electronics

MDPI

Article

SDAE+Bi-LSTM-Based Situation Awareness Algorithm for the CAN Bus of Intelligent Connected Vehicles

Lei Chen *, Mengyao Zheng, Zhaohua Liu, Mingyang Lv, Lv Zhao and Ziyao Wang

School of Information and Electrical Engineering, Hunan University of Science and Technology, Xiangtan 411201, China; 20020401005@mail.hnust.edu.cn (M.Z.); energysmartcontrol@126.com (Z.L.); lvmingyang060607419@126.com (M.L.); zhaolv@hnust.edu.cn (L.Z.); wzy0320@mail.hnust.edu.cn (Z.W.)
* Correspondence: chenlei@hnust.edu.cn

Abstract: With a deep connection to the internet, the controller area network (CAN) bus of intelligent connected vehicles (ICVs) has suffered many network attacks. A deep situation awareness method is urgently needed to judge whether network attacks will occur in the future. However, traditional shallow methods cannot extract deep features from CAN data with noise to accurately detect attacks. To solve these problems, we developed a SDAE+Bi-LSTM based situation awareness algorithm for the CAN bus of ICVs, simply called SDBL. Firstly, the stacked denoising auto-encoder (SDAE) model was used to compress the CAN data with noise and extract the deep spatial features at a certain time, to reduce the impact of noise. Secondly, a bidirectional long short-term memory (Bi-LSTM) model was further built to capture the periodic features from two directions to enhance the accuracy of the future situation prediction. Finally, a threat assessment model was constructed to evaluate the risk level of the CAN bus. Extensive experiments also verified the improved performance of our SDBL algorithm.

Keywords: CAN bus; situation awareness; situation prediction; security assessment; SDAE; Bi-LSTM

Citation: Chen, L.; Zheng, M.; Liu, Z.; Lv, M.; Zhao, L.; Wang, Z. SDAE+Bi-LSTM-Based Situation Awareness Algorithm for the CAN Bus of Intelligent Connected Vehicles. *Electronics* **2022**, *11*, 110. https://doi.org/10.3390/electronics11010110

Academic Editor: Esteban Tlelo-Cuautle

Received: 27 November 2021
Accepted: 26 December 2021
Published: 30 December 2021

1. Introduction

With the development of the Internet of Things and the Industrial Internet, an increasing number of intelligent devices are being assembled into traditional cars to form intelligent connected vehicles (ICVs) [1–3]. Due to this deepening connection with the internet, cyber-attacks can invade the ICVs from the internet. These attacks could seriously affect the normal driving of vehicles, even threatening the safety of drivers. According to statistics from the "*2019 Intelligent Connected Vehicles Information Security Annual Report*", 85% of key vehicle components have security vulnerabilities. In 2020, the number of cyber-attacks on the internet of vehicles reached 2 million, and the trend is showing an exponential increase. For example, the Tesla Model S was easily stolen due to a buffer overflow vulnerability in 2019 [4], BMW suffered an advanced persistent threat (APT) attack in 2019 [5], and Fiat issued a 1.4 million car recall in 2015 [6]. Therefore, it is of great significance to perceive the operating status of the Internet of Vehicles and ICVs to predict security situations and realize early active defense [4].

The concept of situation awareness was first proposed in the military field and has begun to emerge in the field of cyber security. Different from intrusion detection, the purpose of situation awareness is to predict the trend of network development and grasp the future changes of the network based on the network status. Therefore, security situation awareness includes three parts: situation extraction, situation prediction and situation assessment. The research on security situation awareness of ICVs has just started [5–7]. The existing technical methods can be simply divided into the following three categories [8]: statistical model-based, machine learning-based and deep learning-based. **Firstly**, the statistical model-based method usually involves building a mathematical model (immune model,

game model and Markov model) to fit and predict the future state of the network. For example, Meng [9] proposed a hierarchical multi-source network security threat situation assessment model based on dempster shafer (DS) evidence theory. Qiao et al. [10] proposed a network security situation awareness model based on a cooperative artificial immune system. Zhang et al. [11] proposed an approach to improve the awareness of network security, based on the Markov game model (MGM). However, in the real world, the evolution of complex systems is often highly nonlinear and cannot be accurately modeled. **Secondly**, the machine learning-based method usually uses the good adaptability, self-organization and infinite approximation capabilities of machine learning to fit the nonlinearity of network situation evolution, thereby predicting the future trend of network development. For example, Chen et al. [7] further introduced regression prediction into SVM and proposed the RF-SVM model, which can predict potential attacks in future network data streams based on historical data. Zhao et al. [12] combined the support vector machine (SVM) and particle swarm to build a security situation awareness model. However, this type of method cannot accurately extract the deep features of historical data and cannot predict the periodic network situation changes well. **Thirdly**, deep learning-based methods are currently a hot topic in research, and have achieved good results in security situation awareness research [12–19]. For example, Kang et al. [15] combined a stacked auto-encoder (SAE) with long short-term memory (LSTM) to build a deep situation awareness model to capture the time series features of network attack data and complete accurate network situation prediction. Based on historical data, Hu et al. [16] used a recurrent neural network (RNN) as the situation predictor to obtain the future network situation based on the periodic features of the historical data.

In summary, the security situation awareness methods of ICVs are gradually changing from shallow statistical models [20–24] to deep data-driven models. However, the existing data-driven models have the following shortcomings: (1) while noise and interference are inevitable for any dynamic system [25,26], the noise in the data is not considered in these models, which affects their accuracy; (2) the extraction of the time period feature in only a single direction (from the past to the future) results in inaccurate and incomplete feature extraction; and (3) most of these models only consider the time period features of the data, without considering the changes in spatial features.

To solve the above problems, we attempted to fuse multiple deep neural networks to extract temporal and spatial features at the same time from the controller area network (CAN) bus data with noise, in order to obtain a more accurate and robust situation awareness of the CAN bus. Therefore, a security situation awareness algorithm based on stacked denoising auto-encoder (SDAE) and bidirectional long short-term memory (Bi-LSTM) was developed for the CAN bus of ICVs. The main contributions of this paper are as follows:

- SDAE was used to extract the deep spatial features from the CAN data with noise at a certain moment, so as to eliminate the influence of noise and realize the situation extraction;
- Bi-LSTM was used to predict the future situation from two directions, so as to enhance the accuracy and robustness of situation prediction;
- A security assessment model was built to evaluate the predicted situation, and finally determine the risk level of the current CAN bus.

The remaining parts of this paper are organized as follows. The proposed SDBL situation awareness model is given in Section 2. The experiments are presented in Section 3. Finally, a brief conclusion is presented in Section 4.

2. SDAE+Bi-LSTM-Based Security Situation Awareness Algorithm for the CAN Bus of Intelligent Connected Vehicles

2.1. SDAE+Bi-LSTM-Based Situation Awareness Model

In this paper, a security situation awareness model is proposed based on the stacked denoising auto-encoder (SDAE) and bidirectional long short-term memory (Bi-LSTM), as shown in Figure 1. By fusing the domain data and expert knowledge, the proposed model

has better accuracy and intelligence. It can realize the efficient integration of situation extraction, situation prediction and situation assessment. The situation awareness processes of this model are divided into three stages: (1) Stage 1 is situation extraction, where the denoising auto-encoder (DAE) is used to extract the shallow linear features from the CAN data with noise, and SDAE is further used to transform the shallow linear features into deep features. (2) Stage 2 is situation prediction, where LSTM is used to obtain the time period feature from m local spatial features extracted by SDAE, and Bi-LSTM is further used to enhance the accuracy of future situation prediction of the CAN bus from two different directions. (3) Stage 3 is situation assessment, where domain expert knowledge is used to construct a threat assessment model to estimate the future risk level of the CAN bus based on the predicted situation by Bi-LSTM.

