Research Article

Yun Zeng and Xiang Li*

QoS prediction using EMD-BiLSTM for II-IoT-secure communication systems

https://doi.org/10.1515/jisys-2023-0030
received February 28, 2023; accepted October 20, 2023

Abstract: To address the challenges of secure and reliable communication and system quality of service (QoS) prediction in intelligent production lines (IPL) in the Industrial Intelligent Internet of Things (II-IOT) environment, a redundant collaborative security model-based communication architecture is designed. First, the redundant collaborative security communication model is introduced to construct the network communication architecture of IPL, including the industrial-site mechanical floor, data awareness layer, and gateway and application layer. Then, to leverage the advantages of the empirical-mode decomposition (EMD) method and the bidirectional long short-term memory (BiLSTM) model in time-series data analysis and processing, an EMD-BiLSTM-based QoS prediction model is proposed that can synchronously achieve one-step and multi-step prediction of QoS attributes. The proposed model exhibits a prediction accuracy of up to 94.01% on the SourceForge dataset, with prediction, recall, and $F1$ values as high as 91.37, 90.60, and 90.99%, respectively. The proposed EMD-BiLSTM model can achieve better performance than the state-of-the-art QoS prediction models, indicating that the proposed model can be more effectively used to improve the reliable communication level of II-IoT.

Keywords: Industrial Intelligent Internet of Things, secure communication, EMD, BiLSTM, QoS prediction

1 Introduction

Internet of Things (IoT) has attracted widespread attention and has been applied in many fields, such as military, logistics, industrial production, agriculture and forestry, and fire monitoring [1–3]. The rapid development of IoT has also promoted technological innovation in these fields. At the same time, the Industrial Intelligent Internet of Things (II-IoT) has gradually become a research hotspot [4–6]. The II-IoT combines technologies such as IoT and machine-to-machine automated communication to accurately control industrial processes, leading to efficient, stable, and sustainable industrial production.

Compared with the original IoT, the II-IoT has the following four characteristics: (1) the II-IoT is required to have low-latency characteristics due to the timeliness of industrial control instructions. When the delay control is at the millisecond level, the communication reliability can reach over 99.99%. Otherwise, the operation of the industrial control system (ICS) may be significantly affected [7–9]. (2) II-IoT mostly uses lightweight sensors and actuators, and its hardware computing and storage resources are relatively limited. (3) The data volume in II-IoT is relatively small, but it requires higher communication reliability. (4) The II-IoT systems must also be secure to resist malicious attacks and ensure the safety of industrial equipment and workers [10,11].

* **Corresponding author: Xiang Li,** Information Management Office, Yellow River Conservancy Technical Institute, Kaifeng, Henan, 475004, China, e-mail: lix@yrcti.edu.cn
Yun Zeng: Information Management Office, Yellow River Conservancy Technical Institute, Kaifeng, Henan, 475004, China, e-mail: zengy@yrcti.edu.cn

With the deepening of IT/operational technology integration, network intrusion behaviors are becoming more complex and diverse, putting all the field devices, control systems, and network devices of the ICSs at risk [12–14]. To deal with such threats, the traditional ICS must be upgraded to an intelligent control system for intelligent manufacturing. However, II-IoT typically faces challenges such as complex protocol types, incompatibility between protocols, difficulty in effective integration of industrial devices, and low communication efficiency [15–17]. Therefore, designing a practical and feasible secure communication system architecture for II-IoT is essential to ensure the safe operation of intelligent manufacturing systems [18–20]. Moreover, intelligent production line (IPL) networks in II-IoT typically face a severe problem. Specifically, the network is dynamic and variable, and the dynamic quality of service (QoS) attributes of servers exhibit strong instability due to time and space factors. This will make it difficult for users to select services that meet their needs in the candidate service set, and it will also increase the latency of communication node task processing.

To address the challenges of network security and reliable QoS in IPLs, a new II-IoT-secure communication architecture and an EMD-BiLSTM-based QoS prediction model for II-IoT communication systems are proposed in this study. Specifically, the main contributions are as follows:

1. For the secure communication of II-IoT, a redundant collaborative security communication model is introduced. The model ensures secure communication between device data by establishing multiple communication transmission paths between II-IoT communication-aware aggregation nodes.
2. An EMD-BiLSTM-based QoS prediction model is proposed that can address the dynamic and variable characteristics of networks in II-IoT communication systems. The empirical-mode decomposition (EMD) method is combined with the bidirectional long short-term memory (BiLSTM) model EMD to establish a multivariate data input pattern that can mine the potential information of QoS temporal data at a finer granularity level. This allows for accurate monitoring of the service status of network nodes, reduction of task processing delay, and real-time and reliable communication for system devices.

2 Related work

The two important security services of the communication security of industrial scenarios are the authenticity and integrity of messages. Security authentication is an effective security mechanism that can meet the aforementioned requirements. The security authentications of traditional systems are carried out on the physical layer, and the authentication algorithms used usually bring large delays. Therefore, under the II-IoT environment, it is of great practical significance to research on secure communication technology.

2.1 Secure communication schemes of II-IoT

Yoshino et al. [20] aimed to address the current problem of security concerns among managers in different industries about using the Internet to operate machines and the inapplicability of traditional methods to network devices. Choudhary et al. [21] proposed a powerful exchange protocol to solve the vulnerabilities of existing solutions using a variety of different encryption operations. However, this method cannot meet the high real-time and high-stability requirements of II-IoT. Ullah et al. [22] proposed a signcryption scheme to address the problems of key escrow and private key distribution in traditional identity-based or certificateless signcryption schemes. However, the algorithm lacks the proof of encryption effect, can only encrypt a specific number of characters, and cannot carry out bitstream data. Ji et al. [23] analyzed the probability of successful attacks on a random pilot-based key and derived its closed-form mathematical expression. Using this analysis, a solution for safe low-latency communication and active interference in network control systems for II-IoT applications was proposed. However, it cannot solve the problem of asymmetric key management in the resource-constrained environment. Aimed at the external risks and threats faced by II-IoT network performance and node transmission security, Zhu et al. [24] proposed a data transmission method by authorizing access control and increasing users' network access rights. However, the security of this scheme needs to be

