Research of CAN Bus Information Anomaly Detection Based on Convolutional Neural Network

Shi-Nan Wang, Yu-Jing Wu, and Yi-Nan Xu*

***Abstract*—The in-vehicle bus network is an important part that directly affects the safety of the car, so the real-time, safety and reliability of the vehicle bus network must be guaranteed. Connected to smart phones, Bluetooth, Internet, etc., the car enhances the driving pleasure. On the other hand, it brings hacker attacks, security vulnerabilities and other security issues that cannot be ignored, which seriously affects the car's driving safety, personal privacy, and even threatens public safety. The characteristics of the vehicle bus information are hexadecimal data with consistency, time series, and ID. This paper diagnoses the abnormality in the vehicle bus, firstly preprocesses the bus data, and then uses the convolutional neural network method to detect the abnormality of the CAN bus information. By adjusting the neural network parameters during the experiment, the final detection rate is as high as 99.9%. It can well guarantee the security of bus data.**

***Index Terms*—Vehicle bus, convolutional neural network, can, network security, detection rate.**

I. Introduction

The in-vehicle bus network is the main tool for transferring data between the various electronic control systems installed in the car. With the accelerating process of automotive electronics and automation, and the maturity of technology, the vehicle bus network system is no longer an independent and safe network system. Over the past 50 years of development of vehicle bus networks, vehicle bus network protocols such as LIN, CAN, and FlexRay have not considered network security issues. When the car's electronic control system is connected to a smart phone, OBD II network tester, wireless network and other systems used in a car repair shop, it is easy to leak the information of the car's bus network, and there is a possibility of losing the car's control authority. Therefore, how to proactively defend the security vulnerabilities in the data layer and the physical layer in the communication protocol is the key core problem, which must be solved in the development process of the Internet car.

In July 2015, after two U.S. security researchers demonstrated the remote intrusion of the vehicle bus network of the Grand Cherokee SUV vehicle 16 kilometers away. The FBI, the U.S. Department of Transportation, and the National Highway Traffic Safety Administration and other departments jointly issued warnings about car network security in March 2016 [1]. Literature [2] proposed a vehicle network intrusion detection method based on CAN message time interval analysis. The time interval is an important factor for detecting abnormal data on the CAN bus. It has high real-time performance, but this method cannot detect tampering with the data content and does not have the ability to detect aperiodic signals. Reference [3] proposed a method for judging the abnormality of bus data based on the threshold of data change. When the bus data exceeds the original change range, it is judged as a malicious frame. Literature [4] proposed a method for detecting abnormal data based on the application of information entropy. This method needs to intercept data for a period of time to judge, and the real-time performance is poor. The in-vehicle bus network is a real-time communication system, and real-time performance must be guaranteed. Therefore, this method cannot meet the in-vehicle communication network with high real-time requirements.

Considering that the bus data has a time series problem, and the bus data context has a coherent relationship. This paper presents a convolutional neural network algorithm combined with contextual anomaly detection. This detection method can quickly and accurately detect information anomalies on the CAN bus.

The second chapter of this article outlines the reasons why the CAN bus is vulnerable to attack, the ways it can be attacked, and the various methods of ensuring data security. Chapter III describes the establishment of anomaly database based on context, and proposes a preprocessing scheme for data and the construction of neural network framework. Chapter IV verifies the reliability of the method proposed in this paper through experimental simulation. Chapter V summarizes the full text.

II. Network Security Analysis of CAN Bus

A. Network Attack Mode of CAN Bus

1) Network attack with direct physical connection. OBD-II is a bus network diagnostic equipment commonly used in automobile repair stations. OBD-II equipment can be directly connected to the diagnostic segment of the vehicle network, and the vehicle can be controlled by illegally using diagnostic services. In addition, hackers can indirectly enter the vehicle network through a virus-infected USB or mobile phone, which affects the safety of the vehicle bus network [5], [6]. For electric vehicles, you can communicate with the in-vehicle network by connecting the charging interface.