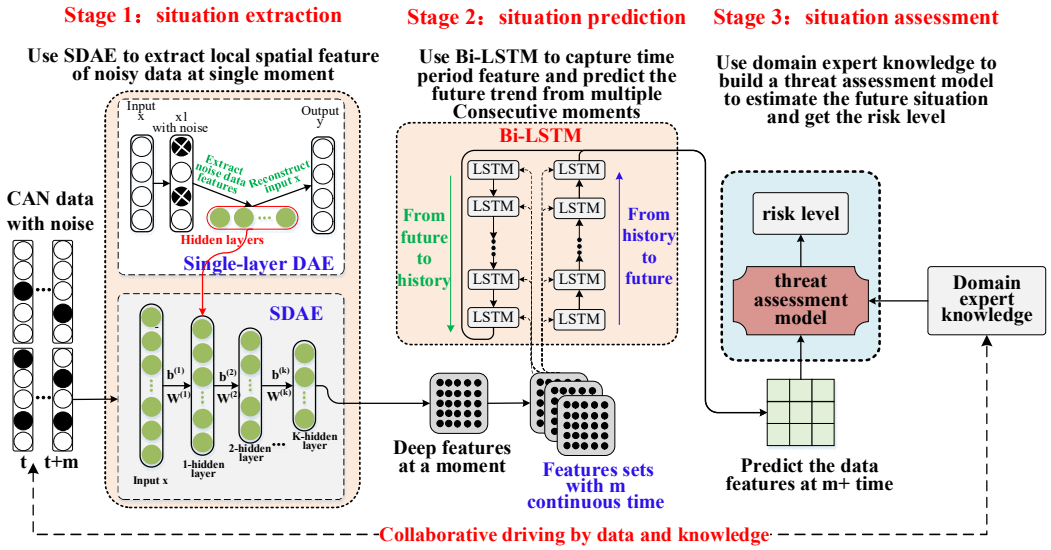

Figure 1. SDAE+Bi-LSTM-based security situation awareness model for CANbus.

2.2. Using SDAE to Extract Deep Spatial Features

The stacked auto-encoder (SAE) is a common feature extractor that can extract the deep features of data. However, with the improvement of the intelligence degree of vehicle equipment, the form of CAN bus data becomes complicated and accompanied by a large amount of noise. This noise makes it impossible for the SAE to obtain low-dimensional features of the CAN data and affects the accuracy of feature extraction and situation awareness.

To solve the above problems, the DAE can be used to extract linear features from the CAN data with noise and the multiple linear features can be further transformed by the SDAE. The SDAE is composed of a stacking multi-layer DAE, which can extract nonlinear deep features, eliminate the influence of noise in CAN data, and then achieve the purpose of improving the accuracy and robustness of situation awareness.

2.2.1. Using DAE to Eliminate Noise Influence

The DAE was used in this paper to reduce the impact of noise in feature extraction. The core idea of DAE is to forcibly add some noise to the input data, carry out feature extraction on this data with noise. And then reconstruct the input data based on the extracted features, so as to reduce the influence caused by the noise. The DAE has the following three main processes:

(1) Degradation processing. Provide the input data X (x_1, x_2, . . . , x_n), define the degradation function to forcibly add the noise to the input data, and obtain the damaged data X' (x'_1, x'_2, . . . , x'_n). The formula is as follows:

$$X' = \varphi(X, \sigma) \quad (1)$$

where σ is the denoising coefficient and φ represents the probability that the input node is zeroed.

(2) Encode and Decode processing. Take the degraded data X' ($x'_1, x'_2, \ldots, x'_n$) as the new input, define the encoder weight W_1 and bias b_1 and the decoder weight W_2 and bias b_2. After calculation, the data features H ($h_1, h_2, \ldots, h_n$) are captured by the hidden layer and the reconstruction data $\hat{X}(\hat{x}_1, \hat{x}_2, \cdots, \hat{x}_n)$ of the output layer are:

$$H = W_1^T X' + b_1 \tag{2}$$

$$\hat{X} = W_2^T H + b_2 \tag{3}$$

(3) Optimization processing. The optimization function of the DAE acts to minimize the loss between all reconstruction data $\hat{x}$ and the original input data x, which is defined as follows:

$$J(w, b) = \frac{1}{m}\sum_{i=1}^{m}\left(\frac{1}{2}\|\hat{x}_i - x_i\|^2\right) \tag{4}$$

2.2.2. Using SDAE to Extract the Deep Spatial Features

The learning ability of single-layer DAE is limited because it can only learn the shallow linear features of CAN data. For this reason, multiple layers of DAE are stacked to form the SDAE to obtain the deep features of CAN data by transforming multiple shallow linear features, as shown in Figure 2.

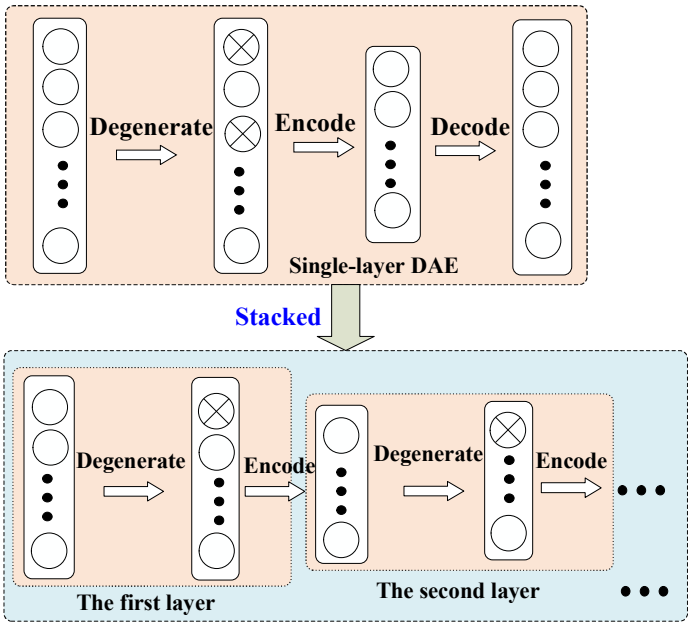

Figure 2. The structure of SDAE.

It should be noted that the number of layers should not be too few to extract deep features. Similarly, too many layers will cause gradient dispersion and lead to model overfitting.

2.3. Using Bi-LSTM to Realize Situation Prediction

A normal control command or network attack in an ICV usually goes through multiple moments from its start to end. Each moment presents different local spatial features, and local features of multiple moments are related to each other to form the overall features. Due to the fact that vehicle CAN data are usually periodic, the possible running state at the next moment can be predicted by the state at previous multiple consecutive moments.

In this paper, the spatial features of m continuous moments extracted by the SDAE were used as input to construct a Bi-LSTM model to extract periodic features from two directions. Through Bi-LSTM, the time periodic features of the CAN data are accurately extracted to predict the future features at m+1 and realize situation prediction.

2.3.1. Using LSTM to Predict Future Features

Taking the m continuous time spatial features extracted by SDAE as input, m LSTM units are used to simulate the information transfer and evolution process between the m continuous time of the CAN data to predict the future state at the m + 1 time. The long-term memory state C_t and short-term memory state h_t are retained and updated through the forget gate, input gate and output gate.