improved, and it may cause network congestion. To address the network physical vulnerabilities in II-IoT, Ullah et al. [25] proposed a signature scheme that enhanced the security of data transmission to a certain extent and reduced the amount of computation in the process of data communication and security assurance. However, this method has not significantly improved in terms of time consumption and resource usage, making it difficult to apply directly in resource-constrained network environment. To address the high computational requirements of traditional II-IoT authentication protocols, which make them unsuitable for resource-constrained devices, a hash function-based authentication protocol has been proposed by Lara et al. [26]. This protocol reduces the communication cost to a certain extent, but its key update and storage methods are not sufficiently robust, which reduces the security of key management. Aiming at the problem that most existing authentication schemes used for II-IoT are vulnerable to privileged user attacks and terminal device tracking attacks, an II-IoT authentication scheme using SGX was proposed by Xin et al. [27], it was based on the characteristics of SGX storage master key and SGX storage confidentiality. However, this method needs to run on specific hardware and cannot be applied to II-IoT defined by software. Chen et al. [28] proposed a multi-factor authentication protocol that effectively alleviates security attacks on IoT devices through physical non-cloning capabilities. However, the running cost of this scheme is relatively high. Parai and Islam [29] proposed a data-monitoring architecture using elliptic curve cryptography for the IoT to improve data security and reduce the execution cost of the scheme. However, this scheme requires a trusted third-party centralized identity authentication mechanism to ensure the normal operation of the system. If it is applied to the II-IoT environment, the flexibility of the system is difficult to be guaranteed. To solve this problem, Zhong et al. [30] designed a cross-domain II-IoT security authentication system for joint production of multiple manufacturers. This approach not only ensures the flexibility of the system but also reduces the overall communication overhead. However, the single-channel communication model adopted in this scheme will easily lead to data transmission failure if the communication node fails, making it unsuitable for ILP in II-IoT.

Several studies have been conducted on QoS security assurance and QoS prediction. Sham and Vidyarthi [31] designed an adaptive communication security scheme for cloud and mist computing collaborative systems. This scheme improves security and synchronization performance but has high requirements for application scenarios. Chen et al. [32] proposed a QoS prediction model based on wide-range perception matrix factorization (WRAMF), improving the prediction accuracy to a certain extent and achieving high communication efficiency. However, the performance is degraded when the model is oriented toward location-based data. Shi et al. [33] proposed a hybrid QoS prediction model based on web semantic information recommendation (WSIR) and effectively improved the service quality of mobile social network users in 5G communication scenarios. Barmpounakis et al. [34] proposed a QoS prediction model using geospatial discretization to solve the vehicle management problem in a 5G communication environment. However, such methods are unable to solve the sparsity problem of data. Chen et al. [35] combined factor decomposition machine with deep cross network (FDM-DCN) and developed a context-aware QoS prediction model for the IoT, considering both low-order and high-order features of user data. However, the performance of this model needs to be improved in dynamic and ever-changing network scenarios.

Numerous existing secure communication architectures use a single channel, which makes it difficult to adapt to ILP scenarios of II-IoT. Therefore, a redundant collaborative security communication model is introduced that establishes multiple communication transmission paths between II-IoT communication-aware aggregation nodes to ensure secure communication of device data. However, most of the above-mentioned methods have been used for QoS prediction and recommendation of Web services on the Internet and 5G scenarios, making it difficult to meet the requirements of service quality analysis and prediction of ILP communication networks and II-IoT service recommendation in the II-IoT environment. If the QoS of the ILP network is poor, the server task processing delay will be significantly increased, and the real-time reliable communication level of the II-IoT equipment in the production line network will be reduced.

This study proposes an EMD-BiLSTM-based QoS prediction model for II-IoT communication systems. The proposed model simultaneously realizes one-step and multi-step prediction of the dynamic QoS attributes of the II-IoT, significantly improving the accuracy of QoS prediction in complex networks. This meets the user's demand for selecting appropriate services from the candidate service set, effectively reduces the node task processing delay, and ensures the best QoS of network nodes within a fixed time range.

3 Proposed model for II-IoT

3.1 II-IoT overall structure

To address the complex and incompatible protocol types of IPL network communication, and the difficulty of integrating industrial equipment, this study proposes an IPL communication architecture that integrates the OPC unified architecture (OPC UA). The architecture maps all kinds of communication equipment in the IPL to the OPC UA address space, realizing the interconnection between the industrial equipment and the upper application, and meeting the flattening requirements of the industrial network [36]. The overall structure of the network communication system for IPL is shown in Figure 1.

