Construction and Application of Internet of Things Network Security Situation Prediction Model Based on BiLSTM Algorithm

Yubao Wu

School of Information Technology, Nanjing Police University; Nanjing, Jiangsu, 210023 China
E-mail: wyb@nfpc.edu.cn

Received 01 February 2024; Accepted 13 March 2024

Abstract

IIoT is more and more extensive. However, security problem of IIoT is increasing. Traditional network security strategies can not fully evaluate the security situation of IIoT. In view of the incomplete selection of situation elements and the single dimension of evaluation system, we selected 14 secondary indicators from four dimensions: operation dimension, fragility dimension, stability dimension and threat dimension, and constructed the evaluation index system of IIoT. In the experiment, we selected 50 enterprises as samples, measured the IIoT system and collected data, and determined weight of each index. This article proposes an improved arithmetic optimization algorithm. Evaluate the performance of the model using a 10x cross validation method. The results show that our model reaches 92% accuracy, which is higher than existing models. Optimize parameters of the BiLSTM

Journal of Cyber Security and Mobility, Vol. 13_5, 843–862.
doi: 10.13052/jcsm2245-1439.1352

network by improving the sparrow search algorithm. The experimental results show that the optimized model also outperforms existing models in prediction accuracy. The MSE and MAE of our model are 0.023 and 0.018, respectively, which are reduced by 30% and 25% compared to existing models.

Keywords: IIoT, situation assessment, situation forecast, two-way long-term and short-term memory network.

1 Introduction

A brand-new Internet of Things era is gradually emerging, with billions of industrial equipment interconnected and interacting with each other, popularization scope of Industrial Internet of Things (IIoT) expanding rapidly, its market scale also rising continuously [1, 2]. According to the report, in 2020, the global IIoT industry market will reach 81.339 billion US dollars.

With the different research fields of network security situation awareness, the definition and understanding of situation awareness are also very different. Situation awareness is to perceive a large number of environmental elements in time and space, understand their meaning, and predict their state in the near future. In this definition, we can extract the three elements of situation awareness, perception, understanding and prediction. In other words, situation awareness can be divided into three levels of information processing, perception, understanding and prediction, and perception and acquisition of important clues or elements in the environment. Integrate sensed data and information and analyze their relevance. Based on the perception and understanding of environmental information, the future development trend of related knowledge is predicted.

IIoT generates incredibly intricate data, rendering manual analysis impractical. If these data cannot be translated into valuable insights, they will remain useless. Fortunately, artificial intelligence (AI) offers a timely solution. The IIoT collects data by connecting network nodes, and with extensive training, AI can extract meaningful information from this vast dataset. Consequently, the integration of IIoT and AI ushers in a new era of intelligence.

As the IIoT continues to evolve, it faces novel security challenges, prompting the emergence of security situation prediction technology. Consequently, related academic research has been on a steady rise over the years [3]. Traditionally, most network managers relied on manual experience analysis or a single security protection device to perceive and assess the current network status. However, these individual security devices are limited to identifying specific types of network attacks, offering only a partial view of potential safety hazards within the network. They fail to provide a comprehensive overview of the network's overall security posture [4, 5].

Network attacks will present a certain law in time sequence, so we choose the network dealing with time sequence data in the experiment. Most situation prediction models consider the internal information of network data or unidirectional time series data, but fail to fully learn the characteristic information in time series data [6, 7]. In this paper, BiLSTM network is selected, which can fully extract time series features and obtain better prediction results. Then connect the dropout layer and the sense layer to improve the generalization ability, transform the output dimension and obtain the predicted value. In this paper, an IoT security situation prediction model based on optimized BiLSTM network is proposed. In order to better learn the upper and lower data information in the IoT data set, BiLSTM layer is superimposed, and then dropout layer and dense layer are connected to improve generalization ability and transform output dimensions to get prediction results.

2 Security Situational Awareness Related Technologies

2.1 Extraction Technology of Situation Elements

Situation element extraction is the first stage and basic technology. The collection of network security situation elements needs to be carried out from two aspects: depth and breadth, and the accuracy of element collection is the prerequisite for network security situation assessment and prediction. Situation element extraction uses the secondary indicators in the index system to extract relevant data from the data collector, and after data preprocessing, it is used as situation elements and provided to the two stages of situation assessment and prediction [8].

The breadth and accuracy of data collection are the basis of extracting situation elements. With the increasingly complex network environment and more frequent network attacks, scholars at home and abroad tend to multi-source data collection. According to different dimensions of data, different technologies need to be adopted for collection, as shown in Table 1.