In the LSTM unit, the forget gate decides to selectively forget or discard some information from the previous C_{t-1}. The input gate selects memory from the current information to update the C_t. The output gate selects output from the current information to update the h_t.

Connecting m LSTM units in series, a C_t is used to capture the common features of m moments, and the h_t of each moment represents the importance of a single moment in the entire long-term memory. The features at m consecutive moments are used to predict the future features at the m + 1 moment.

To ensure the accuracy of the predicted features at time m + 1, Softmax was used as the classifier and cross-entropy as the optimization function to minimize the difference between the real label and the predicted label at time m + 1. The formula is as follows:

$$CE - Loss = -(y_i \log(\hat{y}_i) + (1 - y_i) \log(1 - \hat{y}_i)) \quad (5)$$

where y_i is the real label at one time and $\hat{y}_i$ is the predicted label from Softmax.

2.3.2. Using Bi-LSTM to Enhance Situation Prediction Accuracy

The m local spatial features of m consecutive moments are randomly selected, and this random order is not suitable for the fixed sequence order of the hidden periodic features of CAN data. This means that, based on the spatial features of the m consecutive moments chosen randomly, the LSTM model cannot accurately extract the periodic features of the CAN data. To improve this problem, a Bi-LSTM model was constructed to take the m continuous time data as input, and to extract the periodic features of the CAN data from two directions, as shown in Figure 3.

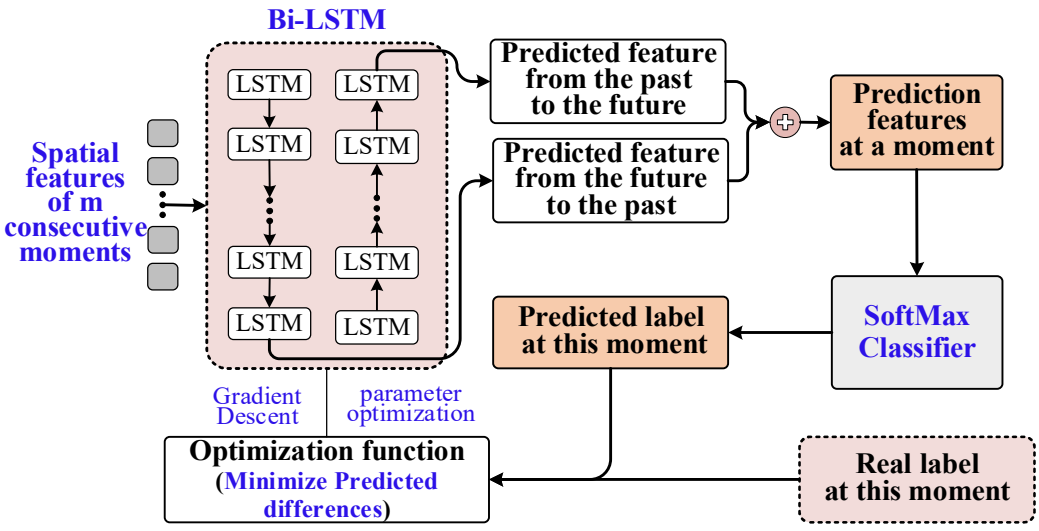

Figure 3. Bi-LSTM update process.

The update process of the Bi-LSTM model is as follows. (1) The spatial features of m consecutive moments extracted by the SDAE are used as input. (2) One predicted feature is generated by the Bi-LSTM in the direction from the past to the future, and another predicted feature is generated in the direction from the future to the past. (3) Two predicted features are combined as the final prediction feature at a moment. (4) Based on the final prediction feature, a SoftMax is used to obtain the predicted label. (5) The predicted label and the real label are added to the optimization function, and the model parameters are updated through stochastic gradient descent (SGD). Through repeated optimization and updates, the Bi-LSTM model is officially used to predict the future situation of the CAN bus.

2.4. SDAE+Bi-LSTM-Based Situation Awareness Model

After feature extraction and situation prediction, we can obtain a predicted future state of the CAN bus from the previous m consecutive moments. However, the security level of the CAN bus is still unknown. Therefore, a risk evaluation method or model is needed to make a risk assessment for the future state of the CAN bus. In this paper, by jointly considering the historical data and domain expert knowledge, a risk assessment model was constructed to cooperate with SDAE and Bi-LSTM models to achieve the final security risk assessment of the CAN bus, as shown in Figure 4.

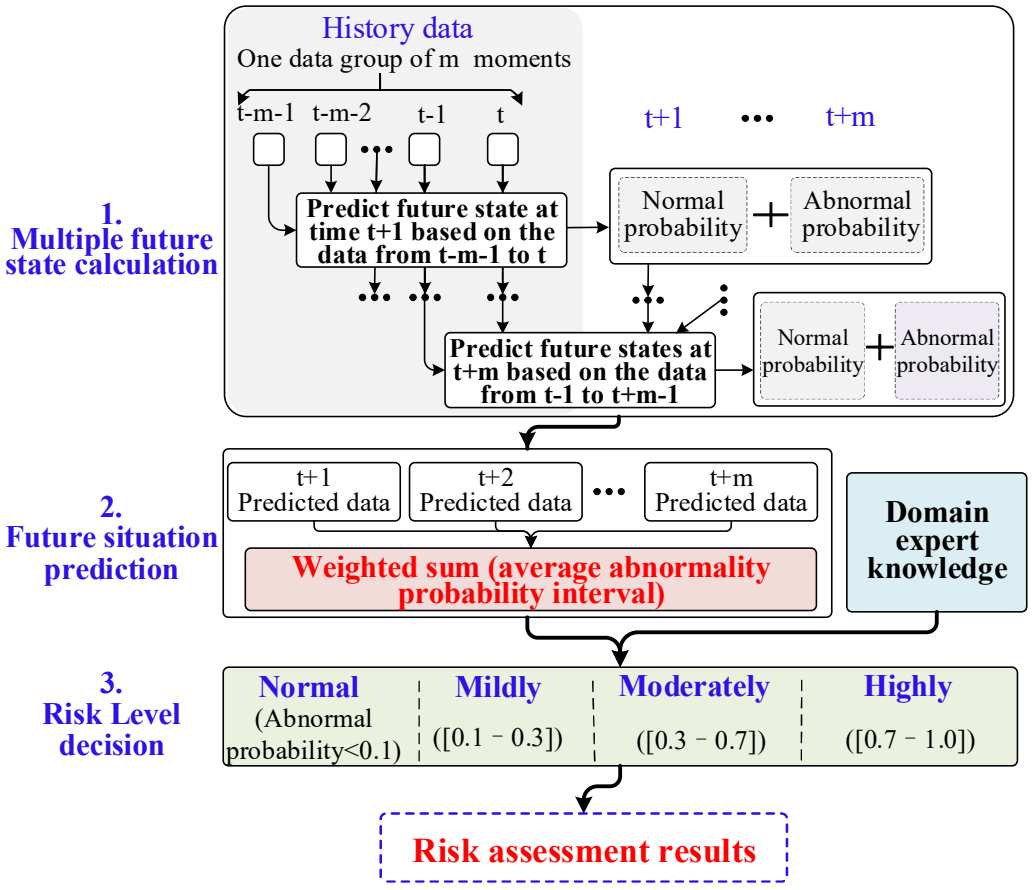

Figure 4. Risk assessment process.