2) Long-distance indirect wireless connection. Most vehicles have bluetooth communication function, and use Bluetooth communication to realize wireless car key control, mobile phone connection, etc. Hackers can invade the

Manuscript received October 15, 2020; revised January 7, 2021. This work was supported by the National Natural Science Foundation of China (61763047).

The authors are with the College of Engineering of Yanbian University, Yanji, 133002, China (e-mail: ynxu@ybu.edu.cn).

DOI: 10.7763/IJCTE.2021.V13.1288

Bluetooth network to control the vehicle bus network. Hackers connect to the network through Wi-Fi or make vehicles access to fake base stations. At present, radar technology, such as millimeter wave radar and ultrasonic radar, is fully used in the active safety and assisted driving systems of automobiles. The hacker played a false radar signal to make the car controller judge wrong.

3) Information service center connection. At present, many vehicles support information service functions and remote information exchange with vehicle service centers. Vehicle mobile communication data connection is an external interface that poses the greatest threat to vehicle network security. A hacker can use a pseudo base station to connect the car's network to a fake TSP, and then use the parsed control commands to issue dangerous commands to the car. For example, open the door, control the steering wheel, and adjust the speed suddenly while driving.

B. Network Vulnerability Analysis of CAN Bus

The CAN bus adopts a multi-master competitive bus structure. It has the characteristics of a serial bus and broadcast communication with multi-master operation and decentralized arbitration. The communication rate can be up to 1Mbps, and it has the characteristics of real-time and strong application. But the CAN bus network has the following network vulnerability determination.

1) The CAN bus has no encryption mechanism. When the vehicle CAN bus network information is exchanged, the plain text data is sent directly, and the data is not encrypted. The CAN bus sends messages in the form of broadcast. Any message on the network can be received by any node in the network. Intruders can easily collect bus data and use the collected data to launch attacks to cause vehicle driving safety problems [7]-[9].

2) The CAN bus lacks a data authentication mechanism. In the vehicle network data transmission, only a few message data contents with higher security level are verified, but the verification algorithm is simple, usually using a simple XOR check, which is easy to be cracked, so the CAN bus lacks effective report Document authentication mechanism, the receiving node cannot identify the authenticity of the data. Once the intruder falsifies or tampers with the data content, it will make the vehicle-mounted control unit unable to perform the control according to the driver's wishes, resulting in the vehicle losing control and even causing traffic accidents [10], [11].

3) Priority arbitration mechanism based on frame ID. In the CAN bus, messages with high priority guarantee transmission of data without affecting the determination time of bus conflicts, while messages with low priority must wait for the next idle state. Therefore, hackers can easily use high-priority IDs to launch network attacks.

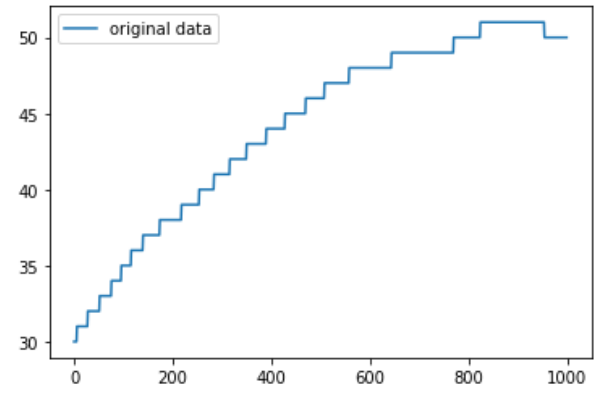
III. CAN Bus Context Anomaly Detection Scheme Based on Convolutional Neural Network