In the real network environment, data preprocessing is crucial due to potential issues such as missing and abnormal values. Therefore, it is imperative to perform data preprocessing [9, 10]. Data cleaning, a vital aspect of preprocessing, involves discarding unique attributes and completing missing

Table 1 Multi-source data acquisition mode

Data Classification	Data Source	Acquisition Method
Asset dimension	System configuration information, network topology, services, user data, etc.	Wireshark, NetFlow, Snmp
Vulnerability dimension	Software vulnerabilities, configuration vulnerabilities, structural vulnerabilities, etc.	CNNVD, CVE, etc Repository
Threat dimension	IDS Alarm, Firewall, Log Data, Traffic Data, etc	Flume, Syslog, Honeypot, Tensor analysis

data from diverse sources. Unique attributes refer to those that uniquely identify the data; if the 'id' attribute fails to reflect the sample distribution rule, it can be eliminated. Methods for completing missing data include mean and homogeneous mean interpolation, modeling prediction, and high-dimensional mapping [11]. Additionally, handling outliers, which involves detecting and addressing abnormal values in a dataset, is also essential. This is often achieved by either eliminating outliers or replacing them with acceptable values.

Data integration involves combining disparate datasets from various sources into a single, coherent dataset, thereby addressing data inconsistency issues [12]. Central to this process are the challenges of entity identification and data redundancy analysis. Entity recognition, a fundamental aspect of data integration, involves determining whether attributes from distinct datasets represent the same entity or concept. This recognition process involves assessing whether a given attribute in one dataset can be derived from another attribute or a set of attributes in another dataset. If such a derivation is possible, the attribute may be considered redundant. Furthermore, variations in attribute naming conventions can also contribute to data redundancy.

Data specification methods primarily encompass attribute selection and data sampling. Attribute selection involves the elimination of irrelevant or redundant attributes, streamlining the dataset to its most relevant features. Quantitative specification, on the other hand, involves substituting the original data with a more concise and representative alternative. Data compression refers to the compressed representation of the original data, achieved through a transformation process.

Data transformation and discrete data transformation are forms of data normalization, which aim to standardize the data. Strategies employed include smoothing, attribute construction, and aggregation. Data smoothing serves to eliminate noise from the data, ensuring its clarity and accuracy. Attribute construction involves creating a new attribute from an existing one and incorporating it into the attribute set, enriching the dataset's descriptive capabilities. Aggregation refers to the consolidation of data points, often used to simplify complex datasets.

Normalization, specifically, refers to scaling attribute data within a specific interval, ensuring consistency and comparability across different attributes. Data fusion, finally, refers to the process of integrating and correlating network data from diverse sources, aiming to extract more effective and comprehensive information.

2.2 Situation Assessment Technology

According to the theoretical basis, situation assessment methods are mainly divided into three categories [13, 14]. Methods based on mathematical model include AHP, comprehensive evaluation method and so on. Knowledge-based reasoning methods mainly include Bayesian network, Markov game model and so on. With the rise of machine learning and its application in various fields, machine learning algorithms have been widely used in network security situation assessment, among which the representative algorithms based on AI are SVM, neural network and so on.

Based on the conceptual model, the process of network security situation awareness encompasses four distinct stages. Central to this awareness is situation prediction, which utilizes the outputs of situation assessment to anticipate the evolving trends in network security status. This predictive capability is the ultimate goal of situation awareness. To achieve a comprehensive understanding, network security situation awareness must possess both depth and breadth, analyzing system security from multiple levels, angles, and granularities. Furthermore, it must provide responsive measures that are presented to users in the form of graphs, tables, and detailed security reports.

Perception includes information about the status, attributes and dynamics of important elements in the network environment, as well as the process of sorting them out. Comprehension is the fusion and interpretation of the information of these important components, not only the judgment analysis of a single analysis object, but also the integration of multiple related objects. At the same time, understanding is constantly updated and evolved with the change of situation, and new information is constantly fused to form a new

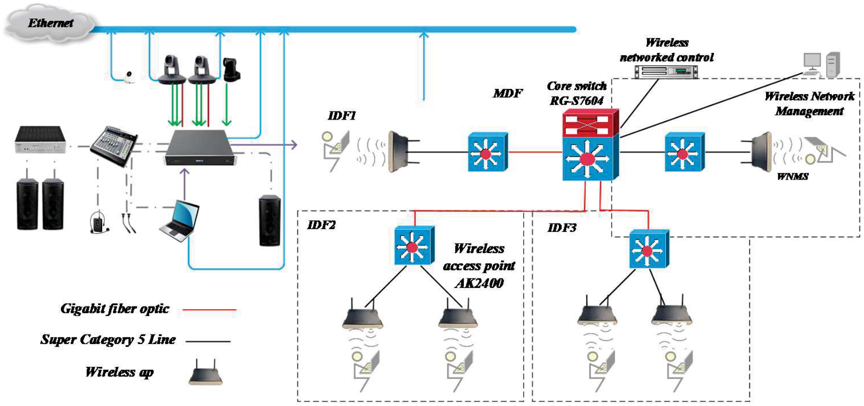

Figure 1 Overall framework of IoT network.

understanding. On the basis of understanding the status and changes of the situation elements, the upcoming status and changes of each element in the situation are predicted.