The detailed process of this risk assessment model for CAN bus security situation awareness is as follows:

- **Multiple future state calculation**: Firstly, the stable SDAE+Bi-LSTM model is used to predict the future state at t + 1 from m previous states between t − m − 1 and t. Secondly, the model is used again to predict the future state at t + 2 from the t − m − 2 to t + 1. Then, repeat the above process until the future states from t + 1 to t + m are

predicted. Finally, SoftMax is used to classify the predicted data at each moment and obtain the rate that it is normal data and abnormal data.

- **Future situation prediction**: According to the abnormal probability of the predicted future states from t + 1 and t + m, the weighted sum is carried out to obtain the abnormal average probability of the future situation in the range of m moments. This abnormal average probability is regarded as the future situation of the CAN bus.
- **Risk level decision**: A risk assessment model is built by using domain expert knowledge. Based on the abnormal average probability of future state within a period of time, this model is used to perform hierarchical evaluation, and to obtain the risk level of the future situation of the CAN bus.

2.5. SDAE+Bi-LSTM (SDBL) Algorithm

Summarizing Sections 2.2–2.4, a SDAE+Bi-LSTM based security situation awareness algorithm, called SDBL, was proposed in this paper for the CAN bus of ICVs. The SDBL algorithm contains two aspects: model building and situation awareness. In which, the model building is responsible for optimizing and training the parameters of the SDAE+Bi-LSTM from the labelled historical data, and the situation awareness is responsible for using the stable SDAE+Bi-LSTM model to predict the future security situation of the CAN bus from newly arrived data. The detailed process of the SDBL algorithm has the following four steps, as shown in Figure 5.

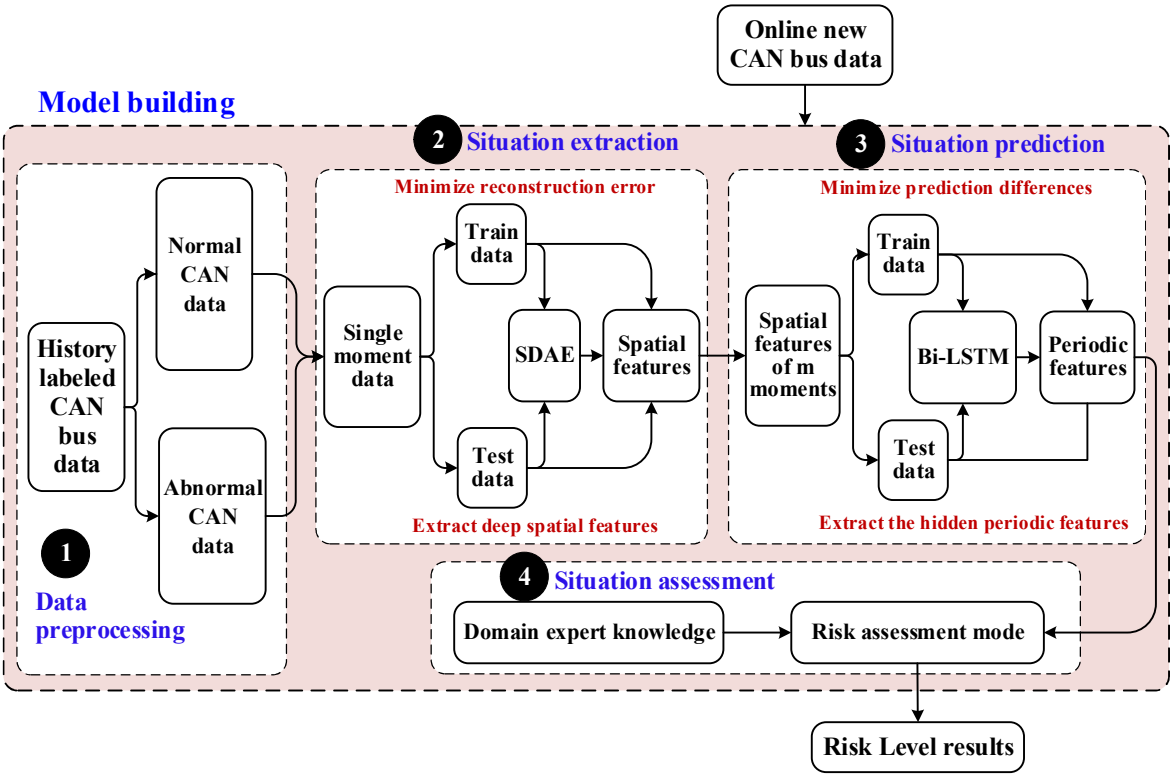

Figure 5. SDAE+Bi-LSTM (SDBL) algorithm.

Step 1, data pre-processing: The historical data is appropriately divided into the labeled abnormal CAN data and normal CAN data. Moreover, regularization and entity alignment are executed on these two types of data.

Step 2, situation extraction: Taking labeled data at a single moment as input, a multiple single-layer DAE is stacked to form the SDAE model. Firstly, an input x is degraded to the new input x_1 by adding some noise. Secondly, the multiple-layer SDAE is used to extract the deep spatial features of x_1, and to generate the reconstruction input y.

Then, mean square loss and SGD are used to update and optimize the model parameters. Finally, the stable SDAE model can extract the deep spatial features of CAN data.

Step 3, situation prediction: Firstly, the Bi-LSTM model is constructed to extract the periodic features from the spatial features of m consecutive moments in the two different directions. Secondly, Softmax is used to classify the predicted periodic feature and obtain the predicted label. Then, cross entropy and SGD are used to update and optimize the model. Finally, the stable Bi-LSTM can predict the future features and security situation based on the previous m moments.

Step 4, situation assessment: Firstly, the stable SDAE+Bi-LSTM is used to predict the future state at t + 1 from t + m − 1 to t, followed by time t + 2, until time t + m − 1. The future states from t + 1 to t + m − 1 compose the future situation set of the CAN bus. Secondly, SoftMax is used to obtain the abnormal probability of the future state at t + 1, followed by t + 2, until t + m − 1. The abnormal probability of the future states from t + 1 to t + m − 1 composes the risk set of the CAN bus. Thirdly, the average of all the abnormal probabilities in the risk set is taken as the risk of the future situation of the CAN bus. Finally, the domain expert knowledge is used to build the risk level assessment model to obtain the risk level of the future situation of the CAN bus.

3. Experiments and Results

3.1. Experiment Preparation

Datasets: In this paper, two Internet of Vehicles datasets were chosen as experimental datasets. The first is the CAR-HACKING dataset, which is a public dataset (https://ocslab.hksecurity.net/Datasets/CAN-intrusion-dataset; accessed on 5 March 2021) that includes 175,302 normal messages and 37,604 abnormal messages. The period of data collected was two weeks, with one CAN message collected every minute. Each piece of data consists of an 8-byte message data segment, a 2-byte arbitration segment message ID and a category label. In this dataset, the types of attacks include denial of service (DoS) attack, fuzzy attack, spoofing the drive gear and spoofing the revolutions per minute (RPM) gauge. In this paper, 60,000 samples were randomly selected as experimental data, including 50,000 training samples and 10,000 test samples. Each sample contained 100 continuous CAN messages where 80 continuous messages were taken to predict the next 20 messages. In all samples, the number of samples with abnormal messages was 70%. The other dataset is the Volvo CAN bus dataset that we collected ourselves; we sent abnormal CAN messages to the vehicle through CANTest (a software for CAN bus data receiving and sending) that contained 65,535 normal messages and 9000 abnormal messages. The period of data collection was one week and one CAN message was collected every 30 s. Each piece of data consists of an 8-byte message data segment, a 4-byte arbitration segment message ID and a category label. In this dataset, the only type of attack was a DoS attack. In this paper, 40,000 samples were randomly selected as experimental data, including 28,000 training samples and 12,000 test samples. Each sample contained 150 continuous CAN messages where 120 continuous messages were taken to predict the next 30 messages. In all samples, the number of samples with abnormal messages was 60%. In two datasets, the data fields of timestamp, CAN ID, data length code, DATA [0–7] and label (normal or abnormal) were selected as the inputs. In the training phase, 100 samples from each of the of two datasets were used as a batch to perform one iteration.