A. Data Processing

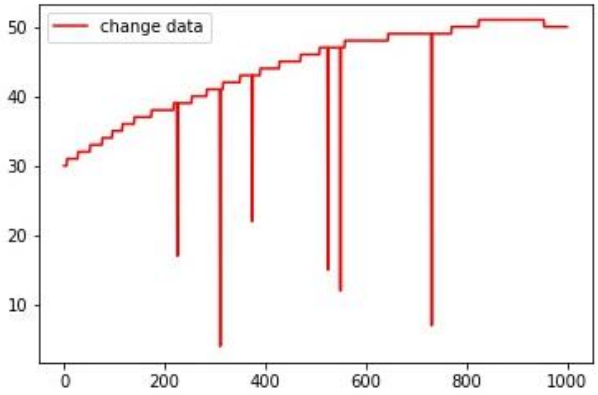
During the driving process of the vehicle, the CAN bus data changes in real time. Under different driving conditions, the data in the corresponding CAN data frame changes. Therefore, the data changes between each context data frame have a certain correlation. However, when the vehicle bus network is invaded, data that will cause driving problems will be added, and the tampered bus data will break the original correct context.

The data used in this study is to read the CAN bus data of the actual car driving through the OBD interface. Data with different IDs on the CAN bus are interleaved and sent alternately, each containing different information. Therefore, this paper first classifies the data according to ID, and aggregates the data with the same parameters. Second, it is the generation of abnormal data on the CAN bus. Since no malicious intrusion has occurred during driving, the erroneous data needs to be made manually. In order to ensure that the erroneous data is in line with reality, and the experimental results are more reliable and effective.

In this paper, based on the driving rules of the car and the principle of contextual anomaly detection, the contextual anomaly detection is reversed to use data processing. By making mutations in the data meets the driving accidents is generated. At the same time, in order to ensure that the abnormal data position and value are irregular, it can be realized by programming, and the abnormal data is inserted in a random generation and random replacement manner. Fig. 1 (a) is the intercepted vehicle speed data with no abnormality in a short period of time. It can be seen that the data is context-sensitive and there is no mutation, and the data is gradually climbing. Fig. 1 (b) is the driving data after randomly inserting abnormal data. The abnormal data is made based on the principle of context detection. It can be seen that multiple mutation data are added when the overall trend is unchanged.



(a) Normal data



(b) Abnormal data

Fig. 1. Comparison of normal speed data and abnormal data set.

B. Network Structure and Principle

Vehicle CAN bus data is a hexadecimal number with time series. In the processing of one-dimensional data with time series, more is applied to the recurrent neural network. In the vehicle bus network, ECUs communicate frequently and the amount of data is huge. It is necessary to ensure the transmission of important information. It is too expensive to use RNN to process huge data sets. Therefore, this paper uses a one-dimensional convolutional neural network, which is less expensive than RNN and performs well in processing one-dimensional time series data.

Convolutional neural networks can be divided into three methods: one-dimensional, two-dimensional, and three-dimensional. The one-dimensional convolution applied in this paper is similarly to the two-dimensional network in principle, but the convolutional layer and the pooling layer are one-dimensional filters and pooling. In the choice of loss function, this paper applies the cross-entropy loss function. The structure of convolutional neural network is mainly composed of convolutional layer, pooling layer and fully connected layer. The convolutional neural network internally adjusts the weights in the network through gradient descent to minimize the loss function, and at the same time improves the accuracy of the neural network through frequent iterative training. The convolutional neural network combines a series of convolutional layers and pooling layers to make the network have a certain degree of displacement, scale, scaling, nonlinear deformation stability, and finally output through the fully connected layer [12].