Figure 1 shows the overall framework of the Internet of Things network. When using AHP to make decisions, it can be divided into the following four steps. The situation assessment problem can be decomposed into simple sub-problems, and then the entity fragments corresponding to the sub-problems are constructed, and these instantiated fragments are recursively merged. According to the specific situation and evidence, the corresponding situation assessment Bayesian network is generated, and the enemy intention is inferred by reasoning algorithm, and finally the enemy intention is output. The multi-entity network model of situation assessment includes intention recognition part and target recognition part.

2.3 Situation Prediction Technology

The neural network has become increasingly intertwined with various disciplines, with representative models including the backpropagation neural network (BPNN), recurrent neural network, cyclic neural network, and the LSTM network [15].

Deep learning exhibits significant advantages in the detection of intrusions within the Internet of Things, particularly in the effective extraction of features that facilitate the dimensionality reduction of sample data. Leveraging the characteristics of massive, multi-modal, and multi-granularity data in large-scale networks, a comprehensive security situation awareness model

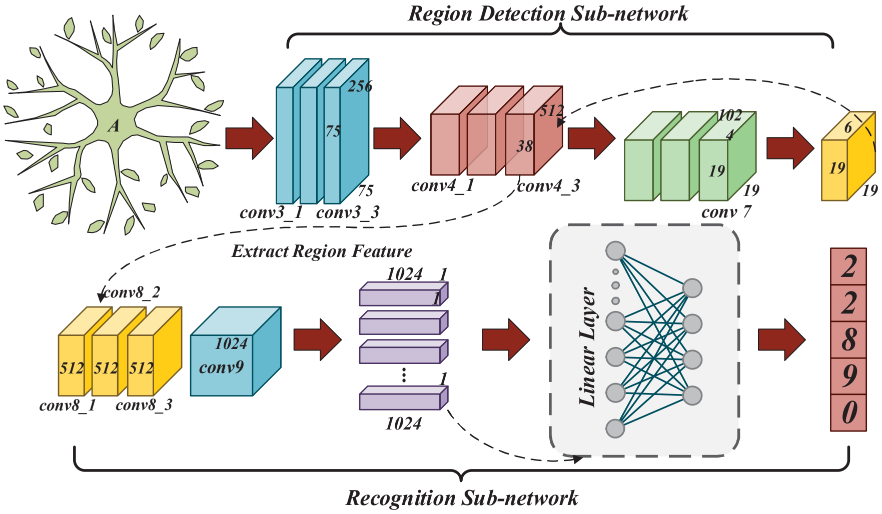

Figure 2 BP algorithm learning process.

has been proposed. This model is comprised of four integral components: data integration, correlation analysis, index system, and situation display, culminating in situation prediction. Figure 2 illustrates the learning process of the Back-propagation algorithm. If the desired output is not achieved, the error propagation process ensues: the error is distributed across all neurons in each layer, leading to the computation of error signals for each unit. Subsequently, the weights of each unit are adjusted accordingly [16, 17].

The Elman network stands as the most widely utilized recurrent neural network [18]. Structurally, it resembles a multi-layer feed forward neural network, with a key distinction: the output feedback from the hidden layer can be integrated as input for the subsequent time step alongside the incoming signal. The BP algorithm is frequently employed in network training. Furthermore, a network framework rooted in target defense enhances both the effectiveness and adaptability of network security situation awareness.

The memory cell structure of LSTM includes input gate, forgetting gate and output gate to control historical information. At the bottom are four S function cells, and the leftmost function may become the input of block according to the situation [19]. The second one on the left is the input gate. On far right is the output gate, which can determine whether the input in the block memory can be output. LSTM unit structure is to control the transmission state through gate mechanism.

3 ISSA Optimizes BiLSTM Model

3.1 Improvement of BiLSTM Network Structure

BiLSTM neural network has a good effect in processing time series related data, and is often applied to sentence-level emotion classification, machine translation and speech recognition. However, nowadays, the processing sequence is not as simple as before, and the neural network structure relying on a single BiLSTM cannot meet the demand. In addition, from the present stage, the model based on BiLSTM neural network not only uses basic BiLSTM unit structure.