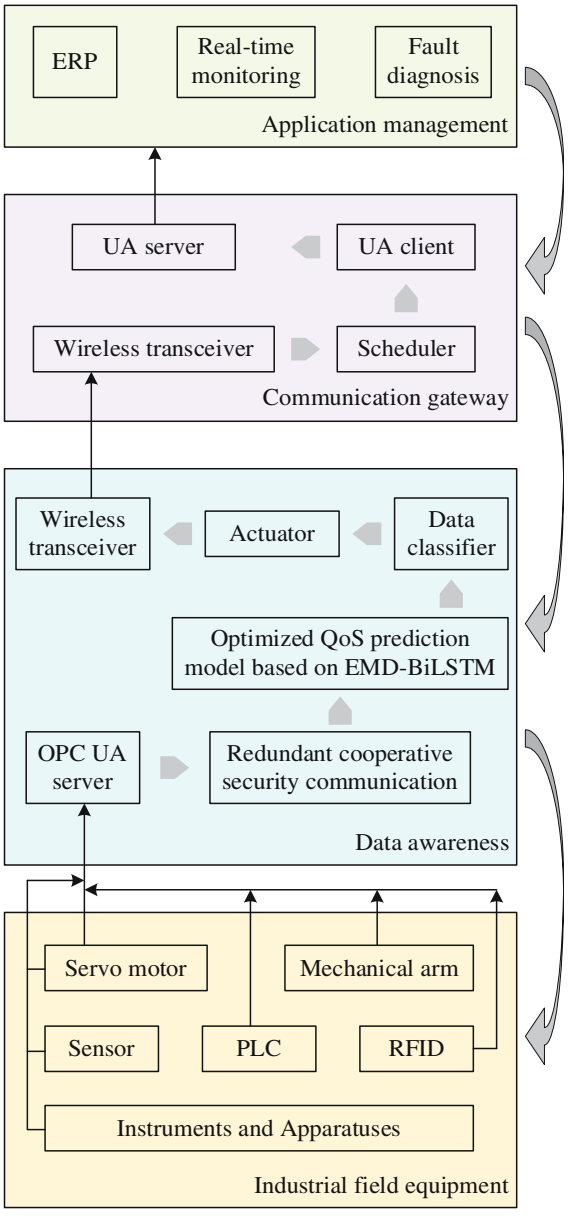

Figure 1: Network communication architecture for IPL.

The network communication architecture for IPLs is divided into the following four parts from bottom to top:

(1) Industrial-site equipment layer. This layer is composed of multiple types of IPL communication equipment and industrial sensors for fault diagnosis. In complex industrial field environments, the IPL system uses programmable logic controller (PLC), radio frequency identification (RFID), industrial instruments, servo motors, mechanical arms, and other equipment to collaborate on the product processing process, improving production efficiency. At the same time, wireless sensors are deployed on the site of the entire IPL to predict and respond to equipment failures in time. This reduces the risk of equipment failures in the IPL.

(2) Data awareness layer. This layer includes an OPC UA communication module, data classifier, actuator, wireless transceiver, and other modules integrated into the IPL equipment, providing data acquisition and signal transmission functions for the system. At the same time, the address space is established to realize the connection and communication between Internet applications and underlying wireless sensor networks. During the data collection phase, the data classifier can be used to assist the IPL system in further setting the type of data to be transmitted.

(3) Communication gateway layer. The UA client accesses the address space to collect and receive data from sensing layer devices. As the data scheduling module in the system, the scheduler performs classified transmission through the predefined data. This module realizes preemptive transmission of high-priority services, and it is an important part of the multi-priority dynamic resource scheduling model.

(4) Application management layer. This layer is composed of various application-level systems that manage IPL equipment. These systems use the OPC UA-based wireless communication environment to collect data, which enables unified system management and provides the functions of sensing equipment operation status, predicting failure probability, and initially diagnosing failure causes.

3.2 Redundant cooperative secure communication model

To address the vulnerability of the traditional II-IoT unitary transmission method and the lack of secure transmission standards for the IPL information data in the II-IoT environment, a basic framework of II-IoT

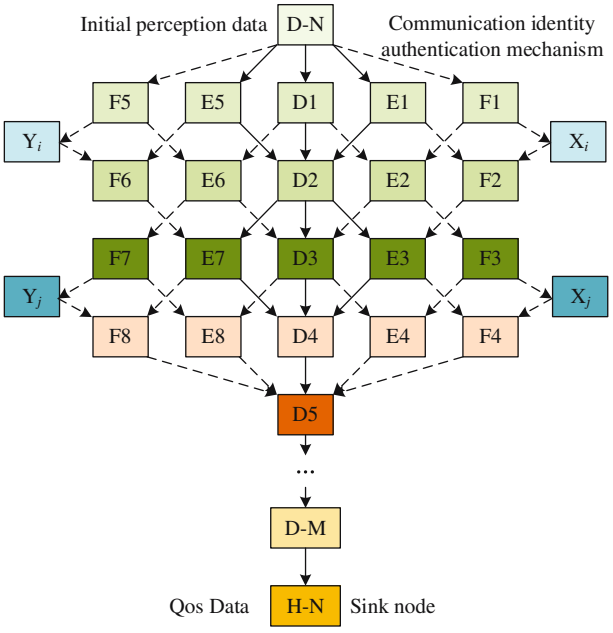

Figure 2: Multipath redundancy cooperative secure network model for II-IoT.

using redundancy communication and auxiliary path redundant security is constructed. The multipath redundancy cooperative secure network model for II-IoT is shown in Figure 2.

In Figure 2, D-N, D-M, and H-N are the initial, relay, and sink nodes, respectively; D is the primary path; E is the primary secondary path; and D represents the secondary path. The multi-path data redundancy communication mechanism has advantages over the II-IoT traditional single-path communication strategy. To ensure secure equipment data transmission in II-IoT environments, multiple communication transmission paths between the II-IoT communication sensing and sink node are established. The path that meets security conditions is selected based on redundant transmission requirements and the status of the communication node and other factors. Based on the redundant communication mechanism, the II-IoT multi-path redundant cooperative secure communication model first splits and encrypts the initial sensing communication data of the II-IoT based on the sensing data splitting encryption method in the II-IoT communication data multi-communication identity authentication mechanism.

The II-IoT communication data threshold secret sharing mechanism splits the data into j data packets that will be sent to the network node. If the aggregation node successfully receives the transmitted packet information, the original data can be restored. Otherwise, the original data cannot be obtained. Next, the multipath redundancy cooperative secure network model uses the II-IoT auxiliary path redundant secure transmission method to establish the multiple redundant auxiliary secure communication paths from the source initial sensing communication node to the sink node to encrypt the split encrypted data point pairs. Finally, the sink node in the multi-path redundant cooperative secure communication model reconstructs the received split encrypted packets based on the encryption-aware QoS data method in the II-IoT communication data multi-communication identity authentication mechanism to restore the true value of the II-IoT initial awareness communication data.