Experimental platform: All experiments were completed on a normal PC, and the hardware information is as follows: an Intel(R) i7-9750H CPU (2.3 GHz), NVIDIA GeForce GTX 1050Ti graphics card, 8 G memory and a Win10 (64-bit) operating system. All experiment codes were based on MATLAB2020a as the programming environment.

Comparison models: To effectively verify the performance of our SDBL model, three models (SDAE, SAE and principal component analysis (PCA)) were chosen as feature extractors, four models (Bi-LSTM, gated recurrent unit (GRU), LSTM and RNN) were chosen as the situation predictors, and four situation awareness algorithms (LSTM+SAE, GRU+SAE, RNN+PCA and GRU+NONE) were chosen as the comparison algorithms.

Evaluation metrics: In this paper, we chose the accuracy (ACC), false negative rate (FNR) and false positive rate (FPR) as evaluation indexes, defined as follows:

$$\mathrm{ACC} = \frac{\mathrm{TP} + \mathrm{TN}}{\mathrm{TP} + \mathrm{FN} + \mathrm{FP} + \mathrm{TN}} \times 100\% \tag{6}$$

$$\mathrm{FPR} = \frac{\mathrm{FP}}{\mathrm{FP} + \mathrm{TN}} \times 100\% \tag{7}$$

$$\mathrm{FNR} = \frac{\mathrm{FN}}{\mathrm{TP} + \mathrm{FN}} \times 100\% \tag{8}$$

where true positive (TP) is a positive sample predicted to be positive, true negative (TN) is a negative sample predicted to be negative, false positive (FP) is a negative sample predicted to be positive and false negative (FN) is a positive sample predicted to be negative.

3.2. Sensitivity Analysis

The first experimental objective was to test the sensitivity of multiple parameters in our SBDL algorithm from the ACC, FPR and FNR.

3.2.1. Sensitivity of Network Structure

In our SBDL algorithm, the SDAE needs to stack multiple layers, each layer needs to set a different number of nodes and Bi-LSTM needs m LSTM units. To obtain a stable interval of the network structure, the node number at each layer, stacked layers of SDAE and the number of LSTM units m form a triple <number of nodes, number of layers, m>. ACC, FPR, FNR and training time were used to test their sensitivity on two datasets.

Table 1 lists the results from the Volvo CAN bus dataset. From the table, three patterns can be found: (1) When only considering the number of stacked layers in the SDAE, the ACC first rises and then falls as the number of stacked layers increases. When the number of stacked layers is three, the SDAE shows the best performance in ACC. (2) When the number of nodes in two adjacent layers differs greatly, the three metrics (ACC, FNR, FPR) of SDAE perform poorly. (3) When only considering the parameterm, the ACC is gradually improved with the increase of m.

Table 1. Performance of SDBL model with different structures.

SDBL <Nodes, Layers, m>	ACC	FPR	FNR	Time/s
[<9-8>,1,3]	0.9321	0.1249	0.1436	381
[<9-5>,1,6]	0.9249	0.0616	0.0857	476
[<9-8>,2,3]	0.9491	0.1035	0.1134	469
[<9-5>,2,9]	0.9358	0.0611	0.0591	552
[<9-8>,3,6]	0.9629	0.0691	0.0518	618
[<9-5>,3,9]	0.9727	0.0584	0.0479	742
[<9-8>,4,3]	0.9509	0.0925	0.1053	867
[<9-5>,4,9]	0.9467	0.0679	0.0761	1098
[<9-8>,5,6]	0.9252	0.1972	0.1024	1345
[<9-5>,5,9]	0.9294	0.0711	0.1176	1448

From the experimental results of the two datasets, it can clearly be seen that three is a good number of stacked layers in the SDAE. The number of nodes in two adjacent layers are not too different, and the stability interval of m is [5–10].

3.2.2. Sensitivity of Denoising Coefficient

The second sensitivity parameter, the denoising coefficient σ, represents how much noise is added to each DAE input layer in SDAE. The larger σ is, the more noise is added to the input and the stronger the ability to eliminate noise in the SBDL model. In this

experiment, we used ACC and FNR as evaluation metrics to observe the trend of the SDBL algorithm affected by σ on the two datasets, are shown in Figure 6.

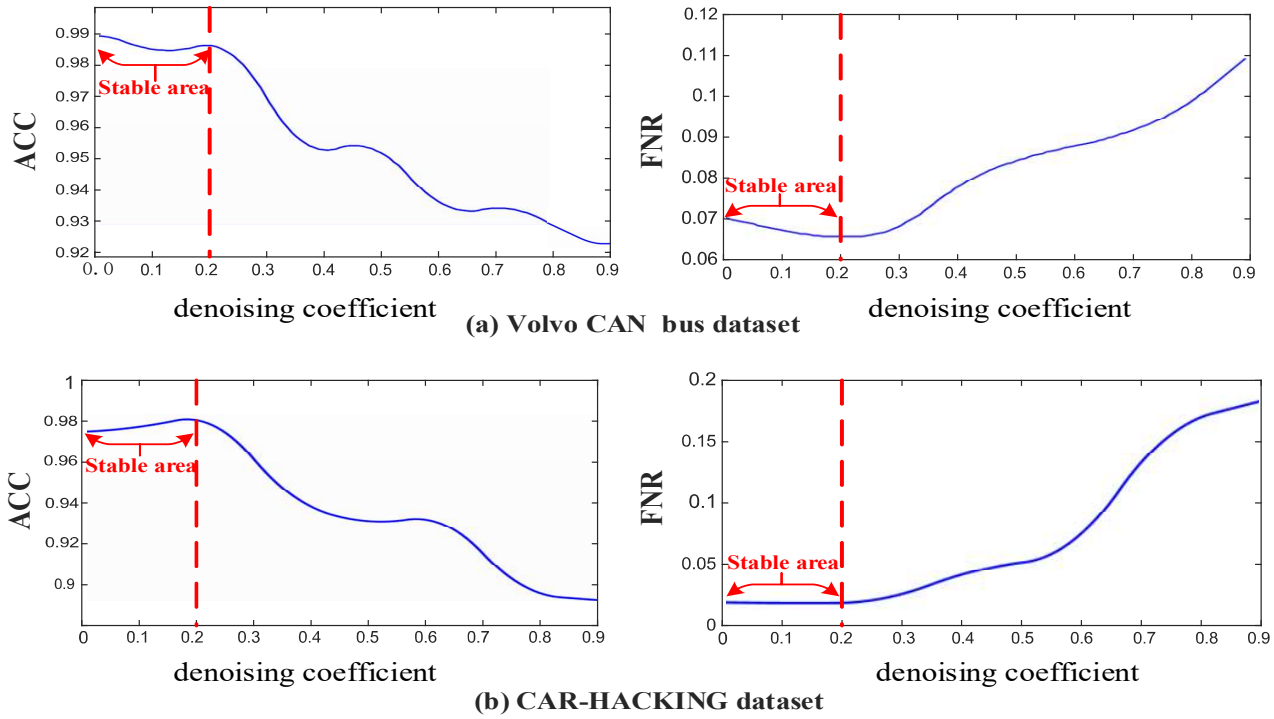

Figure 6. Sensitivity analysis of denoising coefficient σ on two datasets. (**a**) the trend of the SDBL algorithm affected by σ on Volvo CAN bus dataset; (**b**) the trend of the SDBL algorithm affected by σ on CAR–HACKING dataset.