As depicted in Figure 3, traditional single-layer BiLSTM neural networks have been effective in achieving precise predictions for simpler targets in the past. However, given the evolving diversity of network attacks and the intricate nature of the IIoT environment, identifying meaningful relationships within time-series data can pose a challenge. To achieve superior prediction accuracy, it is imperative to delve deeper into the intricate correlations inherent in time-series data. While traditional BiLSTM networks may offer basic data correlation insights, they often fall short in terms of precision. Consequently, a two-layer BiLSTM neural network architecture is introduced. The computational formula for the forgetting gate is outlined in Equation (1).

$$\mathrm{Q}_t = \sigma(W_t k_t) \tag{1}$$

The function of input gate is to update important information, and its calculation formula is shown in (2) and (3).

$$o_t = \sigma(W_i + c_i) \tag{2}$$

$$\dot{G}_t = tanh(k_t.x_{t+1}) \tag{3}$$

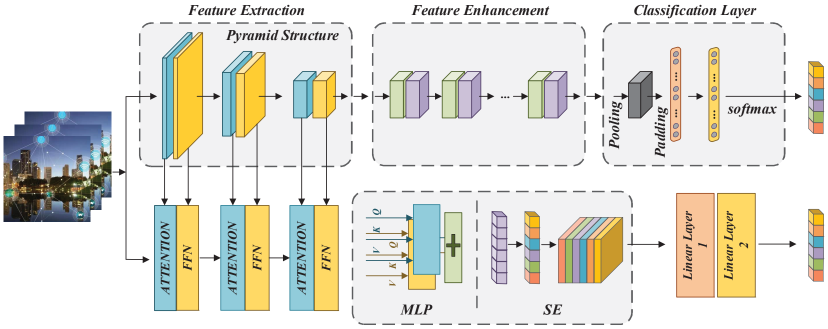

Figure 3 BiLSTM network architecture.

Output value of cell state at the current time is calculated as shown in formula (4).

$$C_t = \tilde{C}_{1-t} k_t \tag{4}$$

State of output gate and hidden layer is shown in Formula (5) and Formula (6).

$$W_t = \sigma(Y_{t-1}) \tag{5}$$

$$Y_t = tanh(Y_i) \cdot o_t \tag{6}$$

Neural network structures are stacked to extract deeper relationships within time series data. Dropout, a regularization technique, randomly discards a proportion of nodes during training, effectively mitigating over fitting and simplifying the complex relationships among nodes. The dense layer, a crucial component, maps the nonlinear transformation of the previous layer's output to the output layer, effectively capturing the essence of the previous layer's representation. The prediction outcome reflects the overall security situation of the IIoT in the subsequent time period, effectively performing a classification task [20, 21].

3.2 ISSA Optimizes BiLSTM Network Parameters

SSA is tested on 19 test functions with gray wolf optimization algorithm, particle swarm optimization algorithm and gravity search algorithm. The results show that compared with other advanced algorithms, SSA has better performance in search accuracy, convergence speed and stability [22]. However, the traditional SSA is easy to fall into local optimal solution, so other strategies should be introduced to help the traditional SSA enhance the global search ability.

Reverse learning strategy is often applied to swarm intelligence optimization algorithm. In the classical SSA, the initial population is randomly generated, sparrows may gather in one region or disperse in various regions. The calculation formula of Internet of Things optimization strategy is shown in Formula (7):

$$Levy(x) = 0.01 \times \frac{r_3 \times \sigma}{|r_4|^{\frac{1}{\xi}}} \tag{7}$$

The operating system version of IIoT equipment will also have a certain impact on the operation. The higher the operating system version, the more favorable the network operation will be, and the higher the index score will be. The quantification formula of the score corresponding to the operating system version information is shown in Formula (8).

$$OSDeviceScore = \sum_{i=1}^{n} OS\,Type_i \tag{8}$$

In the actual environment, the more complex the topology of IIoT, more nodes will be involved. Once a security incident occurs, more devices will be affected. The quantization formula of network topology is shown in formula (9).

$$TopologvScore = \sum_{i=1}^{n} P_i \tag{9}$$

The change of IIoT traffic also reflects ecurity status of IIoT within a certain period of time, and its quantitative formula is shown in Formula (10).

$$f_r = \frac{R_{t-1}}{R_t} \tag{10}$$

Based on historical data of IIoT, it is evident that a higher frequency of security incidents within a fixed time period indicates a lower level of security within the IIoT system. The quantification of this historical occurrence frequency of safety incidents is outlined in Formula (11).

$$s_r = \frac{Nums}{t} \tag{11}$$

The Math Optimizer Probability (MOP) is a coefficient calculated as shown in Formula (12).

$$MOP(iter) = 1 - \frac{iter^{\frac{1}{a}}}{Max_{\_}^{\frac{iter^{a}}{a}}} \tag{12}$$

The standard SSA often faces the challenge of getting trapped in local optimal solutions. If the global optimal solution remains undetected, the optimization task remains incomplete. In the context of random walks with smaller strides, the Levy flight strategy exhibits a higher likelihood of achieving larger strides, thus balancing the need for both local and global search capabilities. Consequently, we incorporate a search algorithm that continuously updates the optimal position of the sparrow within the sparrow search algorithm. This refinement ensures that the SSA avoids getting trapped in local optima, while the enhanced scavenger updates its position. In this study, we introduce the reverse learning strategy and Lévy flight strategy to enhance the sparrow search algorithm. By obtaining an initial population with superior fitness, we guarantee the local and global search abilities of the SSA, leading to an overall improvement in algorithm performance. The optimized parameter process is outlined below.