3.3 Optimized QoS prediction model based on EMD-BiLSTM

The key to II-IoT communication is to select the one with the best QoS from a set of candidate nodes. To accurately grasp the service status of network nodes, this study proposes an optimized QoS prediction model based on EMD-BiLSTM, which integrates the advantages of EMD and BiLSTM in the analysis and processing of time-series data. The proposed model will ensure that the calling object obtains the best quality of service, reduce the network node task processing delay, and provide a solution to deduce the QoS attribute trend over a longer service time and judge the communication service quality of each server in the network.

The optimized QoS prediction model based on EMD-BiLSTM realizes the single-step and multi-step prediction of QoS attributes, enabling the model to capture the characteristics of QoS dynamic transformation. The model mainly includes QoS data preprocessing, hybrid model construction, and single/multi-step prediction execution. The overall architecture of the proposed EMD-BiLSTM-based QoS prediction model is shown in Figure 3.

3.4 EMD

EMD is an adaptive data processing method that can decompose signals according to the time-scale characteristics of the data without any prior system. Therefore, EMD is suitable for signal analysis [37]. EMD decomposes the non-stationary time-series signal into several groups of intrinsic mode functions (IMFs) and residuals (Res) of different frequencies. Each group of IMFs represents the local characteristics of the original signal on a certain time scale, and the sum of these IMFs is equal to the original signal [38]. At the same time, these IMFs have two constraints:

(1) Over the entire time domain, the number of extrema and zero-crossing points of each IMF is the same or differs by at most 1.

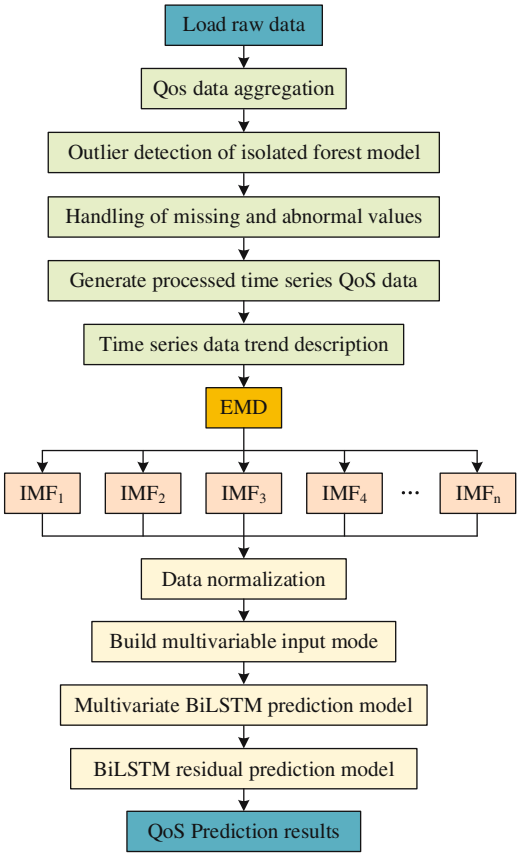

Figure 3: Overall architecture of the optimized QoS prediction model based on EMD-BiLSTM.

(2) The average value of the upper envelope of the local maximum and the lower envelope of the local minimum must be 0.

EMD algorithm superimposes all IMFs to obtain raw data without any loss, which has excellent reconfigurability. QoS time-series data have nonlinear and non-stationary characteristics, and it is affected by many factors. The specific workflow of EMD is shown in Figure 4.

Assuming that the input original time-series signal is expressed as $x(t)$, the local maximum and minimum of $x(t)$ are determined. Then, the upper envelope and the lower envelope are fitted and fused to obtain the average calculation result:

$$m_t = \frac{x_u[t] + x_l[t]}{2}. \tag{1}$$

Subtracting the time-series signal from the average value yields

$$h_t = x(t) - m_t. \tag{2}$$

Determine whether h_t meets the generated conditions of IMF. If these conditions are not met, continue to decompose the decomposed signal. Otherwise, save the generated components of IMF and calculate the corresponding residuals $r(t)$. Determine whether $r(t)$ is a monotonic function. If it is not, continue to decompose the decomposed signal until all IMFsare obtained. Then, calculate the final residual value and the algorithm converges. Use equation (3) to represent the relationship between the initial input signal and the obtained decomposition. In the equation, $x(t)$represents the original input signal, $IMF_i(t)$represents the *i-th* IMF value obtained after multiple decompositions, and $r_n$represents the residual.

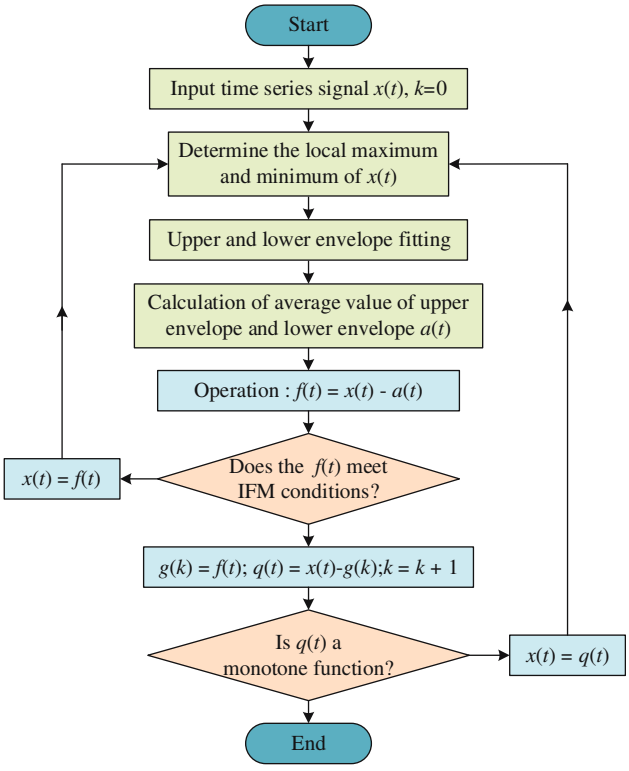

Figure 4: Detailed workflow of EMD.

$$x(t) = \sum_{i=1}^{n} \mathrm{IMF}_i(t) + r_n. \tag{3}$$

Equation (3) indicates that all overlays can obtain the original input signal without any loss, reflecting the strong reconfigurability of this algorithm. The temporal characteristics of QoS have nonlinear and non-stationary characteristics and are simultaneously influenced by many external factors. It can be seen that using EMD to decompose QoS temporal features is reasonable.