We can note the following observations from Figure 6: (1) For the Volvo CAN bus dataset, with the increase of σ, the ACC showed a downward trend, and the FNR showed an upward trend. However, when σ was in the range of [0.2–0.7], the curves of the ACC and FNR were very unstable. (2) For the CAR-HACKING dataset, when σ was less than 0.2, the performance of the ACC and FNR was stable. When σ was greater than 0.2, the ACC curve gradually decreased and the FNR curve gradually increased. (3) In general, when σ was between 0.05 and 0.2, the robustness of our SBDL model was improved.

3.3. Analysis of Results

The second experimental objective was to verify the performance of the SDAE feature extractor awareness, Bi-LSTM situation predictor and SDBL situation awareness algorithm on two datasets.

3.3.1. Performance Analysis of the SDAE Feature Extractor

Taking ACC, FNR and FPR as the evaluation metrics, SDAE, SAE, PCA and NONE were chosen as feature extractors to compare the performance of deep feature extraction, as shown in Figure 7. From the figure, we can note the following observations. (1) For the Volvo CAN bus dataset, the four feature extractors performed well in ACC, FNR and FPR. The ACC value was between 0.92 and 1, the value of FPR and FNR were both less than 0.14. When a situation predictor was fixed, the four feature extractors had different performances. For example, under the GRU, SDAE was the best, SAE was the second best and PCA was the worst. Under RNN, SAE was the best, SDAE was the second best and NONE was fourth. Combined with the four situation predictors, the SDAE had the most stable performance. (2) For the CAR-HACKING dataset, the performance of the four feature extractors was similar to the Volvo CAN bus dataset, and the SDAE had the better

performance and stability of ACC, FNR and FRP. (3) In general, the deep features of CAN data can be better extracted by the SDAE.

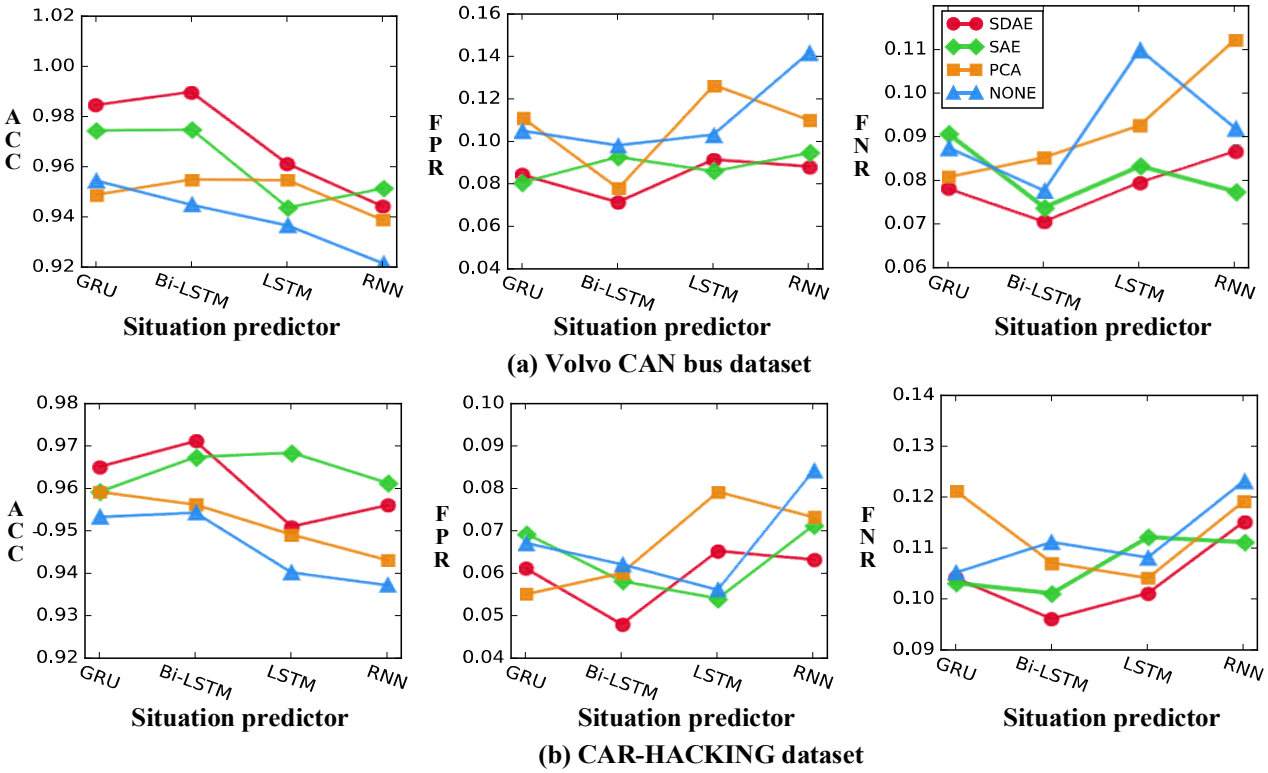

Figure 7. Performance analysis of SDAE on two datasets. (**a**) the performance comparison of four features extractors on Volvo CAN bus dataset; (**b**) the performance comparison of four features extractors on CAR-HACKING dataset.

3.3.2. Performance Analysis of Bi-LSTM Situation Predictor

In this section, the Bi-LSTM, GRU, LSTM and RNN were chosen as the situation predictor to further compare the performance of future situation prediction. Figure 8 gives the comparison results of the four predictors on the two datasets. In the figure, two observations can be obtained. **(1) For the Volvo CAN bus dataset**, the four situation predictors showed excellent performance; the ACCs were greater than 0.91, the FNRs were less than 0.14, and the FPRs were less than 0.11. However, under different feature extractors, the four situation predictors were unstable. For example, the GRU had the best ACC under NONE, the Bi-LSTM had the best ACC under SDAE and the Bi-LSTM had the best FPR under NONE, PCA and SDAE. In terms of the FNR, Bi-LSTM had a better rate than the other three situation predictors. **(2) For the CAR-HACKING dataset**, the performance curves of the four situation predictors fluctuated greatly with the different feature extractors. Compared with the other three predictors, Bi-LSTM had the best performance and stability.

3.3.3. Performance Analysis of SDBL Algorithm

The last experiment divided the test dates of the two datasets into five different groups, and selected four algorithms as the comparison algorithms to verify the performance of our SDBL algorithm. Figure 9 plots the performance of five algorithms on two datasets. (1) Considering ACC, FNR and FPR together, the five algorithms achieved excellent results. However, the five algorithms showed unstable trends and fluctuations in a small range. (2) In terms of the FPR, our SDBL algorithm had the best and most stable performance, followed by GRU-SAE, while the worst was RNN-PCA. (3) In terms of the FNR, the five algorithms had the smallest performance difference on the two datasets. Contrasting the

five algorithms, SDBL and GRU-SAE had the best stability. (4) In summary, the improved performance of our SDBL algorithm was clearly shown.