(1) Initialize improved BiLSTM neural network structure;
(2) Initialize the improved SSA related parameters, including population number, maximum iteration times, leader ratio, watchman ratio and early warning value;
(3) Setting the dimension of sparrow population and the value range of the dimension, which respectively represents the iteration times of the model;
(4) Setting fitness function of sparrow search algorithm, randomly generating initial population, calculating individual fitness value of sparrow, introducing reverse learning strategy, obtaining final initial population, and recording current optimal solution;
(5) Calculate that individual fitness value of the sparrow, update the optimal solution, and update the position of the leader, the eater and the guard;
(6) If the maximum iteration times are reached, the next step is carried out, otherwise, the previous step is returned to continue the iteration;
(7) Obtaining the optimal parameters of BiLSTM model;
(8) Forecast the security situation of the IIoT and obtain the prediction results.

3.3 Security Situation Prediction Model of IIoT Based on ISSA-BiLSTM

According to the above-mentioned flow of BiLSTM network parameters optimized by ISSA, a security situation prediction model of IIoT based on ISSA-BiLSTM is constructed [23, 24]. In this paper, the sliding window method is used to divide the data set, and the training set and test set are made. After preprocessing, there are 213 samples in the industrial IoT data set, and sliding window size is m+1.

Figure 4 illustrates the prediction model for IIoT security situations. In this model, the input layer is configured with m neurons, while the output layer has a single neuron. The aforementioned sample sets are fed into the model, and the ISSA is employed to fine-tune the parameters of the BiLSTM model, aiming to enhance its prediction accuracy. Subsequently, the model

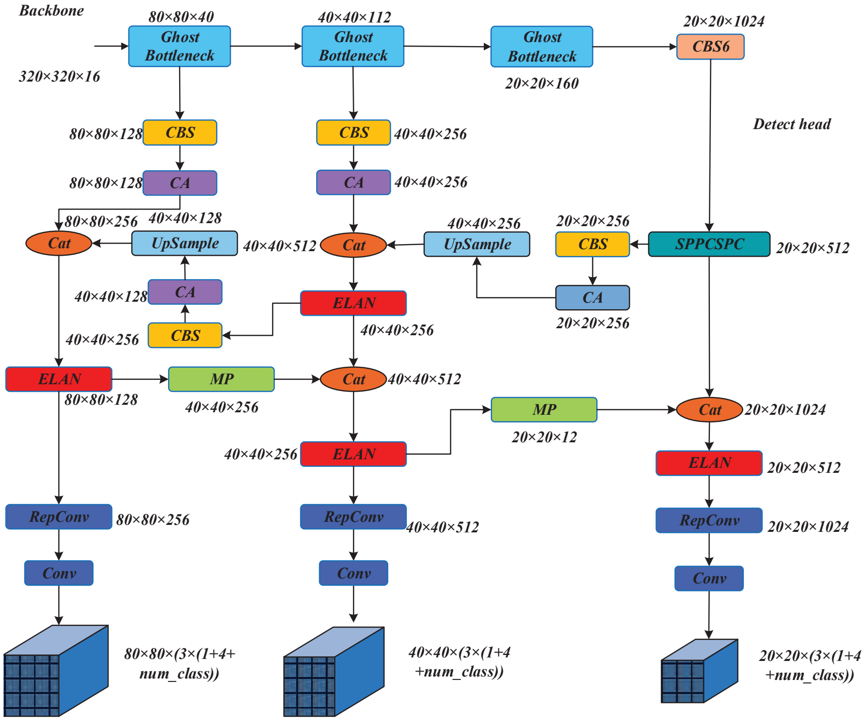

Figure 4 Security situation forecast model of IIoT.

generates prediction outcomes, reflecting the anticipated security situation within the IIoT framework.

4 Results Analysis

4.1 Safety Evaluation System of IIoT

Assets refer to the valuable information or resources present within the IIoT environment, with asset value serving as an indicator of their significance. The assessment of IIoT device asset value encompasses two key components: the type of IIoT devices, including computers and servers, and the importance of the information stored by these devices. By considering both of these aspects, the asset value can be accurately quantified [25].