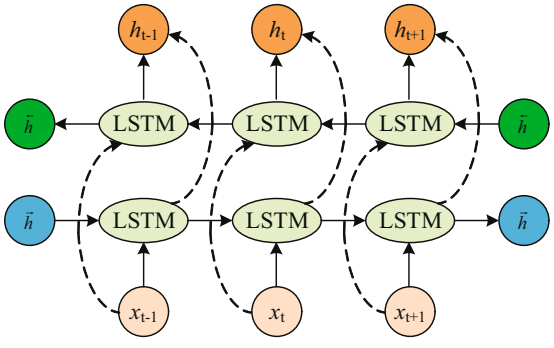

Figure 5: Structure of BiLSTM.

3.5 BiLSTM

BiLSTM is composed of two LSTMs with opposite directions that produce the final output result [39]. The model structure of BiLSTM is shown in Figure 5.

Assuming that the input signal at a time t is x_t, the output signal obtained by extracting temporal features using BiLSTM is as follows:

$$\overrightarrow{h_t} = \mathrm{LSTM}(x_t, \overrightarrow{h_{t-1}}), \tag{4}$$

$$\overleftarrow{h_t} = \mathrm{LSTM}(x_t, \overleftarrow{h_{t-1}}), \tag{5}$$

$$h_t = w_1\overrightarrow{h_t} + w_2\overleftarrow{h_t} + b_t, \tag{6}$$

where h_t is the output result of BiLSTM at t, $\overleftarrow{h_t}$ and $\overrightarrow{h_t}$ are divided into forward output and reverse output of LSTM at t, respectively. $\overrightarrow{h_t}$ is calculated from the input $\overrightarrow{h_t}$ at t and the forward output $\overrightarrow{h_{t-1}}$ at $t-1$, $\overleftarrow{h_t}$ is calculated from the input x_t at t and the reverse output $\overleftarrow{h_{t-1}}$ at $t-1$, and h_t is calculated from $\overleftarrow{h_t}$ and $\overrightarrow{h_t}$.

4 Experiment and analysis

4.1 Experimental environment

Table 1: Experimental environment configuration

Items	Configuration
System environment	Windows 10, CentOS, Colab cloud computing environment
Software	JDK1.8, Python3.7
Database	MySQL 5.7.13, MongoDB 4.0.13, Redis 3.2.12
Deploy software	Maven, Tomcat, Flask
Test tools	MQTTBox, Postman

Table 1 shows the experimental environment. The system test environment consisted of Windows 10, CentOS, and Colab cloud computing. The system was compiled and packaged using Maven and ran on Tomcat in the Windows 10 environment. MongoDB, MySQL, and Redis were deployed on the CentOS server. Chrome browser was used to test the interaction with the front end of the system.

4.2 Dataset

The experiment used the open-source Web service dataset to evaluate and verify the results of the QoS prediction model using EMD-BiLSTM. The open-source Web service dataset from SourceForge was collected daily from 8:00 AM to 5:00 PM in 15-min intervals. It contains response time and throughput data for multiple consecutive days, divided into four sub-datasets of 2,000 continuous data points each. For this experiment, the response time data from “Web Service 4” were used.

4.3 Evaluating indicator

Five evaluation indicators were selected, namely, accuracy (A), precision (P), recall rate (R), and $F1$.

The A refers to the proportion of data classified as correct in all data. The calculation is shown in the following formula:

$$A = \frac{T_P + T_N}{T_P + T_N + F_P + F_N}, \tag{7}$$

where P is the proportion of normal data correctly classified in the actual normal data, and the calculation is shown in the following formula:

$$P = \frac{T_P}{T_P + F_P}, \tag{8}$$

where R is the proportion of correctly classified normal data among all data classified as normal, and the calculation is shown in the following formula:

$$R = \frac{T_P}{T_P + F_N}. \tag{9}$$

$F1$ is calculated by the following equation:

$$F1 = \frac{2DR}{D + R}, \tag{10}$$

where T_P (true positive) represents the data in the forecast result that are actually positive and predicted to be positive, T_N (true negative) indicates that the data are actually negative and predicted to be negative; F_P (false positive) is data that are actually positive but predicted to be negative; and F_N (false negative) is data that are actually negative but predicted to be positive.

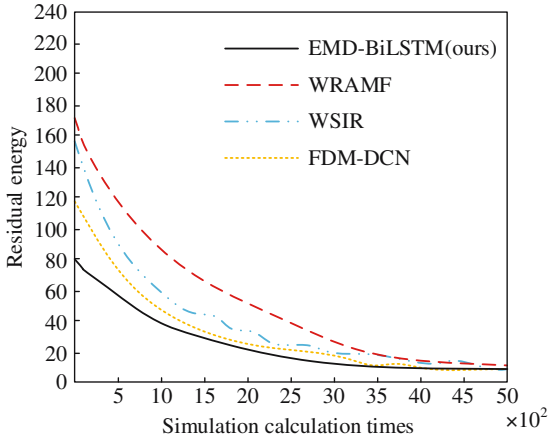

Figure 6: Network energy surplus in different methods.

4.4 Model training

In the process of developing energy-saving systems, the residual energy of the network is an important parameter to be considered. To verify the superiority of the proposed technology based on II-IoT in terms of energy-use efficiency, the EMD-BiLSTM was simulated and compared with WRAMF [32], WSIR [33], and FDM-DCN [35]. The residual energy of different methods is shown in Figure 6.