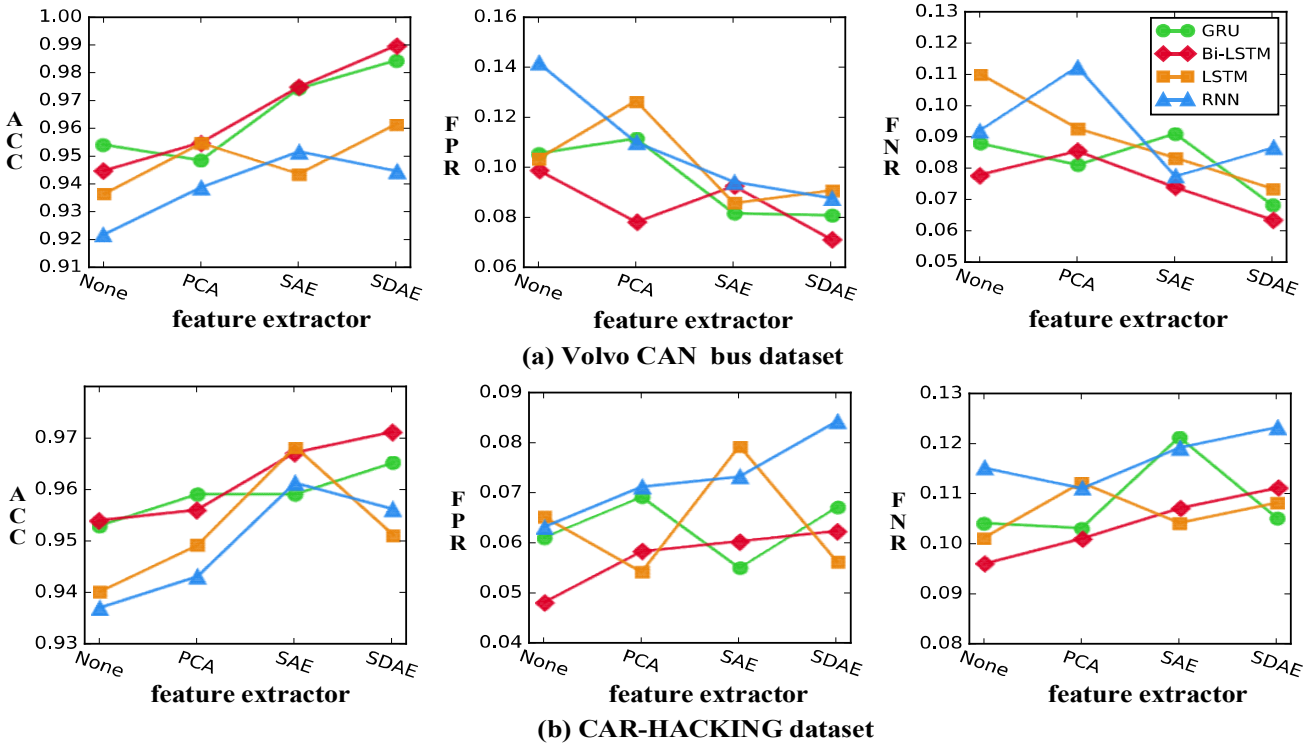

Figure 8. Performance analysis of Bi-LSTM situation predictor. (**a**) the comparison results of the four predictors on Volvo CAN bus dataset; (**b**) the comparison results of the four predictors on CAR-HACKING dataset.

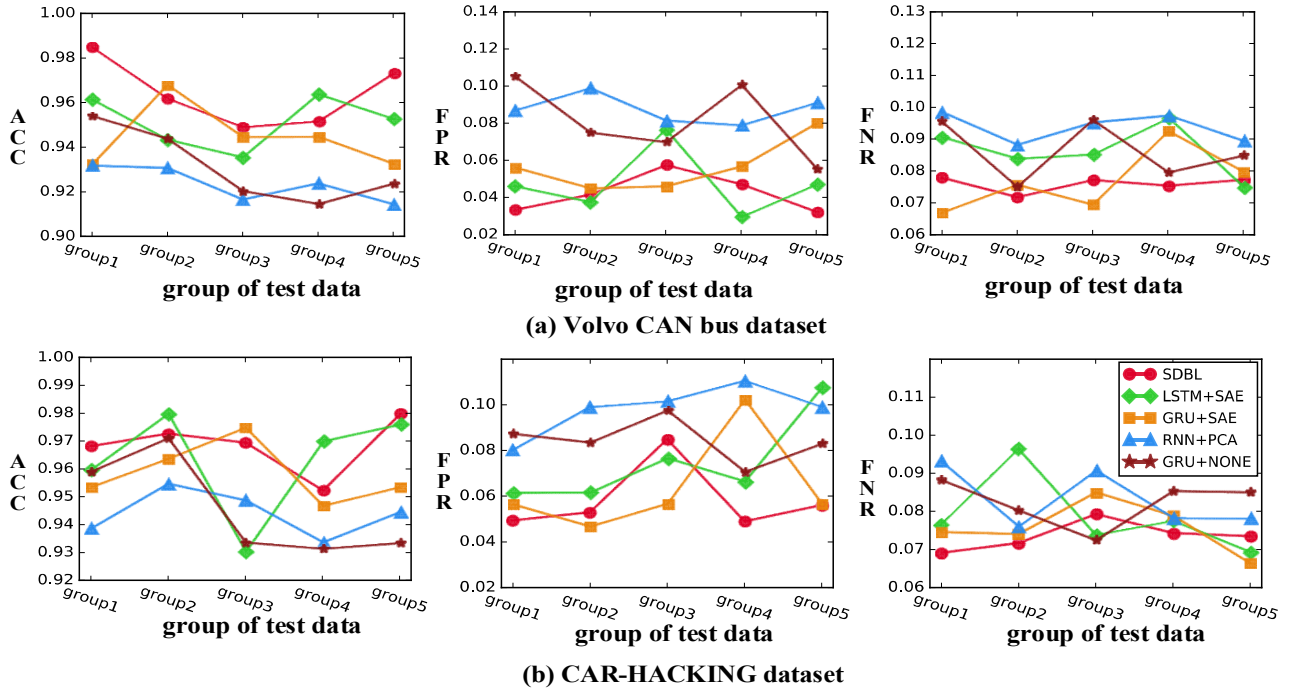

Figure 9. Performance analysis of five algorithms. (**a**) the performance comparison of five algorithms on Volvo CAN bus dataset; (**b**) the performance comparison of five algorithms CAR-HACKING dataset.

4. Conclusions

Driven by data and domain expert knowledge, this paper proposed a SDAE+Bi-LSTM based security situation awareness algorithm, called SDBL, for the CAN bus of ICVs. The main contributions of this work are as follows. Firstly, the SDAE was constructed as the situation extraction model to extract the deep spatial features from single moment CAN data with noise. Secondly, Bi-LSTM was used to capture the periodic features from multiple spatial features of m consecutive moments from two different directions to enhance the future prediction situation accuracy. Finally, a risk assessment model was constructed to obtain the risk level of the future situation of the CAN bus based on multiple predicted future states. Experiments using the Volvo CAN bus and CAR-HACKING datasets proved the performance of our SDBL algorithm. In future work, we will consider designing a lightweight situation awareness model that is suitable for embedded devices under the Internet of Vehicles, while also trying to replace LSTM with GRU to reduce the training of parameters and improve training efficiency.