The operating system version of IIoT equipment will also have a certain impact on the operation. Score corresponding to the operating system version information [26, 27]. The nature and extent of vulnerabilities within the IIoT

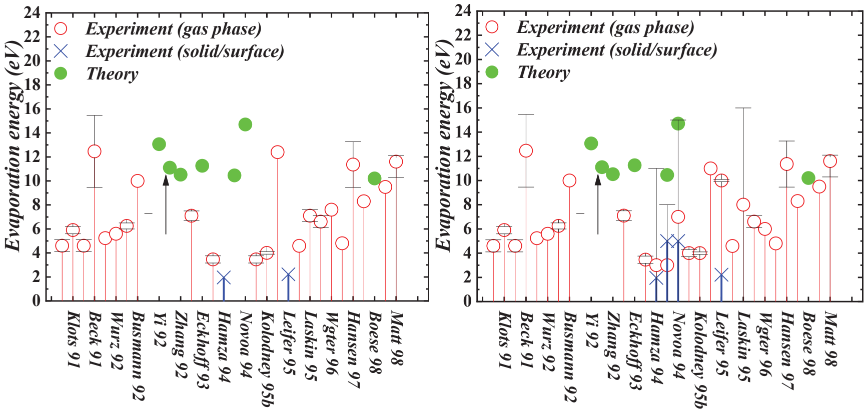

Figure 5 Forecast results of each model.

are pivotal indicators that have a direct impact on network functionality. The severity of these vulnerabilities is gauged by both the type and quantity of vulnerabilities present. In practical settings, as the topological complexity of the IIoT increases, so too does the number of nodes involved, amplifying the challenge of managing these vulnerabilities. Once a security incident occurs, more devices will be affected. The change of IIoT traffic also reflects security status of IIoT within a certain period of time. In historical data of IIoT, the more times a security incident occurs in a fixed period of time, the lower the security of IIoT [28].

4.2 Result Analysis

In order to verify prediction accuracy of the model proposed, experiments were carried out when the window values were 4 and 6 respectively [29, 30]. In this study, the aforementioned sample dataset is evenly distributed into a training set and a test set, following an approximate 80% to 20% split. We compare the predictive outcomes of our model with other SOTA models. The graphical representation of each model's prediction outcomes is presented in Figure 5.

In Figure 5, we observe that the BiLSTM models 4, 6, 36, and 37 demonstrate strong alignment with the actual situation values, maintaining a notable distance from other regions. However, in other regions, they deviate noticeably. The SSA-LSTM model aligns more closely with the actual situation values at samples 4, 23, 34, and 38. Similarly, the IPSO-LSTM model demonstrates a stronger correlation at samples 4, 5, 33, and 37. The

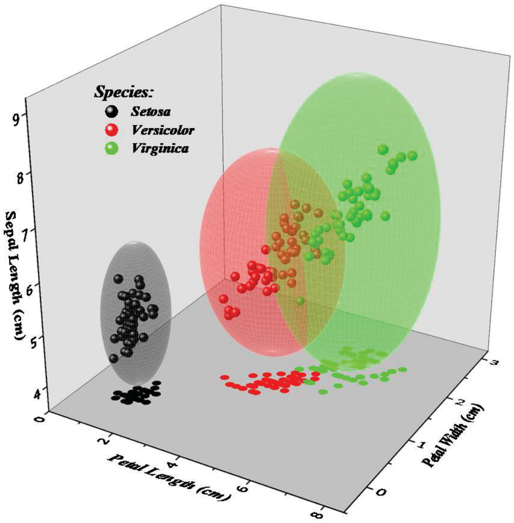

Figure 6 Real situation value distribution.

SSA-BiLSTM model exhibits a higher correlation at samples 13, 14, 23, and 39. When compared to the traditional models exhibit superior prediction performance. However, their predictive abilities are weaker during periods of significant real-world value fluctuation. Notably, the model introduced in our research outperforms all other models in terms of overall prediction effectiveness.

In Figure 6, it is evident that when the real situation value experiences substantial fluctuations, the traditional BiLSTM model demonstrates an absolute error nearing 0.6. Although our proposed model exhibits a reduction in absolute error compared to the standard BiLSTM, the improvement is still considered unsatisfactory. Nevertheless, the model introduced in our study demonstrates remarkable consistency between predicted and actual values, with minimal absolute error. Additionally, its overall narrow fluctuation range underscores its robustness.