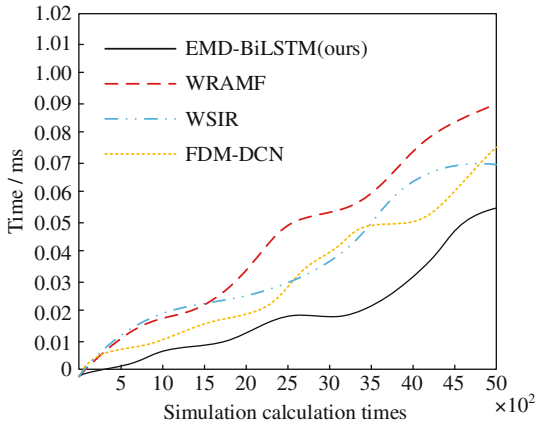

Figure 7: Response time of different II-IoT systems.

The results in Figure 6 indicate that the proposed EMD-BiLSTM has less residual energy and uniform power distribution compared with WRAMF, WSIR, and FDM-DCN. A small amount of residual energy means that the system can use most of the power provided for processing. This is one of the reasons for considering the proposed effective resource allocation method.

The system response time of WRAMF, WSIR, FDM-DCN, and the proposed EMD-BiLSTM is compared, and the results are listed in Figure 7.

It can be seen from Figure 7 that the time consumption curve of all methods is weak at first but rising steadily after some simulations. The proposed method exhibits the slowest increase in response time per simulation, indicating that it takes the least time to achieve the same effect. This is because the power is evenly distributed to all nodes after the cluster, so the system responds quickly.

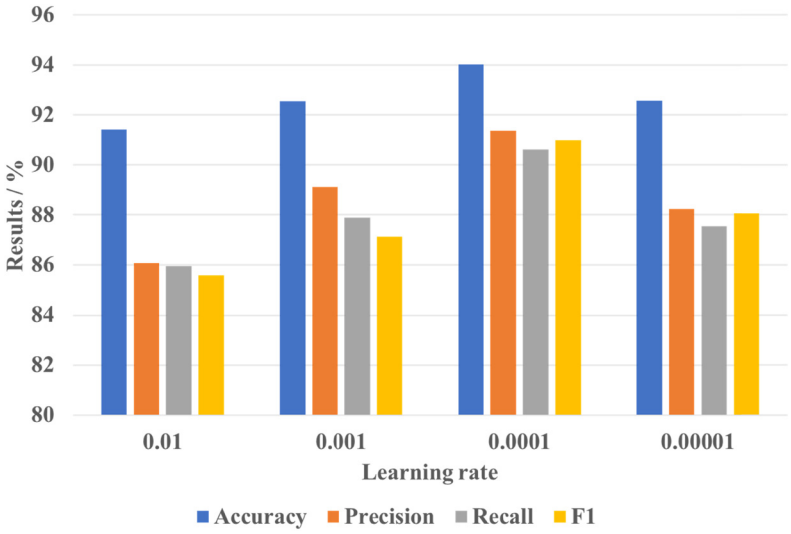

Figure 8: Prediction results obtained under different learning rates.

During the model training process, the setting of the learning rate usually affects the final prediction effect. Therefore, different learning rates were set to explore the best prediction results, as shown in Figure 8.

Figure 8 shows that the proposed EMD-BiLSTM model can achieve the best prediction performance when the learning rate is set to 0.0001. By analyzing the reasons, a high learning rate will lead to underfitting of the

model, resulting in lower prediction results. If the learning rate is too low, it will make the model converge too slowly and unstable, and to some extent, it will also reduce the prediction results.

Table 2: Results obtained by four different methods

Indicator	Method			
	EMD-BiLSTM (ours) (%)	WRAMF (%)	WSIR (%)	FDM-DCN (%)
A	94.01	89.10	92.16	93.29
P	91.37	88.24	89.82	90.08
R	90.60	86.67	88.93	89.78
*F*1	90.99	85.98	88.74	89.03

4.5 Comparative analysis

To verify the superiority of the proposed EMD-BiLSTM, it was compared with WRAMF [32], WSIR [33], and FDM-DCN [35] using the same dataset and evaluation metrics. The final calculation results of different methods are listed in Table 2.

In Table 2, under the same database, the *A*, *P*, *R*, and *F*1 of the proposed EMD-BiLSTM are higher than those of the other three comparison models. The *A* of the proposed algorithm is 94.01%, the *P* is 91.37%, the *R* is 90.60%, and the *F*1 is 90.99%. Analyzing the reasons, several comparative models can usually consider the nonlinear problem of QoS data, but WRAMF and WSIR only focus on the time-varying characteristics of individual component data, ignoring the interaction between component data. Although FDM-DCN can consider the interaction between component data, it ignores the non-stationary characteristics of QoS data. The proposed EMD-BiLSTM model solves the problems of nonlinearity and non-stationary in QoS data through EDM. At the same time, BiLSTM is used to model the temporal characteristics of multiple component time-series data and the potential relationship between components. This allows the model to extract fine-grained

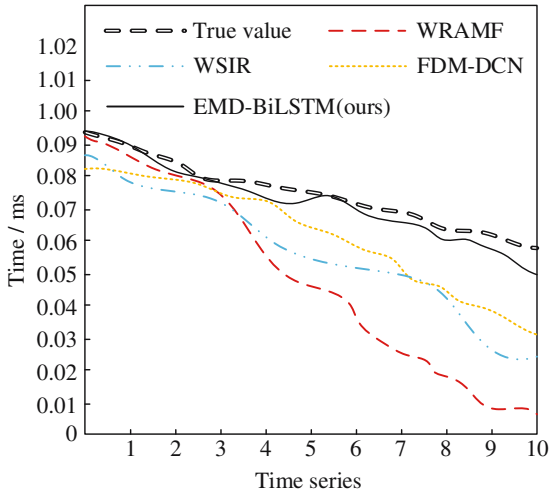

Figure 9: Multi-step predicted results in time series of different methods.

information from QoS time-series data and fully capture the temporal correlations between components of different scales. Therefore, the proposed EMD-BiLSTM model exhibits better prediction performance for dynamically changing QoS temporal data with nonlinear and non-stationary characteristics.

