab, A., Jansen, A., Schmid, C., & Sun, C. (2021). Attention bottlenecks for multimodal fusion. Advances in neural information processing systems, 34, 14200-14213.

[36] Liang Xiaoqiang,Hu Da,Li Yongsuo,Zhang Yunyi & Yang Xian.(2022).Application of GPR Underground Pipeline Detection Technology in Urban Complex Geological Environments.Geofluids,2022,

[37] Wu Dong,Liao Man Wen,Zhang Wei Tian,Wang Xing Gang,Bai Xiang,Cheng Wen Qing & Liu Wen Yu.(2023).Correction to: YOLOP: You Only Look Once for Panoptic Driving Perception.Machine Intelligence Research,20(6),952-952.