In Figure 7, we observe that the BiLSTM models 7, 21, and 32 align well with the actual situation values, maintaining a notable distance from other regions. However, in other regions, they deviate noticeably. Our model demonstrates a stronger correlation with the actual situation values at samples 8, 17, and 21. Similarly, the IPSO-LSTM model aligns more closely at samples 3, 8, and 33. Our model exhibits a higher correlation at samples 1, 9, and 20. When compared to the traditional BiLSTM model, our model

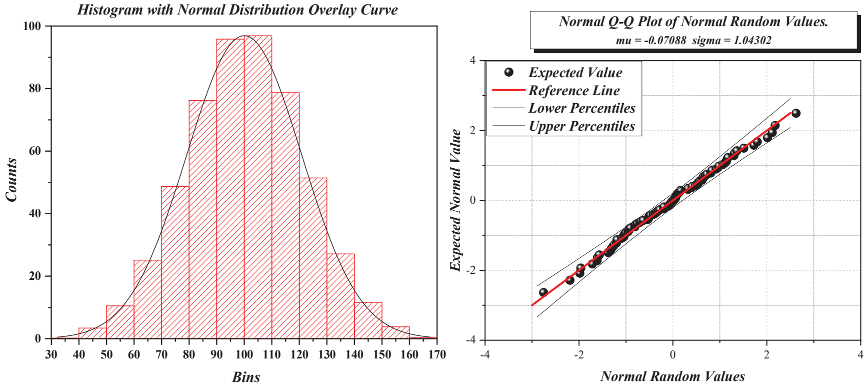

Figure 7 Distribution and fitting curve of predicted value and real situation value.

exhibits superior prediction performance. However, their predictive abilities are weaker during periods of significant real-world value fluctuation. Notably, the ISSA-BiLSTM model introduced in this study outperforms all other models in terms of overall prediction effectiveness. When the real situation value experiences significant fluctuations, the absolute error of the traditional BiLSTM model approaches 0.6. In comparison to the SOTA models demonstrate a reduction in absolute error; however, the improvement remains unsatisfactory. Our model exhibits a minimal absolute error between the predicted and actual values. Furthermore, its overall fluctuation range is narrow, indicating robustness.

5 Summarize

In the realm of IoT situation prediction, we introduce a security situation prediction model that leverages the BiLSTM neural network's prowess in time series prediction. To further augment its capabilities, we make several advancements. By stacking two layers of BiLSTM, we delve deeper into the intricacies of the data, unearthing richer insights. Additionally, we integrate a dropout layer and a dense layer to enhance the model's generalization abilities and facilitate the transformation of the output dimension, ultimately yielding precise predicted values. Furthermore, to address the inherent challenge of the sparrow search algorithm's susceptibility to local optima, we adopt reverse learning and an optimized strategy to refine SSA. This refined SSA algorithm aids in optimizing the parameters of the network, thereby elevating the accuracy of industrial IoT situation predictions.

Experimental results demonstrate the model's superior predictive performance compared to other established models. Notably, our model outperforms its peers in terms of prediction accuracy. Its mean squared error (MSE) and mean absolute error (MAE) stand at 0.023 and 0.018, respectively, representing a 30% and 25% reduction compared to existing models. These impressive figures underscore the model's capability to enhance the accuracy of industrial IoT security situation predictions.

Fundings: The research is supported by: 1. Technical research plan of the Ministry of public security Research on dark network investigation and forensic technology based on operation behavior (2020SJYJC27) and Qinglan Project of Jiangsu Province of China Excellent Youth Key Teacher (202042).

References

[1] Dong, Z., Su, X., Sun, L., and Xu, K. (2021). Network security situation prediction method based on strengthened lstm neural network. Journal of Physics: Conference Series, 1856(1), 012056 (7pp).

[2] Zhang, W., Bai, T. S., and Sun, F. (2019). A method for network security situation prediction based on lstm. Proceedings of the 29th European Safety and Reliability Conference (ESREL).

[3] Yonghao, W., and Cong, L. (2018). Intelligent Substation Network Security Situation Prediction Model Based on Gibbs-LDA. International Conference on Intelligent Computing, Communication and Devices.

[4] Chen, L., Fan, G., Guo, K., and Zhao, J. (2020). Security Situation Prediction of Network Based on Lstm Neural Network. IFIP WG 10.3 International Conference on Network and Parallel Computing. Springer, Cham.

[5] Chen, L., Fan, G., Guo, K., and Zhao, J. (2021). Security Situation Prediction of Network Based on LSTM Neural Network.

[6] Hong, X. (2020). Network security situation prediction based on grey relational analysis and support vector machine algorithm. Int. J. Netw. Secur., 22, 177–182.

[7] Ding, C., Chen, Y., Algarni, A. M., Zhang, G., and Peng, H. (2022). Application of fractal neural network in network security situation awareness. Fractals, 30.

[8] Bian, S., Wang, Z., Song, W., and Zhou, X. (2023). Feature extraction and classification of time-varying power load characteristics based on

pcanet and cnn+bi-lstm algorithms. Electric Power Systems Research, 217, 109149.

[9] Liao, H. M., Li, L. L., Xuan, J. X., and Wang, H. N. (2020). Application of Cryptographic Technology Based on Certificateless System in Electricity Internet of Things. 2020 3rd International Conference on Advanced Electronic Materials, Computers and Software Engineering (AEMCSE).