The multi-step predicted results in time series of WRAMF, WSIR, FDM-DCN, and the proposed EMD-BiLSTM are listed in Figure 9.

It can be seen from Figure 9 that the predicted response time values by the proposed EMD-BiLSTM model are closer to the real values. The errors of WSIR and FDM-DCN are relatively large, and the prediction results of WRAMF begin to have a large deviation at the fifth moment, which is due to the accumulation of prediction errors in the previous steps. The proposed model has an error correction function, which can properly correct the deviation and reduce the deviation of the prediction results. Although the prediction results of the other three comparison methods differ significantly from the real response time, the trend of the actual corresponding time data can still be captured. The proposed EDM-BiLSTM model can maintain high prediction

Table 3: Experimental results of ablation model

Indicator	Model			
	A **(%)**	***P*** **(%)**	***R*** **(%)**	***F*****1 (%)**
EMD	62.42	58.39	56.48	57.79
LSTM	75.32	73.48	72.74	71.66
EMD-WLSTM	89.46	87.29	86.62	87.07
EMD-BiLSTM (ours)	94.01	91.37	90.60	90.99

accuracy while ensuring a small-time error with the true value, which has effectively reduced the task processing delay of communication nodes. Overall, the proposed model has better performance than the other models.

To better verify the role and importance of each part of the model, Table 3 shows the ablation experiment results.

In Table 3, the results of the proposed EMD-BiLSTM model are the highest. The index value of the EMD-LSTM model is relatively low. However, the evaluation index values of EMD and LSTM models are very low, making them inapplicable to the actual situation. This is because the simple EMD model can decompose the signal according to the time-scale characteristics of the data itself, but it cannot properly capture the dependence of a long distance, while the simple LSTM is the opposite. Although the EMD-LSTM model can learn and forget information through the training process, it cannot capture the two-way semantic dependence. The EMD-BiLSTM model combines the advantages of both EMD and BiLSTM models and achieves the best performance results.

5 Conclusion

To address the challenges of secure and reliable communication and system QoS prediction in IPLs under the II-IoT environment, this study proposes a communication architecture based on a redundant collaborative security model. Compared to the single-path communication model, the introduction of a multi-path redundancy mechanism effectively improves the security of II-IoT systems. This study proposes an EMD-BiLSTM-based QoS prediction model that combines the advantages of the EMD method and the BiLSTM model in time-series data analysis and processing. EMD can reconstruct raw data without loss and has excellent reconfigurability, which improves the performance of QoS time-series data analysis. The optimized QoS prediction model based on EMD-BiLSTM can reduce the task processing delay of network nodes, providing technical solutions to

deduce the QoS attribute trend in a longer service time and judge the quality of communication service of each server in the network.

One of the limitations of this article is that the proposed EMD-BiLSTM model has only been validated on small-scale datasets. Therefore, in future work, technologies such as BERT and transformer will be introduced to design new prediction models for solving multidimensional data problems in large-scale complex industrial scenarios. In addition, as the number of terminal devices continues to increase, the computing center load of the designed II-IoT system will also continue to increase, which is not conducive to application in ultra-large application scenarios. Therefore, federated learning and blockchain technology with distributed characteristics will be introduced into the designed II IoT security system. While the security is improved, it will be better applied in ultra-large industrial scenarios.

Acknowledgments: This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

Funding information: This study was not supported by any fund projects.

Author contributions: Yun Zeng: Writing – Original Draft; Writing – Review & Editing; Formal analysis. Xiang Li: Conceptualization; Methodology.

Conflict of interest: All authors declare that there have no conflicts of interest to publish this article.

Data availability statement: The data included in this study are available without any restriction.

References

[1] Du M, Wang K. An SDN-enabled pseudo-honeypot strategy for distributed denial of service attacks in industrial internet of things. IEEE Trans Ind Inform. 2020;16(1):648–57.

[2] Serror M, Hack S, Henze M, Schuba M, Wehrle K. Challenges and opportunities in securing the industrial internet of things. IEEE Trans Ind Inform. 2021;17(5):2985–96.

[3] Jiang X, Pang Z, Luvisotto M, Pan F, Candell R, Fischione C. Using a large data set to improve industrial wireless communications: Latency, reliability, and security. IEEE Ind Electron Mag. 2019;13(1):6–12.

[4] Xu S, Xu W, Pan C, Elkashlan M. Detection of jamming attack in non-coherent massive SIMO systems. IEEE Trans Inf Forensics Secur. 2019;14(9):2387–99.

[5] Ramu G, Mishra Z, Acharya B. Hardware implementation of Piccolo Encryption Algorithm for constrained RPID application. 2019 9th Annual Information Technology, Electromechanical Engineering and Microelectronics Conference (IEMECON). Jaipur, India: 2019. p. 85–9.

[6] Kim J, Jo G, Jeong J. A novel CPPS architecture integrated with centralized OPC UA server for 5G-based smart manufacturing. Procedia Comput Sci. 2019;155:113–20.

[7] Jirsik T, Trka T, Celeda P. Quality of service forecasting with LSTM neural network. 2019 IFIP/IEEE Symposium on Integrated Network and Service Management (IM). Arlington, VA, USA: 2019. p. 251–60.

[8] Li M, Yin Z, Ma Y, Wang C, Chai A, Lian M. Design and verification of secure communication scheme for industrial IoT IPL system with multi-path redundancy and collaboration. Neural Comput Appl. 2021;35:13879–93.

[9] Xie N, Zhang S. Blind authentication at the physical layer under time varying fading channels. IEEE J Sel Areas Commun. 2018;36(7):1465–79.

[10] Li Y, Jiang J, Lee C, Hong SH. Practical implementation of an OPC UA TSN communication architecture for a manufacturing system. IEEE Access. 2020;8(5):100–11.

[11] Morato A, Vitturi S, Tramarin F, Cenedese A. Assessment of different OPC UA implementations for industrial IoT-based measurement applications. IEEE Trans Instrum Meas. 2020;70:1–11.