The convolution layer is a feature extraction operation through a convolution kernel, which is to multiply a region according to the dimensional shape of the convolution kernel, multiply point by point and then sum, condense into a scalar value, that is, drop to zero Dimension, the step size in the convolutional layer is an important parameter. The mathematical calculation of convolution is shown in Equation 1. Where s and t represent the width of the convolution kernel in the x and y directions, F is the parameter matrix of the convolution kernel, G is the local image matrix calculated with the convolution kernel function, and k is the size of the convolution kernel.

$$Cov(x,y) = \sum_{t=0}^{k} \sum_{s=0}^{k} F(s,t) \times G(x-s, y-t) \quad (1)$$

The maximum pooling layer is to take the maximum value in the pooling range, which is equivalent to performing dimensionality reduction operations on the data, which can effectively reduce the amount of network operations and extract the most obvious features. The mathematical expression is shown in Equation 2. Among them, P is the feature matrix obtained after pooling, A is the feature matrix obtained by convolution, and w is the width of the pooling area. The fully connected layer is equivalent to the classifier in the neural network. The neurons in the fully connected layer are fully connected with all the neurons in the previous layer to integrate the information in the pooling layer. According to the needs of the experimental network, the output is passed to softmax Layer to make the final judgment.

$$P = max_{w \times w}(A^{l \times l}) \quad (2)$$

The fully connected layer acts as a classifier in the convolutional neural network, integrates the highly abstracted features after multiple convolutions, and then can be normalized to output a probability for various classification situations. Probability for subsequent classification. The mathematical expression is shown in Equation 3. Where z_j^{l+1} is the activation value of the j-th neuron in layer $(l + 1)$, a_i^l is the activation value of the i-th neuron in layer l, and W_{ij}^l is the $(l + 1)$-th layer. The weight between the j-th neuron and the i-th neuron in layer l, b_j^l is the offset of all neurons in layer l to the j-th neuron in layer $l + 1$.

$$z_j^{l+1} = \sum_{i=1}^{n} W_{ij}^l a_i^l + b_j^l \quad (3)$$

The overall experimental process gathers the contents of 3.1 and 3.2. After reading the data through the data processing module, it enters the convolutional neural network module. First, the data and the label are separated, and the convolutional neural network is established. Set and test set, adjust the network parameters for training, and finally judge whether the data is abnormal through the network's convolution layer, pooling layer and fully connected layer. Observe whether the training result reaches the target detection rate. If it does not reach the target detection rate, adjust the parameters, and finally retain the parameters in the optimal state, use the remaining part of the data to test, and finally output the result graph. The overall flow chart is shown in Fig. 2.

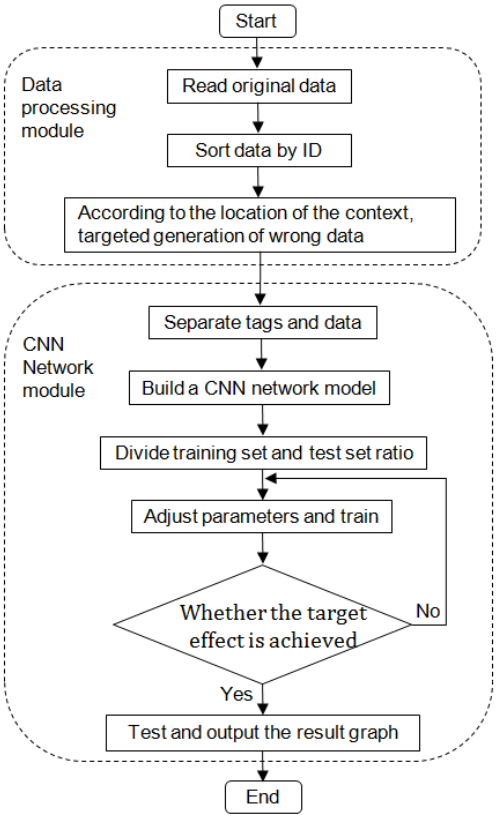


Fig. 2. Flow chart of bus information anomaly detection.