[10] Zhang, H., Kang, C., and Xiao, Y. (2021). Research on network security situation awareness based on the lstm-dt model. Sensors, 21(14), 4788.

[11] Xiang-Hao, C., and Zhen, L. (2019). Research on sql injection attack detection based on lstm neural network. Journal of Tianjin University of Technology.

[12] Albahrani, E. A., Lafta, S. H., and Ghayad, N. H. (2023). A Chaos-Based Encryption Algorithm for Database System. Journal of Cyber Security and Mobility, 12(01), 25–54.

[13] Yang, H., Zeng, R., Wang, F., Xu, G., and Zhang, J. (2020). An unsupervised learning-based network threat situation assessment model for internet of things. Security and Communication Networks, 2020(9), 1–11.

[14] Dong, M., Zhao, J., Li, D. A., Zhu, B., An, S., and Liu, Z. (2021). Isee: IIoT perception in solar cell detection based on edge computing:. International Journal of Distributed Sensor Networks, 17(11), 21–856.

[15] Li, J., Zhi, J., Hu, W., Wang, L., Yang, A. (2020). Research on the improvement of vision target tracking algorithm for internet of things technology and simple extended application in pellet ore phase. Future Generation Computer Systems, 110, 233–242.

[16] Zhang, B., Hu, W., Ghias, A. M. Y. M., Xu, X., Chen, Z., and Yan, J. (2023). Two-timescale autonomous energy management strategy based on multi-agent deep reinforcement learning approach for residential multicarrier energy system.

[17] Huang, Z., and Liang, Y. (2019). Research of data mining and web technology in university discipline construction decision support system based on mvc model. Library Hi Tech.

[18] Zang, Z. (2022). Analysis of financial management and decision-making in institution of higher learning based on deep learning algorithm. Mobile Information Systems.

[19] Kollipara, V. N. H., Kalakota, S. K., Chamarthi, S., Ramani, S., Malik, P., and Karuppiah, M. (2023). Timestamp Based OTP and Enhanced

RSA Key Exchange Scheme with SIT Encryption to Secure IoT Devices. Journal of Cyber Security and Mobility, 12(01), 77–102.

[20] Prasanna, K. S. L., and Challa, N. P. (2023). Deep bi-lstm with binary harris hawkes algorithm-based heart risk level prediction. SN Computer Science, 5(1).

[21] Liu, D., Cheng, J., Yuan, Z., Wang, C., and Niu, H. (2021). Prediction methods for energy internet security situation based on hybrid neural network. IOP Conference Series Earth and Environmental Science, 645, 012085.

[22] Lin, Z., Yu, J., and Liu, S. (2021). The prediction of network security situation based on deep learning method. International Journal of Information and Computer Security, 15(4), 386.

[23] Shang, L., Zhao, W., Zhang, J., Fu, Q., and Yang, Y. (2019). Network Security Situation Prediction Based on Long Short-Term Memory Network. 2019 20th Asia-Pacific Network Operations and Management Symposium (APNOMS).

[24] Lv, Y., Ren, H., Gao, X., Sun, T., and Guo, X. (2020). Multi-scale Risk Assessment Model of Network Security Based on LSTM.

[25] Li, S., Zhao, D., and Li, Q. (2020). A framework for predicting network security situation based on the improved lstm. EAI Endorsed Transactions on Collaborative Computing, 4(13), 165278.

[26] Zhao, W., Yang, H., Li, J., Shang, L., Hu, L., and Fu, Q. (2021). Network traffic prediction in network security based on EMD and LSTM.

[27] Tang, X., Chen, M., Cheng, J., Xu, J., and Li, H. (2019). A Security Situation Assessment Method Based on Neural Network. International Symposium on Cyberspace Safety and Security. Springer, Cham.

[28] Baccari, S., Hadded, M., Touati, H., & Muhlethaler, P. (2021). A Secure Trust-aware Cross-layer Routing Protocol for Vehicular Ad hoc Networks. Journal of Cyber Security and Mobility, 10(2), 377–402.

[29] Ashawa, M., Douglas, O., Osamor, J., and Jackie, R. (2022). Improving cloud efficiency through optimized resource allocation technique for load balancing using lstm machine learning algorithm. Journal of Cloud Computing, 11(1), 1–17.

[30] Yan, W., Qiao, L., Krishnapriya, S., and Neware, R. (2022). Research on prediction of school computer network security situation based on iot. International Journal of System Assurance Engineering and Management, 13.

Biography

Yubao Wu graduated from the University of Electronic Science and Technology of China of Information and Software Engineering 2016. Studied in Software Engineering, Nanjing Police University. He research interests include information security, computer forensics, and cyber crime investigation.