[12] Pan F, Pang Z, Luvisotto M, Jiang X, Jansson RN, Xiao M, et al. Authentication based on channel state information for industrial wireless communications. 44th Annual Conference of the IEEE Industrial-Electronics-Society (IECON). Washington, DC; 2018. p. 4125–30.

[13] Su WT, Chen WC, Chen CC. An extensible and transparent thing-to-thing security enhancement for MQTT protocol in IoT environment. 2019 Aarhus, DENMARK: Global IoT Summit (GIoTS); 2019. p. 1–4.

[14] Syu Y, Wang CM. QoS time series modeling and forecasting for web services: A comprehensive survey. IEEE Trans Netw Serv Manag. 2020;18(1):926–44.
[15] Wan J, Yang J, Wang S, Li D, Li P, Xia M. Cross-network fusion and scheduling for heterogeneous networks in smart factory. IEEE Trans Ind Inform. 2020;16(9):6059–68.
[16] White G, Clarke S. Short-term QoS forecasting at the edge for reliable service applications. IEEE Trans Serv Comput. 2022;15:1089–102.
[17] White G, Palade A, Clarke S. Forecasting QoS attributes using LSTM networks. International Joint Conference on Neural Networks (IJCNN). Rio de Janeiro, Brazil; 2018. p. 1–8.
[18] Wu H. Research proposal: Reliability evaluation of the apache kafka streaming system. 2019 IEEE International Symposium on Software Reliability Engineering Workshops (ISSREW). Berlin, Germany; 2019. p. 112–3.
[19] Yang GR, Molano-Mazon M. Towards the next generation of recurrent network models for cognitive neuroscience. Curr Opin Neurobiol. 2021;70:182–92.
[20] Yoshino D, Watanobe Y, Naruse K. A highly reliable communication system for internet of robotic things and implementation in RT-middleware with AMQP communication interfaces. IEEE Access. 2021;9(6):167229–41.
[21] Choudhary K, Gaba GS, Butun I, Kumar P. MAKE-IT-A lightweight mutual authentication and key exchange protocol for industrial internet of things. Sensors. 2020;20(18):246–55.
[22] Ullah I, Alomari A, Abdullah AM, Kumar N, Alsirhani A, Noor F, et al. Certificate-based signcryption scheme for securing wireless communication in industrial internet of things. IEEE Access. 2022;10(3):105182–94.
[23] Ji ZJ, Yeoh PL, Chen GJ, Zhang J, Zhang Y, He Z, et al. Physical-layer-based secure communications for static and low-latency industrial internet of things. IEEE Internet Things J. 2022;9(19):18392–405.
[24] Zhu W, Zheng XD, Huang FX, Ruan Z, Cui J. DTSW: A data transmission scheme based on weighted security partition model in industrial Internet of Things environment. Adv Mech Eng. 2019;11(4):125–34.
[25] Ullah I, Alkhalifah A, Althobaiti MM, Al-Wesabi FN, Hilal AM, Khan MA, et al. Certificate-based signature scheme for industrial internet of things using hyperelliptic curve cryptography. Wirel Commun Mob Comput. 2022;2022(15):38–46.
[26] Lara E, Aguilar L, Sanchez MA. Lightweight authentication protocol for M2M communications of resource-constrained devices in industrial Internet of Things. Sensors. 2020;20(2):216–25.
[27] Xin L, Zhenbin G, Yuchen S. An authentication scheme based on SGX for industrial Internet of Things. Netinfo Secur. 2021;6(5):1–10.
[28] Chen Z, Cheng Z, Luo W, Ao J, Liu Y, Sheng K, et al. FSMFA: Efficient firmware-secure multi-factor authentication protocol for IoT devices. Internet Things. 2023;21:100685.
[29] Parai K, Islam SH. IoT-RRHM: Provably secure IoT-based real-time remote healthcare monitoring framework. J Syst Architecture. 2023;138:102859.
[30] Zhong H, Gu C, Zhang Q, Cui J, Gu C, He D. Conditional privacy-preserving message authentication scheme for cross-domain Industrial Internet of Things. Ad Hoc Netw. 2023;144:103137.
[31] Sham EE, Vidyarthi DP. CoFA for QoS based secure communication using adaptive chaos dynamical system in fog-integrated cloud. Digital Signal Process. 2022;126:103523.
[32] Chen Z, Sun Y, You D, Li F, Shen L. An accurate and efficient web service QoS prediction model with wide-range awareness. Future Gener Comput Syst. 2020;109:275–92.
[33] Shi LL, Liu L, Jiang L, Zhu R, Panneerselvam J. QoS prediction for smart service management and recommendation based on the location of mobile users. Neurocomputing. 2022;471:12–20.
[34] Barmpounakis S, Maroulis N, Koursioumpas N, Kousaridas A, Kalamari A, Kontopoulos P, et al. AI-driven, QoS prediction for V2X communications in beyond 5G systems. Comput Netw. 2022;217:109341.
[35] Chen Y, Yu P, Zheng Z, Shen J, Guo M. Modeling feature interactions for context-aware QoS prediction of IoT services. Future Gener Comput Syst. 2022;137:173–85.
[36] Younan M, Houssein EH, Elhoseny M, Ali AA. Challenges and recommended technologies for the industrial internet of things: A comprehensive review. Measurement. 2020;151(7):107–15.
[37] Tangxiao Y, Huafei F, Huifen W, Adjallah KH, Zhouhang W. Data transmission scheme based on publish/subscribe in workshop. 2019 10th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS). Metz, France; 2019. p. 953–8.
[38] Zhang P, Jin H, Dong H, Song W, Wang L. LA-LMRBF: Online and long-term web service QoS forecasting. IEEE Trans Serv Comput. 2019;14(6):1809–23.
[39] Zhou B, Sun B, Gong X, Liu C. Ultra-short-term prediction of wind power based on EMD and DLSTM. 2019 14th IEEE Conference on Industrial Electronics and Applications (ICIEA). Xi'an, China; 2019. p. 1909–13.