IV. Simulation Experiment

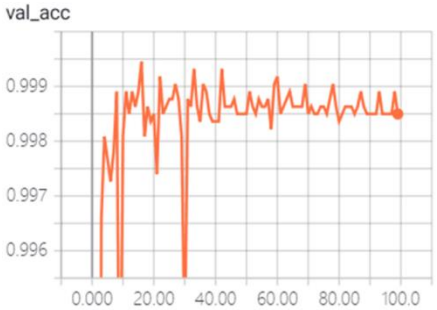
After the network is successfully built, the processed data is passed in, the training set and the test set are divided into proportions, and the parameters are adjusted. The optimized parameter settings are shown in Table I.

TABLE I. CONVOLUTIONAL NEURAL NETWORK PARAMETERS

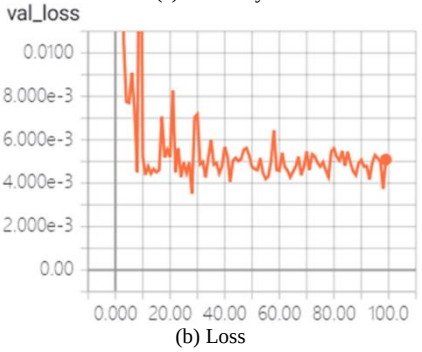
Name	Parameter value	Name	Parameter value
Filter_number	512	Filter_length	1
Dropout	0.4	Dense_num	2
Dense1	2048	Dense2	1024
Learn rate	0.1	Nesterov	True
Momentum	0.9	Decay	1e-6
Batch -size	16	epoch	3

In Table I, Filter_number is the number of convolution kernels, representing the number of extracted features. Filter_length is the length of each convolution kernel. Dropout is used to avoid overfitting, and makes the network training with fewer parameters, testing with more parameters and strong performance. Dense is a fully connected layer. The experimental model in this paper has two fully connected layers. The first fully connected layer has 2048 neurons and the second fully connected layer has 1024 neurons. Learn rate is the initial learning rate. If the learning rate is too large, the parameters to be optimized will fluctuate around the minimum value and will not converge. If the learning rate is too small, the parameters to be optimized will converge slowly. Nesterov represents whether Newton momentum is used, which is an optimization method. Decay is the regular term coefficient, which is used to slow down the overfitting of the model. The neural network is input by batch, Batch_size refers to how much data each batch contains when input.

Under the conditions of the above network parameters, the final training result is shown in Fig. 3. It can be seen that the accuracy rate has dropped significantly twice during the training process, but the overall is above 99%. The test result is shown in Fig. 4. There were two large fluctuations in the accuracy rate during the test, and the other fluctuations were all controlled within 0.01%, and the accuracy rate in the later test reached close to 99%. The test accuracy rate is relatively stable, the two obvious small fluctuations are also within 0.02%, the final accuracy rate is more than 99.9%, and the loss function also declines rapidly and steadily. The overall network effect is better.



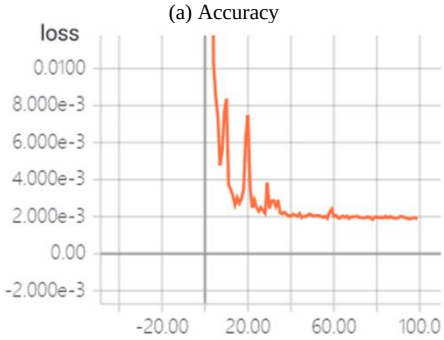
(a) Accuracy



(b) Loss

Fig. 3. Training results.

(a) Accuracy



(b) Loss

Fig. 4. Test results.

V. CONCLUSION

With the increase in the number of electronic and communication devices carried in the vehicle, the vehicle bus network is no longer an independent network system, and the vehicle bus network system is relatively easy to be invaded, so vehicle safety poses a hidden danger to network security. As a widely used vehicle bus network system, the safety of the on-board CAN bus network is crucial. This paper proposes a CAN bus information anomaly detection method based on convolutional neural network for CAN bus network. And according to the principle of contextual anomaly detection, a network test environment where vehicles are invaded while driving is built. Using Tensorflow program for experimental simulations, the results show that the bus information anomaly detection method proposed in this study has an accuracy rate of more than 99.9% for vehicle bus anomaly data detection under the optimal parameter state.