Author Contributions: Conceptualization, L.C., M.Z., Z.L. and M.L.; methodology, M.L. and L.Z.; validation, M.Z., L.Z. and Z.W.; formal analysis, L.C.; investigation, M.Z. and Z.W.; resources, Z.L.; data curation, M.L.; writing—original draft preparation, L.C.; writing—review and editing, M.Z. and M.L.; visualization, Z.L., L.Z. and Z.W.; supervision, L.C. and Z.L. All authors have read and agreed to the published version of the manuscript.

Funding: This work was funded by the National Natural Science Foundation of China (No.62103143); the Hunan Provincial Natural Science Foundation of China (No.2020JJ5199); the Open Project of Key Laboratory of Intelligent Computing and Information Processing of Ministry of Education, Xiangtan University (2020ICIP06); and the Scientific Research Fund of Hunan Provincial Education Department (Grant No.20B216, No.20C0786).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The CAR-HACKING dataset is a public dataset, it can be attained at https://ocslab.hksecurity.net/Datasets/CAN-intrusion-dataset, accessed on 5 March 2021. The Volvo dataset is available on request from the corresponding author.

Acknowledgments: We would like to acknowledge the support by the New Energy Technology and Intelligent System Laboratory of the School of Information and Electrical Engineering of Hunan University of Science and Technology.

Conflicts of Interest: The authors declare conflict of interest.

References

1. Yang, F.C.; Wang, S.G.; Li, J.L.; Liu, Z.H.; Sun, Q.B. An Overview of Internet of Vehicles. *Chin. Commun.* **2014**, *11*, 1–15. [CrossRef]
2. Algarni, A.; Thayananthan, V. Improvement of 5G Transportation Services with SDN-Based Security Solutions and beyond 5G. *Electronics* **2021**, *10*, 2490. [CrossRef]
3. Pascale, F.; Adinolfi, E.A.; Coppola, S.; Santonicola, E. Cybersecurity in Automotive: An Intrusion Detection System in Connected Vehicles. *Electronics* **2021**, *10*, 1765. [CrossRef]
4. Wu, W.F.; Li, R.F.; Zeng, G.; Xie, Y.; Xie, G.Q. Survey of the Intelligent and Connected Vehicle Cyber Security. *J. Commun.* **2020**, *41*, 161–174.
5. Li, Y.; Wang, C.Z.; Huang, G.Q.; Zhao, X.; Zhang, B.; Li, Y.C. A Survey of Architecture and Implementation Method on Cyber Security Situation Awareness Analysis. *Acta Electron. Sin.* **2019**, *47*, 927–945.
6. Gong, J.; Zang, X.D.; Su, Q.; Hu, X.Y.; Xu, J. Survey of Network Security Situation Awareness. *J. Softw.* **2017**, *28*, 1010–1026.
7. Chen, G. RF-SVM based awareness algorithm in intelligent network security situation awareness system. Proceedings of 2017 3rd Workshop on Advanced Research and Technology in Industry Applications. *Inst. Manag. Sci. Ind. Eng.* **2017**, *5*. [CrossRef]
8. Shi, L.Y.; Liu, J.; Liu, Y.H.; Duan, P.F. Survey of research on network security situation awareness. *Comput. Eng. Appl.* **2019**, *55*, 1–9.
9. Meng, J. *Research on Key Techniques in Network Security Situation Assessment and Prediction*; Nanjing University of Scence&Technology: Nanjing, China, 2012.

10. Qiao, Y.; Xu, J. A network security situation awareness model based on cooperation artificial immune system. In Proceedings of the 2011 International Conference on Computer Science and Service System (CSSS), Nanjing, China, 27–29 June 2011; pp. 1945–1947.
11. Zhang, Y.; Tan, X.B.; Cui, X.L.; Xi, H.S. Network Security Situation Awareness Approach Based on the Markov Game Model. *J. Softw.* **2011**, *22*, 495–508. [CrossRef]
12. Zhao, D.M.; Liu, J. Study on Network Security Situation Awareness Based on Particle Swarm Optimization Algorithm. *Comput. Ind. Eng.* **2018**, *125*, 764–775. [CrossRef]
13. Jin, L.; Li, S.; Hu, B.; Liu, M. A survey on projection neural networks and their applications. *Appl. Soft Comput.* **2019**, *76*, 533–544. [CrossRef]
14. Xie, X.Y.; Zhou, J.H.; Zhang, Y.J. Application and challenge of deep learning in Ubiquitous Power Internet of Things. *Electr. Power Autom. Equip.* **2020**, *40*, 77–87.
15. Kang, S.Q.; Zhou, Y.; Wang, Y.J.; Xie, J.B.; Mikulovich, V.I. RUL Prediction Method of a Rolling Bearing Based on Improved SAE and Bi-LSTM. *Acta Automat. Sin.* **2020**. [CrossRef]
16. Hu, X. Prediction of Network Security Situation Based on RNN. *Mod. Comput.* **2017**, *2*, 14–16.
17. Wu, X.X.; He, Y.G.; Duan, J.J.; Zhang, H.; Zeng, Z.R. Bi-LSTM-based transformer fault diagnosis method based on DGA considering complex correlation characteristics of time sequence. *Electr. Power Autom. Equip.* **2020**, *40*, 184–193.
18. Yan, J.K.; Jin, L.; Yuan, Z.T.; Liu, Z.Y. RNN for Receding Horizon Control of Redundant Robot Manipulators. *IEEE Trans. Ind. Electron.* **2021**, *69*, 1608–1619. [CrossRef]
19. Jin, L.; Li, S.; Yu, J.G.; He, J.B. Robot manipulator control using neural networks: A survey. *Neurocomputing* **2018**, *285*, 23–34. [CrossRef]
20. Eiza, M.H.; Owens, T.; Ni, Q. Situation-Aware QoS Routing Algorithm for Vehicular Ad Hoc Networks. *IEEE Trans. Veh. Technol.* **2015**, *64*, 5520–5535. [CrossRef]
21. Meng, R.; Pei, X.B. Research and Design of Network Situation Awareness System Based on Big Data. *J. Phys. Conf. Ser.* **2020**, *1550*, 032118. [CrossRef]
22. Zhang, Z.J.; Zhang, Y.; Wang, J. An Anomaly Detection System Applied to CAN bus. *Inf. Secur. Commun. Priv.* **2015**, *8*, 92–96.
23. Feng, Z.J.; He, M.; Li, B.; Deng, M. Research on Car Information Security Attack and Protection Technology. *J. Cyber Secur.* **2017**, *2*, 1–14.
24. Yu, H. Research on Connected Vehicle Cyber Security and Anomaly Detection Technology for In-vehicle CAN Bus. Ph.D. Thesis, Jilin University, Jilin, China, 2016.
25. Jin, J. A robust zeroing neural network for solving dynamic nonlinear equations and its application to kinematic control of mobile manipulator. *Complex Intell. Syst* **2021**, *7*, 87–99. [CrossRef]
26. Ying, L.F.; Jin, L.; Xu, J.Q.; Xiao, X.C.; Fu, D.Y. Reformative Noise-Immune Neural Network for Equality-Constrained Optimization Applied to Image Target Detection. *IEEE Trans. Emerg. Top. Comput.* **2021**. [CrossRef]