CONFLICT OF INTEREST

The authors declare no conflict of interest.

AUTHOR CONTRIBUTIONS

Shi-Nan Wang: Methodology and writing of original draft; Yu-jing Wu: Software and formal analysis; Yi-Nan Xu: Conceptualization and supervision.

REFERENCES

[1] C. Miller and C. Valasek, "Remote exploitation of an unaltered passenger vehicle," *Black Hat*, Las Vegas, USA, 2015.

[2] H. M. Song, H. R. Kim, and H. K. Kim. "Intrusion detection system based on the analysis of time intervals of CAN messages for in-vehicle network," in *Proc. International Conference on Information Networking*, 2016, pp. 63-68.

[3] Z.-J. Zhang, Y. Zhang, and J. Wang, "An anomaly detection system applied to CAN bus," *Information Security and Communications Privacy*, 2015.

[4] W. Wu, "A survey of intrusion detection for in-vehicle networks," *IEEE Transactions on Intelligent Transportation Systems*, p. 99, 2019.

[5] T. Hoppe, S. Kiltz, and J. Dittmann, "Security threats to automotive CAN networks–practical examples and selected short-term countermeasures," *Computer Safety, Reliability, and Security*, Springer Berlin Heidelberg, 2008.
[6] C. Lin and A. Sangiovanni-Vincentelli, "Cyber-security for the Controller Area Network (CAN) communication protocol," in *Proc. 2012 International Conference on Cyber Security*, 2012, pp. 1-7.
[7] M. J. Kang and J. W. Kang, "A novel intrusion detection method using deep neural network for in-vehicle network security," in *Proc. Vehicular Technology Conference*, 2016, pp. 1–5.
[8] T. Vasistha and D. Kumar, *Detecting Anomaliesin Controller Area Network*.
[9] A. Taylor, S. Leblanc, and N. Japkowicz, "Anomaly detection in automobile control network data with long short-term memory networks," in *Proc. International Conference on Data Science & Advanced Analytics*, 2016, pp. 130–139.
[10] Z. Gu, G. Han, H. Zeng *et al*., "Security-aware mapping and scheduling with hardware co-processors for FlexRay-based distributed embedded systems," *IEEE Transactions on Parallel and Distributed Systems*, vol. 27, no. 10, pp. 3044-3057, 2016.
[11] S. Woo, H. J. Jo, and H. L. Dong, "A practical wireless attack on the connected Carand security protocol for in-vehicle CAN," *IEEE Transactions on Intelligent Transportation Systems*, vol. 16, no. 2, pp. 993–1006, 2015.
[12] A. Krizhevsky, I. Sutskever, and G. Hinton, "ImageNet classification with deep convolutional neural networks," *Advances in Neural Information Processing Systems*, vol. 25, no. 2, 2012.

Shi-Nan Wang was born at Jilin Province of China. She received the bachelor degree in communication engineering from Yanbian University, China, in 2019.

She is a currently working toward a master degree in the area of in-vehicle network, which include the design of security architecture of FlexRay.

Yu-Jing Wu was born at Jilin Province of China. She received her M.S. and Ph.D in electronic and information engineering from Chonbuk National University, South Korea, in 2013 and 2016, respectively.

She is a lecturer of the Division of Electronic and Communication Engineering of Yanbian University, China. Her research interests are in the area of VLSI implmentation for digital signal processing and communication system, which include the design and in implementation of security protocol for in-vehicle networks.

Yi-Nan Xu was born at Jilin Province of China. He received the Ph.D. degree in electronics engineering from the Chonbuk National University, South Korea, in 2009.

He is a professor of the Division of Electronics and Communication Engineering of Yanbian University, Yanji, China. His research interests include the In-vehicle network and automobile electronic control.